



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Fraktal Audit

Security Assessment
11. March, 2022

For



FRAKTAL

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Inheritance Graph	12
CallGraph	13
Scope of Work/Verify Claims	14
Modifiers and public functions	17
Source Units in Scope	19
Critical issues	20
High issues	20
Medium issues	20
Low issues	20
Informational issues	20
Commented Code exist	21
Audit Comments	21
SWC Attacks	22

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

Version	Date	Description
1.0	11. March 2022	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Ethereum Chain

Website

<https://www.fraktal.io/>

Twitter

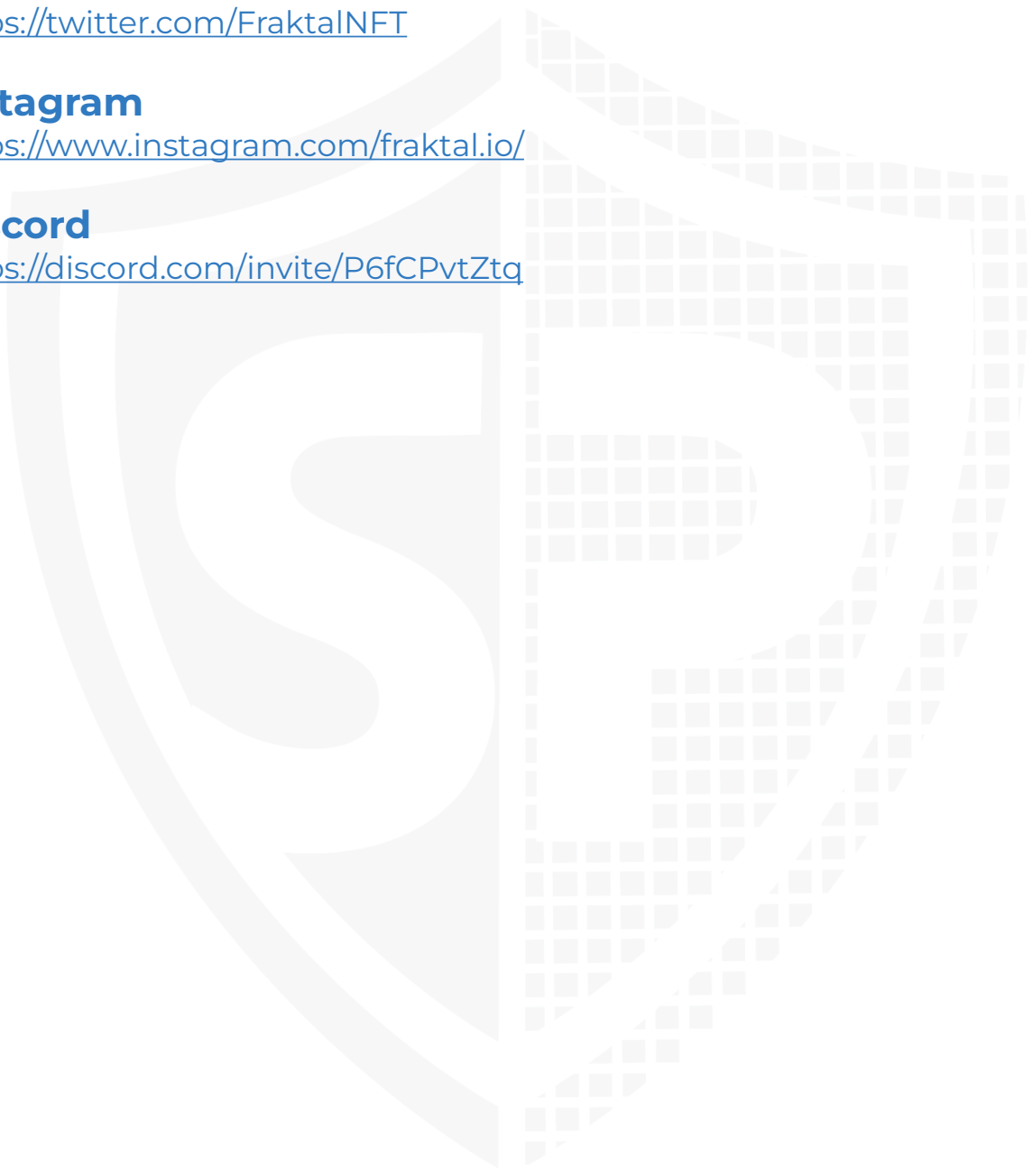
<https://twitter.com/FraktalNFT>

Instagram

<https://www.instagram.com/fraktal.io/>

Discord

<https://discord.com/invite/P6fCPvtZtq>



Description

Fraktal is a community first project, with a mission to to empower artists to be in full control of their work and have unlimited creative freedom.

