



SOLIDProof

Bring trust into your projects

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

MADE IN GERMANY

Sifi

AUDIT

SECURITY ASSESSMENT

15. December, 2023

FOR



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
Inheritance Graph	20
Centralization Privileges	21
Audit Results	22
Critical issues	22
High issues	22



Medium issues	23
Low issues	24
Informational issues	24



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.

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, PancakeSwap 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 the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Sifi
Website	https://sifi.org
About the project	Sifi is a router for dexes and bridges. It allows the caller to use many different protocols; from the Uniswap DEX to the Stargate bridge, with a familiar interface
Chain	Ethereum, Arbitrum, Avalanche, Base, BNB Chain, Optimism, Polygon
Language	Solidity
Codebase Link	https://github.com/sifiorg/sifi/tree/master/packages/hardhat/contracts
Commit	1939e8b
Unit Tests	Provided

Social Medias

Telegram	N/A
Twitter	https://twitter.com/sifiorg
Facebook	N/A
Instagram	N/A
Github	N/A
Reddit	N/A
Medium	N/A
Discord	https://discord.gg/UGFqXxqFsu
Youtube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	15. December 2023	<ul style="list-style-type: none"> • Layout Project • Automated- /Manual-Security Testing • Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized 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
contracts/EnergyShield.sol	bf5da1487f7a11f375a10ae2d4c707c8e24adddb
contracts/SifiDiamond.sol	b090c3370752e744860174a9c11cc0709da94f05
contracts/init/DiamondMultinit.sol	0abd00e754894e243758d2f408a88698527df44d
contracts/init/InitUniV2Router.sol	3b5a5cb330a4ff0d8ecbbd5ed39770cd496691a1
contracts/init/InitLibWarp.sol	23cc1e1866f38520c46b377a96fa6da2921f613e
contracts/facets/Ens.sol	4beaba9b51487747d204e2aea29884a21887c64b
contracts/facets/UniV3Like.sol	c1716d501364201a9c142603019df2afbf8537e8
contracts/facets/Stargate.sol	5108a8f94c9517f43b5b92b3b75191778e6a4a4c
contracts/facets/UniV2LikeFacet.sol	5da6e71d1a607ad78a5262194f6ef36b31f3c7b7
contracts/facets/Curve.sol	0b358b4ee54ae4bb7250e3c0ca87e3cfef505b3d
contracts/facets/UniV2RouterFacet.sol	f29c09c72d4254a5dfde421639397d7b4a55824a
contracts/facets/Stateless.sol	0beef7ccce36451440fa2b2bdb8970d32be67d9c
contracts/facets/DiamondLoupeFacet.sol	d6577a93c7ece283f7a69db9b963c33cce066899
contracts/facets/UniV3Callback.sol	c23c37288ba1a40bcc100dadd9ff880c7d57a361
contracts/facets/WarpLink.sol	19ecadc0615e50332ac76c6635d7d04b3bc5eb61
contracts/facets/StarVault.sol	1eb91ac7e5d5e9f377ec8eb1408d601229c0a4ee
contracts/facets/OwnershipFacet.sol	70dd6f56cb02a11d4dbed4dfd87a4fe3f6d13c74
contracts/facets/DiamondCutFacet.sol	27e144648b91a17742323a5341d8f3ba3c0776ad

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).

Dependency / Import Path	Count
@openzeppelin/contracts/access/Ownable.sol	1
@openzeppelin/contracts/token/ERC1155/utils/ERC1155Holder.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	10
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	10
@openzeppelin/contracts/token/ERC721/IERC721.sol	1
@openzeppelin/contracts/token/ERC721/utils/ERC721Holder.sol	1
@openzeppelin/contracts/utils/Address.sol	4
@uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router02.sol	1
@uniswap/v2-periphery/contracts/interfaces/IWETH.sol	3

