



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

v1.0: 13. October, 2021

Audit

Security Assessment
01. November, 2021

For



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	10
Scope of Work	14
Inheritance Graph	14
Verify Claims	15
CallGraph	20
Source Units in Scope	21
Critical issues	22
High issues	22
Medium issues	22
Low issues	22
Informational issues	22
Audit Comments	23
SWC Attacks	24

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 security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	13. October 2021	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary
	01. November 2021	<ul style="list-style-type: none">• MasterChef added

Network

Binance Smart Chain (BEP20)

Website

<https://avnrich.shop/>

<https://farm.avnrichdefi.com/>

Telegram

https://t.me/AVNRich_Chat

Twitter

<https://twitter.com/avnrich>

Facebook

<http://fb.me/avnrich>

Github

<https://github.com/AvnrichDefi>

LinkedIn

<https://linkedin.com/company/avnrich-company>

Medium

<https://medium.com/@avnrich>

Instagram

<https://instagram.com/avnrich?igshid=tly8ahkyInc7>

Description

AVNRich was founded in 2019, AVNRich token is an innovative e-commerce and decentralized token based on the Binance Smart Chain Network that is used to reward users in a modern way by providing shopping, staking, farming, and IFO benefits to all users.

Project Engagement

During the 8th of October 2021, **AVNRich 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



Contract Link

v1.0

<https://bscscan.com/address/0xbf151f63d8d1287db5fc7a3bc104a9c38124cdeb#code>

MasterChef: <https://bscscan.com/address/0x413829Fa42aaf3De9b40Ee52597D85CCfADDe12C#code>

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:

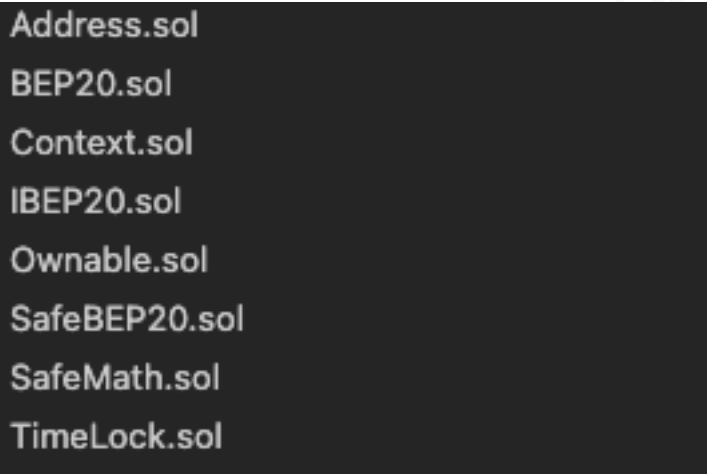
1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line 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)

V1.0

No packages Imported

MasterChef:



- Address.sol
- BEP20.sol
- Context.sol
- IBEP20.sol
- Ownable.sol
- SafeBEP20.sol
- SafeMath.sol
- TimeLock.sol

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

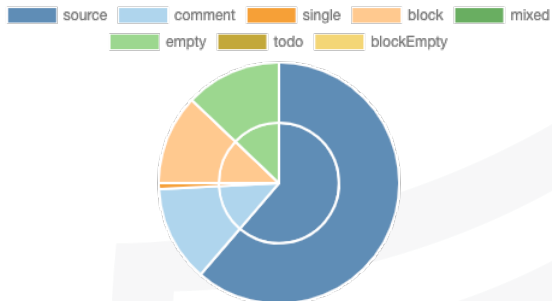
File Name	SHA-1 Hash
contracts/avnrich.sol	6518817d7a55d41dd72330e820ae4f7194ad137f

MasterChef

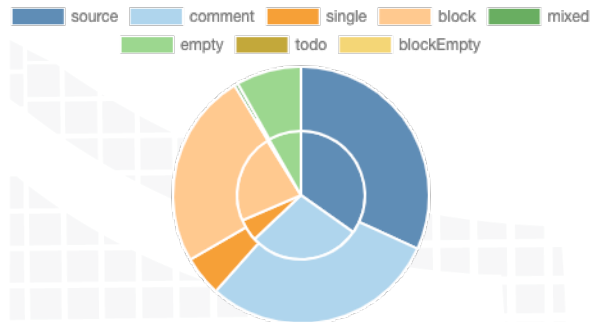
File Name	SHA-1 Hash
contracts/IBEP20.sol	889aa208892944008a537d4237688e7c82ec5673
contracts/BEP20.sol	9ff65ea16fed64f4f31d732badf546b7eafe04b6
contracts/Context.sol	a34cc2179b2da819d60afa9d711d0094d5a72799
contracts/MasterChef.sol	8e35f25f3288b421b0f8b8adf9f9894de7de68f1
contracts/SafeBEP20.sol	fd04404c0141a9d5807076b77bc7cb9c9b4a2422
contracts/TimeLock.sol	1c73eec94c713697bbe83de7fe987aab87abdda4
contracts/Address.sol	1aea000b5e51774d55f9dbeb58553f5d25caeb0b
contracts/SafeMath.sol	3906485abfad296a4f57098778ae0b75fec61892
contracts/Ownable.sol	a3c5d16bc16703a5502735531bf738c020df0f0d
contracts/Token.sol	812ab4874758b050beb0ddffc4c69ffcf9324d9

