



SOLIDProof

Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

Dirac Finance

AUDIT

SECURITY ASSESSMENT

25. February, 2024

FOR



DIRAC FINANCE



SolidProof_io



@solidproof_io

Introduction	4
Disclaimer	4
Project Overview	5
Summary	5
Social Medias	5
Audit Summary	6
File Overview	7
Imported packages	8
Audit Information	9
Vulnerability & Risk Level	9
Auditing Strategy and Techniques Applied	10
Methodology	10
Overall Security	11
Upgradeability	11
Ownership	12
Ownership Privileges	13
Minting tokens	13
Burning tokens	14
Blacklist addresses	15
Fees and Tax	16
Lock User Funds	17
Components	18
Exposed Functions	18
StateVariables	18
Capabilities	19
Centralization Privileges	20
Audit Results	21
Critical issues	21
High issues	21
Medium issues	21



Low issues

22

Informational issues

23



Introduction

[SolidProof.io](https://solidproof.io) is a brand of the officially registered company MAKE Network GmbH, based in Germany. We mainly focus on Blockchain Security, such as Smart Contract Audits and KYC verification for project teams.

Solidproof.io assesses potential security issues in implementing smart contracts, reviews potential inconsistencies between the code base and the whitepaper/documentation, and provides suggestions for improvement.

Disclaimer

[SolidProof.io](https://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 contracts or services (such as Uniswap, Uniswap, PancakeSwap, etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analysed or any indication of the technology proprietors. SolidProof Audits should not be used to make decisions around investment or involvement with any particular project. These reports do not provide investment advice, nor should they be leveraged as investment advice.

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 due diligence and continuous security. SolidProof does not claim any guarantee of the security or functionality of the technology we agree to analyse.

Project Overview

Summary

Project Name	Dirac Finance
Website	https://www.dirac.finance/
About the project	Dirac Finance redefines DeFi yield generation by combining TradFi sophistication with DeFi accessibility. This marks the emergence of a new generation of innovative DOV protocols.
Chain	Polygon zkEVM, SKALE, zkSync
Language	Solidity
Codebase Link	Provided as Files (Private Repo)
Commit	N/A
Unit Tests	Provided

Social Medias

Telegram	https://t.me/diracfinanceofficial
Twitter	https://twitter.com/DiracFinance
Facebook	N/A
Instagram	N/A
Github	https://github.com/Dirac-Finance
Reddit	N/A
Medium	https://medium.com/@DiracFinance/introducing-dirac-finance-decentralized-structured-products-vaults-6266e810aee3
Discord	https://discord.gg/wtdxVcvF
Youtube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	21. January 2024	<ul style="list-style-type: none"> • Layout Project • Automated- /Manual-Security Testing • Summary
v1.1	25. February	<ul style="list-style-type: none"> • Reaudit

Note - The following audit report presents a comprehensive security analysis of the smart contract utilised in the project that includes outside manipulation of the contract's functions in a malicious way. 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 we did not functionally test it. This includes internal calculations in the formulae used in the contract.



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 an SHA-1 Hash.

File Name	SHA-1 Hash
DiracV1Broker.sol	9aa9d954ceb67415a9ba06c3cbf82c87996315c0
DiracV1VaultFactory.sol	588cb514becd9aa74aa62916efe2d1c4925345f9
DiracV1Base.sol	732417b8c944a6f2c8ddcd34d338695a10a3d16b
DiracV1ProxyRazor.sol	5659de40e3c42b7a964cb1d874906effd0452291
DiracV1Vault.sol	ccb3a3838053c37911df1cdc51a7bc83c6aeaeae
DiracV1ProxyChainlink.sol	381b1d374ec5a9e1a848ce548ebeede265ce141d
DiracV1ProxyApi3.sol	4281b5b6bc022862249fc8ed4991ab85a3b05a32
DiracV1Base.sol	b76ad4b7ba11fcb6c20e4e283268387f729ccbd8

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) indicate 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).

Dependency / Import Path	Count
@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol	2
@openzeppelin/contracts/access/Ownable.sol	8
@openzeppelin/contracts/token/ERC20/IERC20.sol	9
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	2
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	1

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way

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. The 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.

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 determines whether test cases 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 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

Upgradeability

Contract is not an upgradeable



Deployer cannot update the contract with new functionalities

Description

The contract is not an upgradeable contract. The deployer is not able to change or add any functionalities to the contract after deploying.

Comment

N/A



Ownership

The ownership is not renounced

✗ The owner is not renounce

Description

The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:

- Centralizations
- The owner has significant control over contract's operations

Comment

N/A

Note - If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.



Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens

 **The owner cannot mint new tokens**

Description	The owner is not able to mint new tokens once the contract is deployed.
Comment	N/A



Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens		 The owner cannot burn tokens
Description	The owner is not able burn tokens without any allowances.	
Comment	N/A	



Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses



The owner cannot blacklist addresses

Description

The owner is not able blacklist addresses to lock funds.

Comment

N/A



Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%



The owner cannot levy unfair taxes

Description

The owner is not able to set the fees above 25%

Comment

The Fees functionality has not been implemented yet



Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Owner cannot lock the contract



The owner cannot lock the contract

Description

The owner is not able to lock the contract by any functions or updating any variables.

Comment

N/A

External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
7	2	2	4


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable
21	1



External	Internal	Private	Pure	View
9	26	0	2	8

StateVariables

Total	 Public
14	12



Capabilities

Solidity Versions observed	Transfers ETH	Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
0.8.20	Yes	Yes		



Centralization Privileges

Centralisation can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if a single entity controls the contract or if certain participants have special permissions or abilities that others do not.