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	N/A



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
18	0	0	1


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
52	20

External	Internal	Private	Pure	View
50	69	1	0	7

StateVariables

Total	 Public
9	0



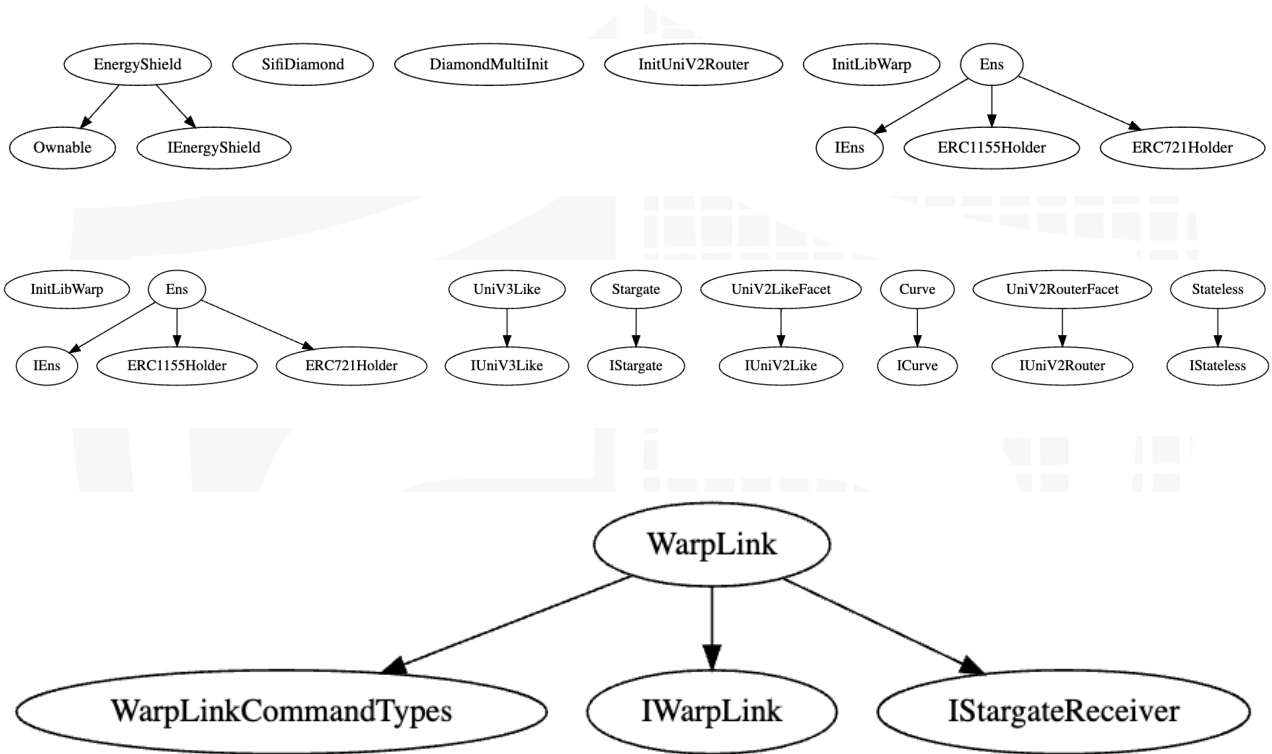
Capabilities

Solidity Versions observed	Transfers ETH	💰 Can Receive Funds	💻 Uses Assembl y	💣 Has Destroyable Contracts
^0.8.19	Yes	Yes		



Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.



Centralization Privileges

Centralization 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 the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project, there are authorities that have access to the following functions:

File	Privileges
EnergyShield	<ul style="list-style-type: none"> The owner can withdraw any type of tokens from the contract without any restrictions

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 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

#1 | Any user can drain tokens

File	Severity	Location	Status
EnergyShield	High	L23, 54, 92, 135	ACK

Description - Any arbitrary user can call this function to drain the holdings of this contract. If the 'delivers' params is false and also params.target can be passed as zero as there is no check for "msg.value" Then, according to the logic, the whole contract balance will be transferred to the caller.

Remediation - We recommend checking that the msg.value and the target parameter must be non-zero. It is also a better practice not to take input directly from the users because the caller can send arbitrary values in the parameters, leaving the function vulnerable.

Alleviation - The EnergyShield contract is meant to be stateless and never hold a balance. Because it can be instructed to perform any call by any user, any balance left in it would be up for grabs by any other user. To explain this further, we will add a comment in the code contracts/EnergyShield.sol line 20.

Medium issues

#1 | Missing Parameter Checks

File	Severity	Location	Status
Stargate	Medium	L20, 64	ACK
Stateless	Medium	L23, 62, 120	ACK

Description - The functions should check the validity of the parameters as well as the msg.value sent to this function. If the parameters are invalid, then the function call will revert. These functions can be called for free because of no checks for the msg.value.

Remediation - Make sure to validate all the parameters and check that msg.value is non-zero

Alleviation - Since the function on line 20 is internal, its parameters are checked by the callers in the functions on lines 64, 94, and 101. When bridging tokens, the user needs to first estimate the fees using Stargate's contract and use this value as msg.value. As you point out, the cal to stargateRouter.swap may revert if msg.value is insufficient, but we see this as acceptable to save gas on not estimating the fees inside the Sifi contract.

Low issues

No low issues

Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
All	Informational	N/A	ACK

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	ACK

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	ACK

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