SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

OrangeDX

AUDIT

SECURITY ASSESSMENT

25 August, 2024

for

OrangeDX

CONTENTS

Introduction

SolidProof.io is a brand of the officially registered company FutureVisions Deutschland, based in Germany. We're mainly focused on Block-chain Security such as Smart Contract Audits and KYC verification for project teams. Solidproof.io 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 are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, Pancake-Swap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	OrangeDX
Website	https://orangedx.com
About the Project	N/A
Chain	None
Language	Rust
Codebase	N/A
Commit	N/A
Unit Tests	N/A

Social Medias

Telegram	https://t.me/OrangeDx_Official_Chat
Twitter	https://twitter.com/OrangDx_BRC20
Facebook	N/A
Instagram	N/A
GitHub	N/A
Reddit	N/A
Medium	https://medium.com/orange_dex
Discord	N/A
YouTube	N/A
TikTok	N/A
LinkedIn	N/A
CoinMarketCap	N/A

Audit Summary

Version	Delivery Date	Change Log
v1.0	25 August, 2024	• Layout Project • Automated/Manual-Security Review • Summary

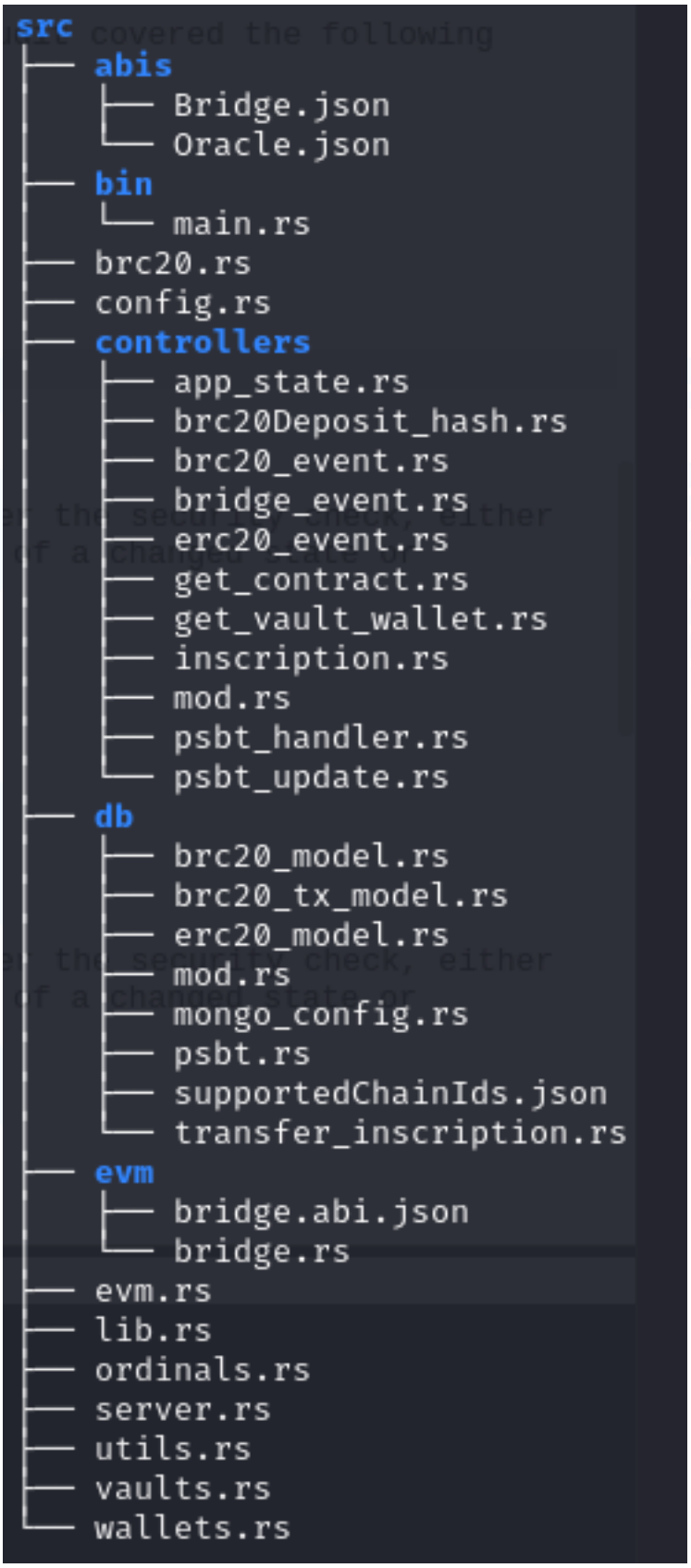
Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.