In the project, some authorities have access to the following functions:

File	Privileges
DiracV1Vault	<ul style="list-style-type: none"> • Deposit, Withdraw assets • Mint, Redeem Shares
DiracV1Broker	<ul style="list-style-type: none"> • Manually Settle Options
DiracV1Base	<ul style="list-style-type: none"> • Claim Protocol Revenues manually
DiracV1Controller	<ul style="list-style-type: none"> • Set Protocol Fee and Price Oracle Address

Recommendations

To avoid potential hacking risks, the client should carefully manage the private key of the privileged account. Additionally, we recommend enhancing the security practices of centralised privileges or roles in the protocol through a decentralised mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of 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 of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency 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

#1 | Signature Malleability

File	Severity	Location	Status
DiracV1Broker	Low	L115	Fixed

Description - The contract lacks a check to verify that the same signature should not be used again for a transaction. We recommend implementing nonces to track the used signatures.



Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
DiracVTVault	Informational	L31—84	Fixed

Description - If you started to comment on your code, comment on all other functions, variables etc.

#2 | Floating Pragma

File	Severity	Location	Status
All	Informational	N/A	Fixed

Description - The contracts should be deployed with the same compiler version and flag that they have been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions.

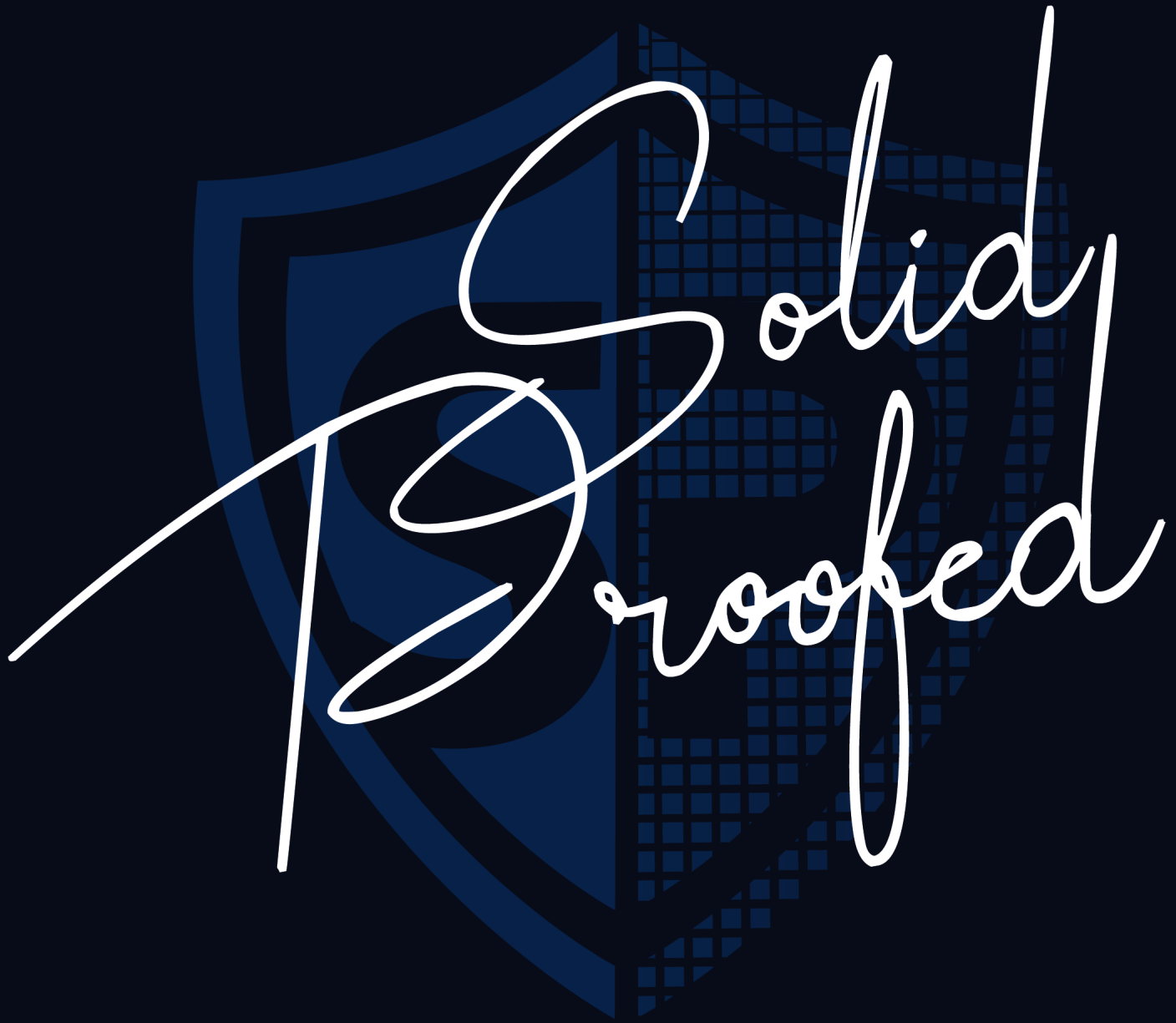
#3 | Contract doesn't import npm packages from source (like OpenZeppelin etc.)

File	Severity	Location	Status
All	Informational	N/A	Fixed

Description - We recommend importing all packages from npm directly without flattening the contract. Functions could be modified or can be susceptible to vulnerabilities.

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