Metrics

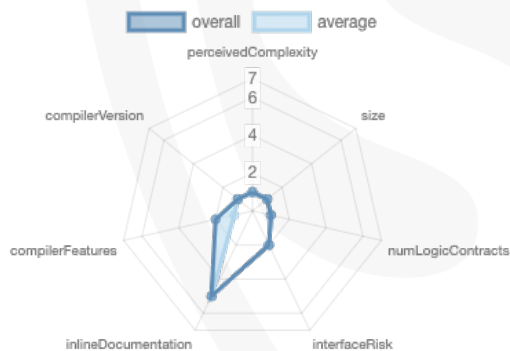
Source Lines v1.0



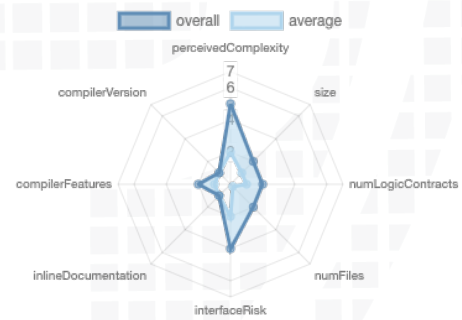
MasterChef



Risk Level v1.0



MasterChef



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	1	0	0	0
MasterChef	4	3	1	2

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	9	0
MasterChef	55	2

Version	External	Internal	Private	Pure	View
1.0	0	9	0	0	1
MasterChef	19	98	2	16	27

State Variables

Version	Total	Public
1.0	8	8
MasterChef	30	22

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	0.8.2			**** (0 asm blocks)	
MasterChef	>=0.6.4 >=0.4.0 >=0.6.0 <0.8.0 0.6.12 >=0.6.2 <0.8.0 >=0.6.1 2		yes	yes (3 asm blocks)	

Version	Transfers ETH	Low-Level Calls	Delegate Call	Uses Hash Functions	ECRecover	New/Create/Create2
---------	---------------	-----------------	---------------	---------------------	-----------	--------------------

1.0						
2.0	yes	yes	yes	yes	yes	



Scope of Work

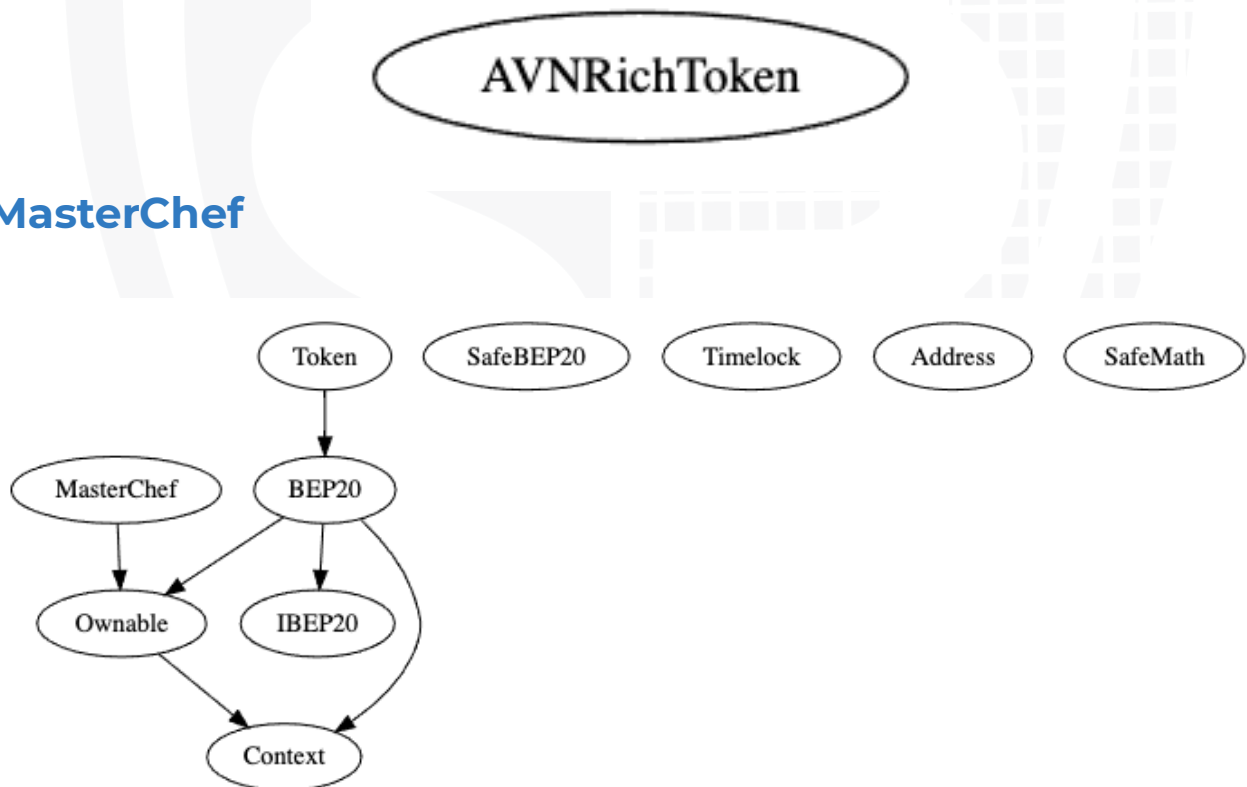
The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Correct implementation of Token standard
2. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Overall checkup (Smart Contract Security)

Inheritance Graph v1.0

MasterChef



Verify Claims

Correct implementation of Token standard

Tested	Verified
✓	✓

Function	Description	Exist	Tested	Verified
TotalSupply	provides information about the total token supply	✓	✓	✓
BalanceOf	provides account balance of the owner's account	✓	✓	✓
Transfer	executes transfers of a specified number of tokens to a specified address	✓	✓	✓
TransferFrom	executes transfers of a specified number of tokens from a specified address	✓	✓	✓
Approve	allow a spender to withdraw a set number of tokens from a specified account	✓	✓	✓
Allowance	returns a set number of tokens from a spender to the owner	✓	✓	✓

Optional implementations

Function	Description	Exist	Tested	Verified
renounceOwnership	Owner renounce ownership for more trust	✓	✓	✗

Deployer cannot mint any new tokens

Name	Exist	Tested	Verified	File
Deployer cannot mint	✓	✓	✗	Main
Comment	Line: -			

Max / Total Supply: 0

Comments:

v1.0

- OnlyIssuer can mint tokens
- OnlyOwner (modifier restricted) can set Issuer

1. approve	→
2. burn	→
3. burnFrom	→
4. mint	→
5. setIssuerRights	→
6. transfer	→
7. transferFrom	→
8. transferOwnership	→

MasterChef

1. add	→
2. deposit	→
3. dev	→
4. emergencyWithdraw	→
5. massUpdatePools	→
6. renounceOwnership	→
7. set	→
8. setFeeAddress	→
9. transferOwnership	→
10. updateEmissionRate	→
11. updatePool	→
12. withdraw	→

Deployer cannot burn or lock user funds

Name	Exist	Tested	Verified
Deployer cannot lock	✓	✓	✓
Deployer cannot burn	✓	✓	✗

v1.0

1. approve	→
2. burn	→
3. burnFrom	→
4. mint	→
5. setIssuerRights	→
6. transfer	→
7. transferFrom	→
8. transferOwnership	→

MasterChef

1. add	→
2. deposit	→
3. dev	→
4. emergencyWithdraw	→
5. massUpdatePools	→
6. renounceOwnership	→
7. set	→
8. setFeeAddress	→
9. transferOwnership	→
10. updateEmissionRate	→
11. updatePool	→
12. withdraw	→

Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	✓	✓	✓

v1.0

1. approve	→
2. burn	→
3. burnFrom	→
4. mint	→
5. setIssuerRights	→
6. transfer	→
7. transferFrom	→
8. transferOwnership	→

MasterChef

1. add	→
2. deposit	→
3. dev	→
4. emergencyWithdraw	→
5. massUpdatePools	→
6. renounceOwnership	→
7. set	→
8. setFeeAddress	→
9. transferOwnership	→
10. updateEmissionRate	→
11. updatePool	→
12. withdraw	→

Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

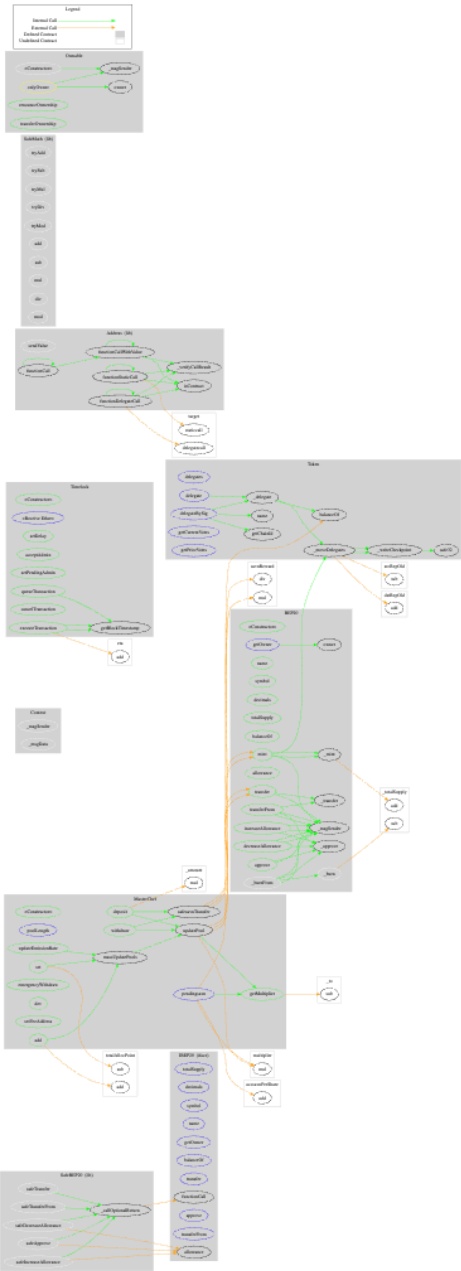
Legend

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

CallGraph V1.0





MasterChef





















Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/avnrich.sol	1	————	108	108	76	16	49	————
	Totals	1	————	108	108	76	16	49	————

MasterChef

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/IBEP20.sol	————	1	94	23	17	66	21	————
	contracts/BEP20.sol	1	————	298	298	98	170	91	————
	contracts/Context.sol	1	————	24	24	10	12	1	
	contracts/MasterChef.sol	1	————	246	246	179	50	137	
	contracts/SafeBEP20.sol	1	————	75	74	33	32	25	————
	contracts/TimeLock.sol	1	————	134	134	85	16	76	
	contracts/Address.sol	1	————	189	169	78	113	47	
	contracts/SafeMath.sol	1	————	214	214	61	139	16	
	contracts/Ownable.sol	1	————	68	68	27	33	24	————
	contracts/Token.sol	1	————	238	208	129	47	79	
	Totals	9	1	1580	1458	717	678	517	

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 found -

High issues

- no high issues found -

Medium issues

- no medium issues found -

Low issues

V1.0

- no low issues found -

V2.0

Version	Issue	File	Type	Line	Description
MasterChef	#1	MasterChef	Missing Zero Address Validation	75, 76, 231, 236	Check that the address is not zero
MasterChef	#2	Timelock	Missing Zero Address Validation	41, 103, 70	Check that the address is not zero

Informational issues

Version	Issue	File	Type	Line	Description
1.0	#1	Main	State variables that could be declared constant (constable-states)	24, 22, 23	Add the `constant` attributes to state variables that never change

Audit Comments

13. October 2021:

- There is still an owner (Owner still has not renounced ownership)
- OnlyIssuer can mint tokens
- OnlyOwner (modifier restricted) can set Issuer

MasterChef: 01. November 2021:

- There is still an owner (Owner still has not renounced ownership)
- On every updatePool call the dev address get 10 percent of savnReward

```
uint256 savnReward = multiplier.mul(savnPerBlock).mul(pool.allocPoint).div(totalAllocPoint);
savn.mint(devaddr, savnReward.div(10));
savn.mint(address(this), savnReward);
```

- devAddress/feeAddress can only set by the previous dev/fee address

SWC Attacks

ID	Title	Relationships	Status
SW C-13 6	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-13 5	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-13 4	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-13 3	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-13 2	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-13 1	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-13 0	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-12 9	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-12 8	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-12 7	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-12 5	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-12 4	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-12 3	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-12 2	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-12 1	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-12 0	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-111	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-10 9	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-10 8	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-10 7	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-10 6	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-10 5	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-10 4	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-10 3	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	PASSED
SW C-10 2	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SW C-10 1	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-10 0	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

The logo features the word "SolidProofed" in a white, handwritten-style script. The "P" is particularly large and stylized, with a long horizontal stroke that extends to the left. The background is a solid blue color with a faint, large shield emblem. The shield has a grid-like pattern on its right side and a solid blue area on its left side.

SolidProofed

Blockchain Security | Smart Contract Audits | KYC

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

MADE IN GERMANY