File Overview

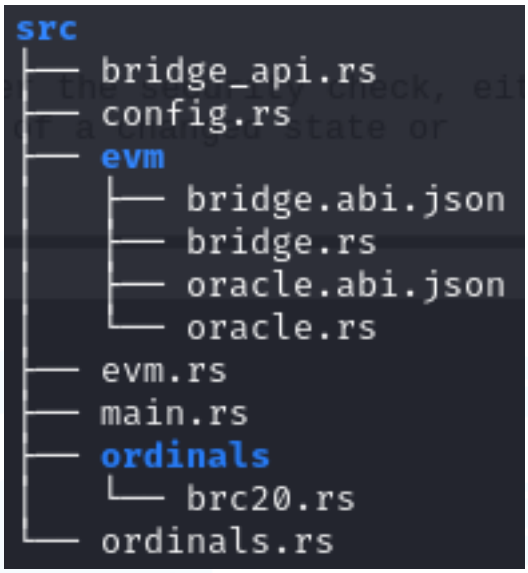
The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with a SHA-1 Hash.

1. inscription-multisig-master.zip (99a7a80cd803af3fca82fe7bd1e9db6c82f98030)

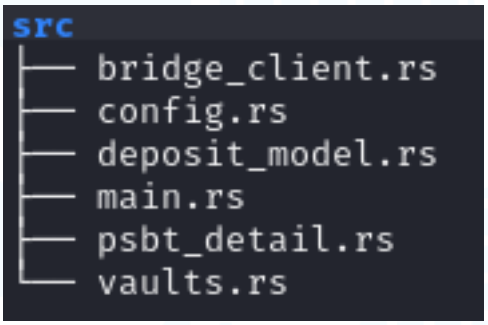
2. orange_bridge_api-master.zip (5189dfc2227299ce644d3f3c2e4d1ca605278165)



3. orange_oracle-master.zip
   (32c56dac22527d793c606ed1e3bb62bbbbd229f9)



4. signing_server-master.zip
   (7685c3519255f9284c1ee39ca53db3eb12a97ede)



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).

1. inscription-multisig
   (a) anyhow = ”1.0.81”
   (b) bdk = ”0.28.0”
   (c) bincode = ”1.3.3”
   (d) ctrlc = ”3.4.4”
   (e) dotenv = ”0.15.0”
   (f) nix = ”0.28.0”
   (g) ordinals = ”0.0.7”
   (h) ping = ”0.5.2”
   (i) reqwest = ”0.12.3”
   (j) serde = ”1.0.197”
   (k) tokio = ”1.37.0”
2. orange_bridge_api
   (a) tokio =”1”
   (b) axum = ”0.7.4”
   (c) dotenv = ”0.15.0”
   (d) serde_json = ”1.0.114”
   (e) ethers = ”2.0.14”
   (f) eyre = ”0.6.12”
   (g) hex = ”0.4.3”
   (h) futures = ”0.3.30”
   (i) mongodb = ”2.8.1”
   (j) serde = ”1.0.197”
   (k) tower-http = ”0.5.2”
   (l) tracing = ”0.1.40”
   (m) tracing-subscriber = ”0.3.18”
   (n) warp = ”0.3.6”
   (o) reqwest = ”0.12.3”
   (p) anyhow = ”1.0.79”
   (q) inscription-multisig = ”0.1.12”
   (r) axum_typed_multipart = ”0.11.1”

3. orange_oracle
   (a) anyhow = ”1.0.82”
   (b) bincode = ”1.3.3”
   (c) dotenv = ”0.15.0”
   (d) ethers = ”2.0.14”
   (e) reqwest = ”0.12.4”
   (f) serde = ”1.0.198”
   (g) serde_json = ”1.0.116”
   (h) sled = ”0.34.7”
   (i) tokio = ”1”
   (j) tokio-stream = ”0.1.15”
   (k) tracing = ”0.1.40”
   (l) tracing-subscriber = ”0.3.18”
4. signing_server
   (a) anyhow = ”1.0.83”
   (b) tokio = ”1”
   (c) tracing = ”0.1.40”
   (d) tracing-subscriber = ”0.3.18”
   (e) dotenv = ”0.15.0”
   (f) sled = ”0.34.7”
   (g) serde_json = ”1.0.114”
   (h) serde = ”1.0.197”
   (i) inscription-multisig = ”0.1.7”
   (j) reqwest = ”0.12.4”

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.

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
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 as possible.
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 pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered. We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodolgy

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 analysing a program to determine what inputs causes 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

Medium or higher issues

No critical issues found	✅ **Program is safe to use**
Description	The program does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the source code.
Comment	N/A

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart- contract-based accounts, such as multi-signature wallets.