Project Engagement

During the 23rd of February 2022, **Fraktal Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



FRAKTAL

Contract Link

v1.0

- Github
 - <https://github.com/FraktalNFT/contracts>
 - Commit:
 - fb292000554f97196485543fea4d1bb225a0961e
 - 51d3bac9509c514c472ab44b48a52afb50cccd26

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 evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

Dependency / Import Path	Count
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	1
@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/utils/SafeERC20Upgradeable.sol	2
@openzeppelin/contracts/access/AccessControl.sol	1
@openzeppelin/contracts/access/Ownable.sol	1
@openzeppelin/contracts/security/Pausable.sol	1
@openzeppelin/contracts/security/ReentrancyGuard.sol	2
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	1
@openzeppelin/contracts/utils/cryptography/MerkleProof.sol	1
@openzeppelin/contracts/utils/structs/EnumerableSet.sol	1

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

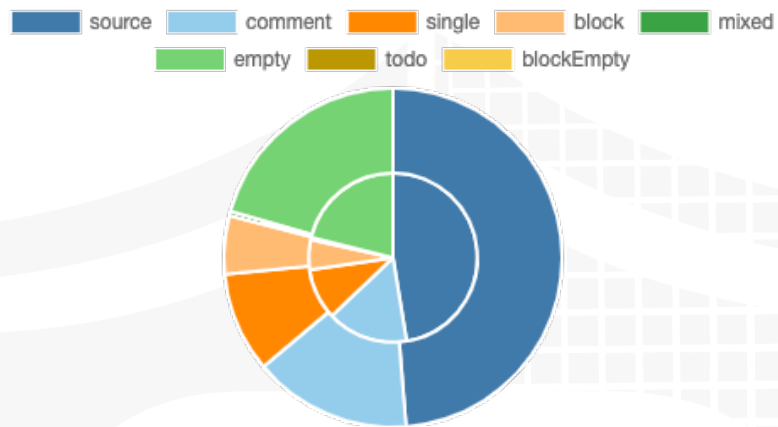
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

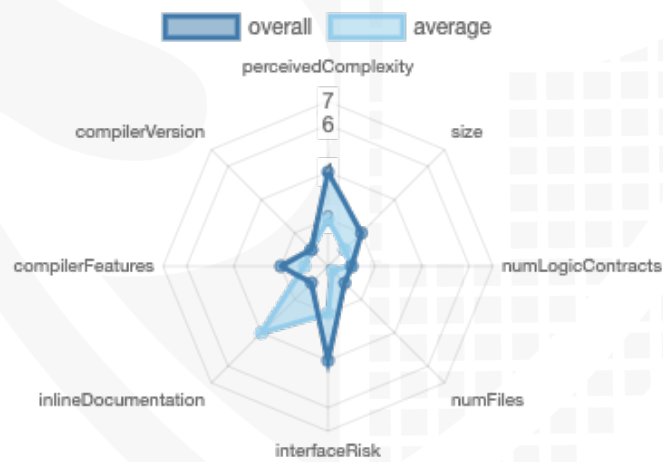
File Name	SHA-1 Hash
contracts/FeeSharingSystem.sol	bc29c221f8afb0603abc7b7060398dc369c865a2
contracts/FeeSharingSetter.sol	09f0f195de44f31c5111d062d8917033fdb587bd
contracts/IRewardConvertor.sol	c289c5dea4177d8533d772e82eca662a0ada51ab
contracts/TradingRewardsDistributor.sol	f803d0d67ca27a73cdb5648946c169af03fb40f9

Metrics

Source Lines v1.0



Risk Level v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	3	0	1	0

Exposed Functions

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

Version	Public	Payable
1.0	29	2

Version	External	Internal	Private	Pure	View
1.0	28	33	0	0	10

State Variables

Version	Total	Public
1.0	28	27

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	<code>^0.8.0</code>		<code>yes</code>		

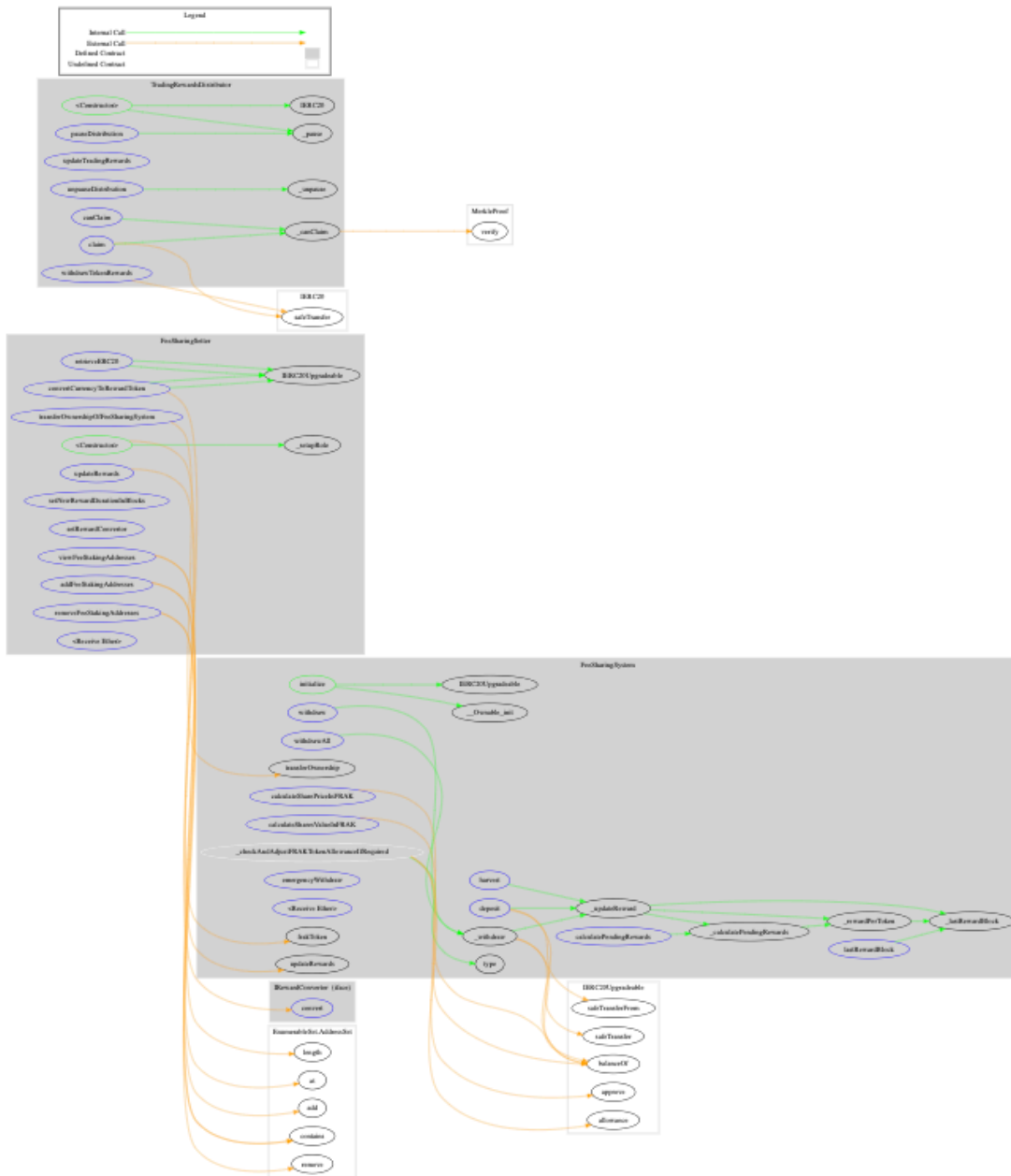
Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	EC Recover	New/Create/Create2
1.0	<code>yes</code>			<code>yes</code>		

Inheritance Graph

v1.0



CallGraph v1.0



Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Overall checkup (Smart Contract Security)



Write functions of contract v1.0

▼ FEESHARINGSYSTEM	▼ FEESHARINGSETTER	▼ TRADINGREWARDSDISTRIBUTOR
deposit	addFeeStakingAddres...	claim
emergencyWithdraw	convertCurrencyToRe...	pauseDistribution
harvest	grantRole	renounceOwnership
initialize	removeFeeStakingAd...	transferOwnership
renounceOwnership	renounceRole	unpauseDistribution
transferOwnership	retrieveERC20	updateTradingRewards
updateRewards	revokeRole	withdrawTokenRewards
withdraw	setNewRewardDurati...	
withdrawAll	setRewardConvertor	
	transferOwnershipOff...	
	updateRewards	

Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗
Not available	—

Modifiers and public functions

v1.0

FeeSharingSetter

- updateRewards
 - onlyRole
- convertCurrencyToRewardToken
 - nonReentrant
 - onlyRole
- addFeeStakingAddresses
 - onlyRole
- removeFeeStakingAddresses
 - onlyRole
- setNewRewardDurationInBlocks
 - onlyRole
- setRewardConvertor
 - onlyRole
- transferOwnershipOfFeeSharingSystem
 - onlyRole
- retrieveERC20
 - onlyRole

TradingRewardsDistributor

- claim
 - whenNotPaused
 - nonReentrant
- updateTradingRewards
 - onlyOwner
- pauseDistribution
 - onlyOwner
 - whenNotPaused
- unpauseDistribution
 - onlyOwner
 - whenPaused
- withdrawTokenRewards
 - onlyOwner
 - whenPaused

FeeSharingSystem

- initialize
 - initializer
- deposit
 - nonReentrant
- harvest
 - nonReentrant
- withdraw
 - nonReentrant
- withdrawAll
 - nonReentrant
- updateRewards
 - onlyOwner
- emergencyWithdraw
 - onlyOwner
- <Constructor> 💰

Info: Not listed functions are functions from imported libraries (OpenZeppelin)

Comments















Information: Not listed functions are from imported libraries

- FeeSharingSetter
 - DEFAULT_ADMIN_ROLE can
 - Add new fee staking addresses
 - Remove fee staking addresses
 - Update next reward duration in block
 - Set new reward convertor address
- FeeSharingSystem
 - onlyOwner can
 - Set current reward per block
 - Set period end block
 - Call emergency withdraw
- TradingRewardsDistributor
 - onlyOwner can
 - Update
 - merkleRootOfRewardRound
 - merkleRootUsed
 - maximumAmountPerUserInCurrentTree
 - OnlyOwner can lock user funds here if it is set to 0
 - Un-/Pause contract
- rewardConvertor was not provided to Solidproof, please do your own research here
- Claim can only be called in TradingRewardsDistributor if contract is not paused
- Tokens can be only withdraw by owner and while paused but there is a limitation of 3 days

Please check if an OnlyOwner or similar restrictive modifier has been forgotten.

Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/FeeSharingSystem.sol	1	————	258	256	155	36	108	
	contracts/FeeSharingSetter.sol	1	————	190	186	114	20	123	  
	contracts/IRewardConvertor.sol	————	1	10	5	3	1	3	————
	contracts/TradingRewardsDistributor.sol	1	————	159	151	67	54	57	
 	Totals	3	1	617	598	339	111	291	  

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Audit Results

AUDIT PASSED

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

Issue	File	Type	Line	Description
#1	FeeShar ingSyst em	A floating pragma is set	2	The current pragma Solidity directive is „^0.8.0“.
#2	FeeShar ingSett er	A floating pragma is set	2	The current pragma Solidity directive is „^0.8.0“.
#3	Trading Reward sDistrib utor	A floating pragma is set	2	The current pragma Solidity directive is „^0.8.0“.

Informational issues

Issue	File	Type	Line	Description
#1	FeeShar ingSyst em	State variables that could be declared constant	29	Add the `constant` attributes to state variables that never change

#2	FeeSharingSystem	Functions that are not used	185	Remove unused functions
#3	FeeSharingSystem	Wrong comment	128	Require statement error message should be changed or the condition to match statement with error message
#4	FeeSharingSystem	Unused state variable	29	Remove unused state variables

Commented Code exist

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

File	Line	Comment
FeeSharingSetter	93	// uint256 reward = rewardToken.balanceOf(address(this));
	99	// rewardToken.safeTransfer(address(feeSharingSystem), reward);
	113	// require(token != address(rewardToken), "Convert: Cannot be reward token");
FeeSharingSystem	93	// rewardToken.safeTransfer(msg.sender, pendingRewards);
	117-118	// rewardToken.safeTransfer(msg.sender, pendingRewards); // address payable receiver = payable(msg.sender);
	236	// rewardToken.safeTransfer(msg.sender, pendingRewards);

Recommendation

Remove the commented code, or address them properly.

Audit Comments

11. March 2022:

- [Read whole report for more information](#)

SWC Attacks

ID	Title	Relationships	Status
SW C-1 36	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-1 35	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-1 34	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-1 33	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-1 32	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-1 31	Presence of unused variables	CWE-1164: Irrelevant Code	NOT PASSED
SW C-1 30	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-1 29	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-1 28	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-1 27	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-1 25	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-1 24	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-1 23	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-1 22	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-1 21	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-1 20	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SW C-11 9	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-11 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SW C-11 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-1 09	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-1 08	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-1 07	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-1 06	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-1 05	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-1 04	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-1 03	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SW C-1 02	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SW C-1 01	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-1 00	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

The logo features the words "Solid Proofed" in a white, elegant script font. The word "Solid" is positioned above "Proofed". Behind the text is a faint, stylized shield emblem with a grid-like pattern, rendered in a darker shade of blue. The entire composition is set against a solid blue background.

Solid
Proofed

Blockchain Security | Smart Contract Audits | KYC

A small horizontal bar representing the German flag, with black, red, and gold stripes.

MADE IN GERMANY