Here are some suggestions what the client can do.

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness on privileged operations
- Introduce a DAO/Governance/Voting module to increase transperancy and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

No low issues

Informational issues

#1 | Delete unused code

File	Severity	Location	Status
Main	informational	–	open

Description - On multiple files and sections of the code, unused code is commented out instead of being deleted. For good readable code, it is recommended to delete that lines instead.

#2 | Using rust naming convention

File	Severity	Location	Status
Main	informational	–	open

Description - On multiple files and sections of the code, functions names are not named after the rust naming convention.

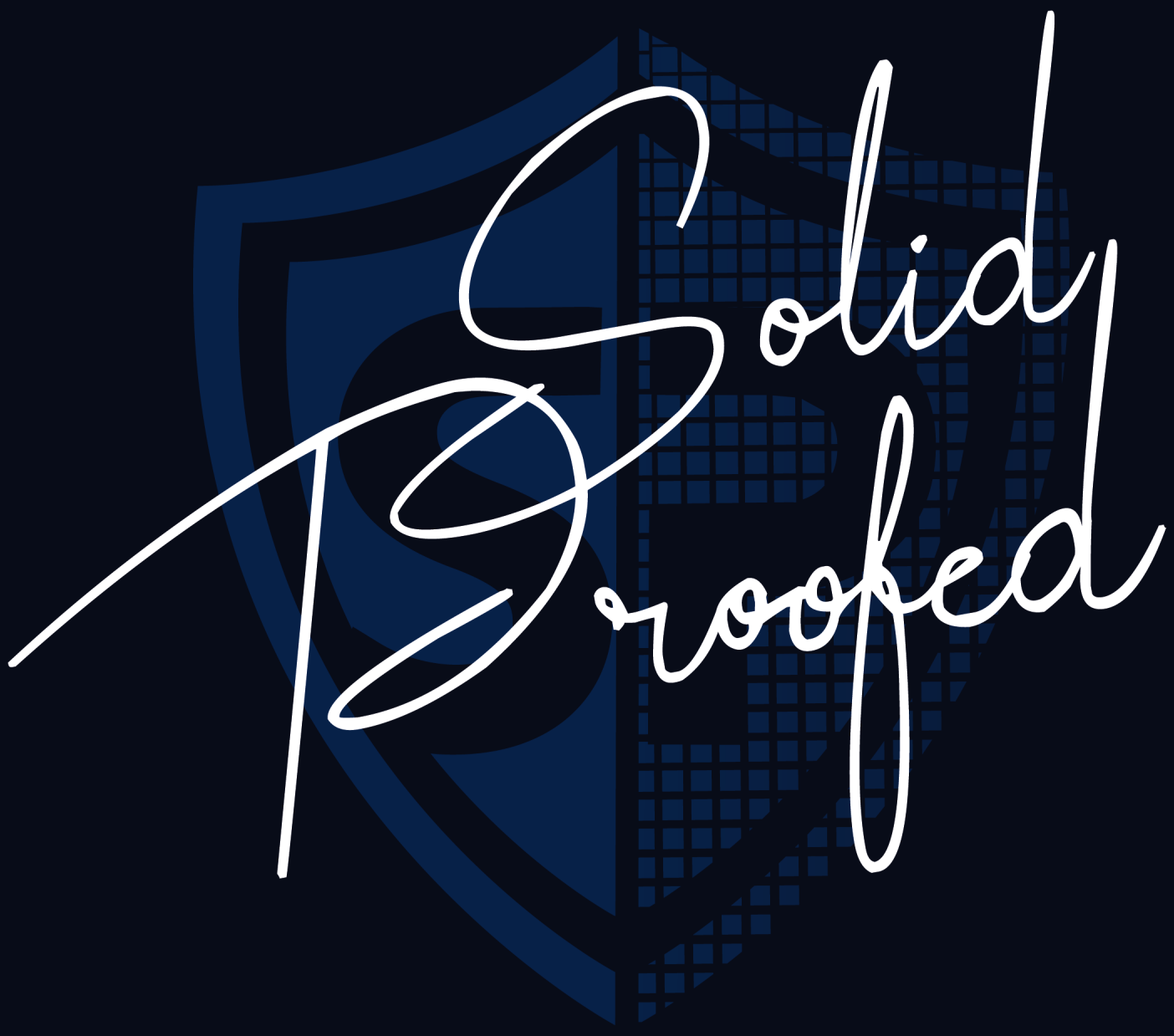
#3 | Delete unsued imports

File	Severity	Location	Status
Main	informational	–	open

Description - On multiple files, there are unused imports, it is recommended to delete these unused imports.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.



Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY