SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

BOM

Audit

Security Assessment

31. May, 2022

For

BOM

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	31. May 2022	• Layout project • Automated- /Manual-Security Testing • Summary

Network
Polygon MATIC

Website
https://bomcoin.com/

Telegram
https://t.me/bomcoinofficial

Twitter
https://twitter.com/bom_coin

Facebook
https://facebook.com/bomcoinofficial

Instagram
https://www.instagram.com/bom.coin

Medium
https://bomcoin.medium.com/

Discord
https://discord.gg/xrtEEMmZfU

Youtube
https://www.youtube.com/c/BomCoinOfficial

Description
TBA

Project Engagement
During the 30th of May 2022, **BOM 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
- Github
  - https://github.com/BOM-Token/BomSmartContract/commit/5442b25c6228a5cb78d20a2afa3f73e6df1e40a8
  - Commit: 5442b25c6228a5cb78d20a2afa3f73e6df1e40a8

  - https://github.com/BOM-Token/BomSmartContract/commit/c49b6f29b608af8fd240630435398a90dc186266
  - Commit: c49b6f29b608af8fd240630435398a90dc186266

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 aspossible.
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/access/Ownable.sol	2
@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol	1
@openzeppelin/contracts/utils/Strings.sol	1
@openzeppelin/contracts/utils/math/SafeMath.sol	2

Tested Contract Files

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

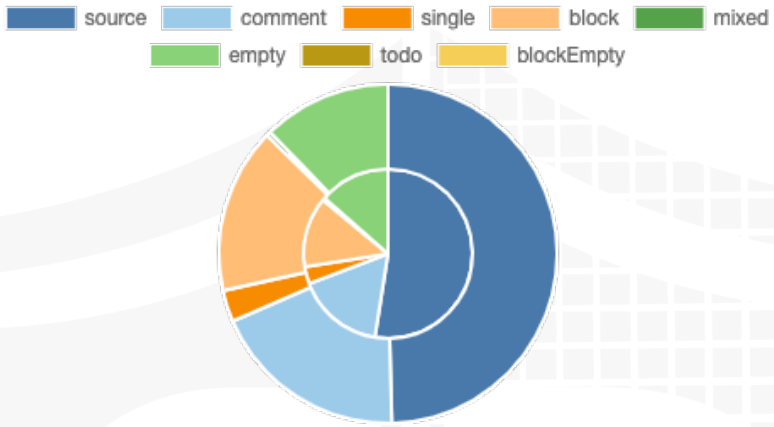
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

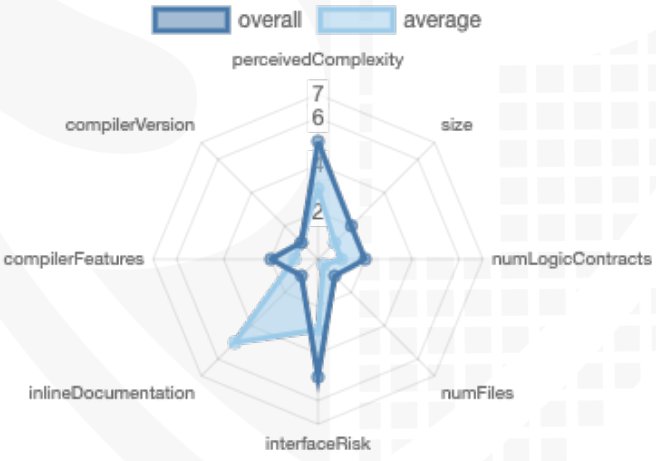
File Name	SHA-1 Hash
contracts/BOMNFT.sol	39d6ae4f455cb2bcb05a610ded26783556b92c7c
contracts/BOMToken.sol	628de59531807d049a15d7f038d8fa4838355581
contracts/IERC20.sol	5cafd4d53f797d5c18267a2c3deb3d5e68f77bc6

Metrics

Source Lines
v1.0



Risk Level
v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	5	0	4	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.

Version	Public	Payable
1.0	79	3

Version	External	Internal	Private	Pure	View
1.0	52	57	0	0	33

State Variables

Version	Total	Public
1.0	46	41

Capabilities

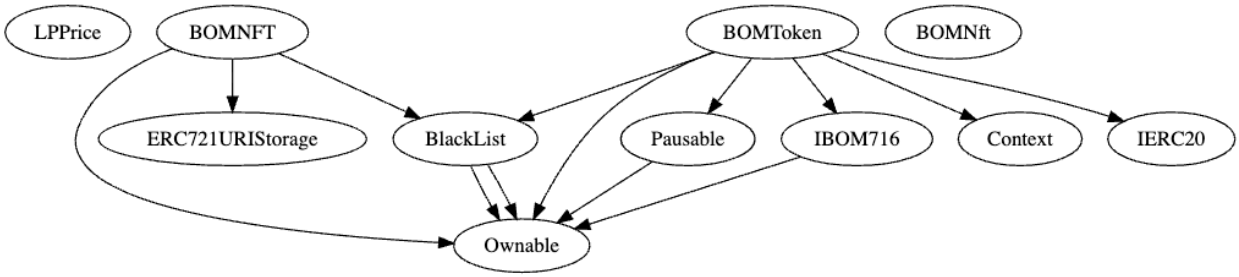
Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	`^0.8.1` `^0.8.7`		`yes`		

Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	EC Recover	New/Create/Create2

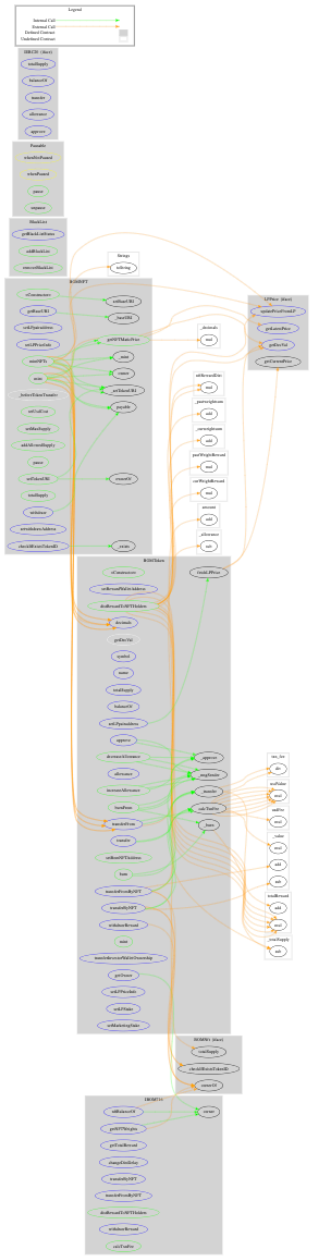
1.0	yes					

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. 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)

Correct implementation of Token standard

ERC20				
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	✓	✓	✓

ERC721				
Function	**Description**	**Exist**	**Tested**	**Verified**
BalanceOf	Count all NFTs assigned to an owner	✓	✓	✓
OwnerOf	Find the owner of an NFT	✓	✓	✓
SafeTransferFrom	Transfers the ownership of an NFT from one address to another address	✓	✓	✓
SafeTransferFrom	See above - Difference is that this function has an extra data parameter	✓	✓	✓
TransferFrom	Transfer ownership of an NFT	✓	✓	✓
Approve	Change or reaffirm the approved address for an NFT	✓	✓	✓
SetApprovalForAll	Enable or disable approval for a third party ("operator") to manage all of `msg.sender`'s assets	✓	✓	✓
GetApproved	Get the approved address for a single NFT	✓	✓	✓
IsApprovedForAll	Query if an address is an authorized operator for another address	✓	✓	✓
SupportsInterface	Query if a contract implements an interface	✓	✓	✓
Name	Provides information about the name	✓	✓	✓
Symbol	Provides information about the symbol	✓	✓	✓
TokenURI	Provides information about the TokenUri	✓	✓	✓

Write functions of contract v1.0

1. addBlackList
2. approve
3. burn
4. burnFrom
5. changeDistDelay
6. decreaseAllowance
7. distRewardToNFTHolders
8. fetchLPPrice
9. increaseAllowance
10. mint
11. pause
12. removeBlackList
13. renounceOwnership
14. setBornNFTAddress
15. setLPPriceInfo
16. setLPStake
17. setLPpairaddress
18. setMarketingStake
19. setRewardWalletAddress
20. transfer
21. transferByNFT
22. transferFrom
23. transferFromByNFT
24. transferInvestorWalletOwnership
25. transferOwnership
26. unpause
27. withdrawReward

1. addAllowedSupply
2. addBlackList
3. approve
4. mint
5. mintNFTs
6. pause
7. removeBlackList
8. renounceOwnership
9. safeTransferFrom
10. safeTransferFrom
11. setApprovalForAll
12. setBaseURI
13. setLPPriceInfo
14. setLPpairaddress
15. setMaxSupply
16. setTokenURI
17. setUsdCost
18. setwithdrawAddress
19. transferFrom
20. transferOwnership
21. withdraw

Deployer cannot mint any new tokens

Name	Exist	Tested	Status
Deployer cannot mint	✓	✓	✗

Comments:

v1.0

- Anyone can mint new nfts
- Owner can mint new tokens in BOMToken to him-/herself

Deployer cannot burn or lock user funds

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

Comments:

v1.0

- Owner can lock user funds by
  - blacklisting addresses
  - Pause contract
- Tokens
  - can be burned by msg.sender

Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	✓	✓	✗

Comments:

v1.0

- Owner can pause contract

Overall checkup (Smart Contract Security)

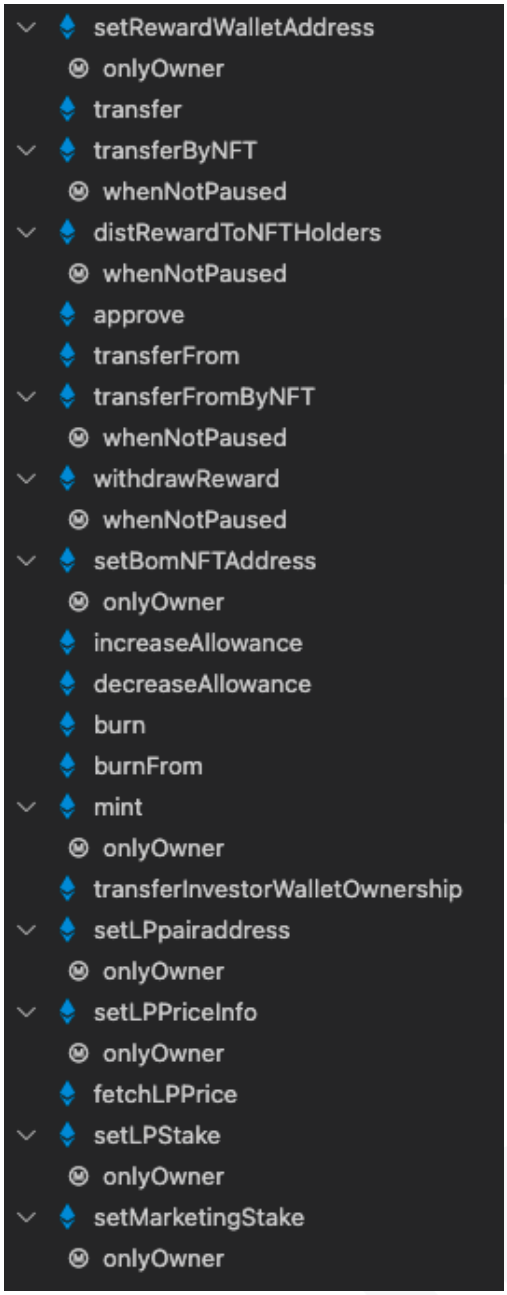
Tested	Verified
✓	✓

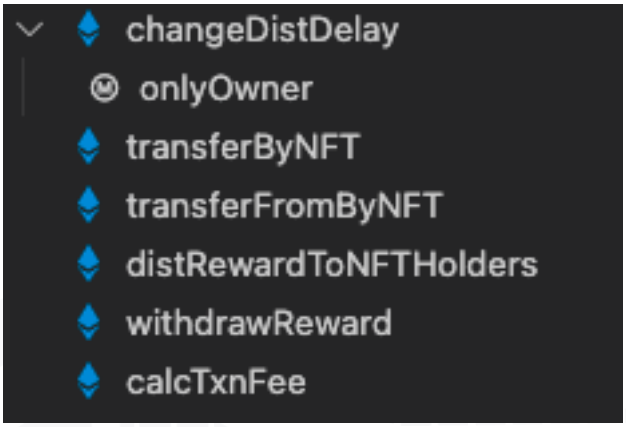
Legend

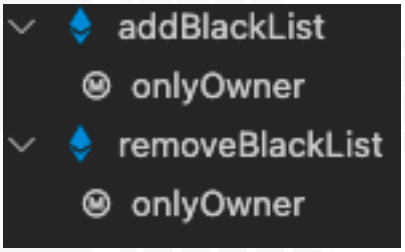
Attribute	Symbol
Verfified / Checked	✓
Partly Verified	⚑
Unverified / Not checked	✗
Not available	-

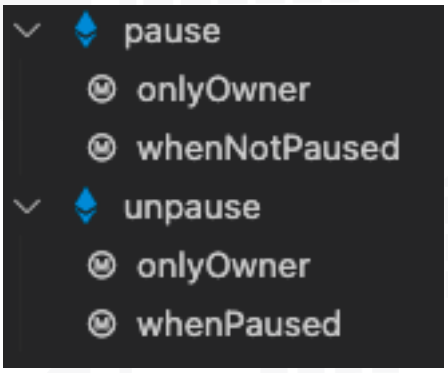
Modifiers and public functions

v1.0









Comments

- *Deployer can set following state variables without any limitations*
  - BOMToken
    - Can only be decreased
      - marketingStake
      - lpStake
  - BOMNFT
    - usdCost
    - maxSupply
    - allowedSupply

- *Deployer can enable/disable following state variables*
  - BOMNFT
    - paused
    - isBlackListed

- *Deployer can set following addresses*
  - BOMToken
    - lpinfo
    - lpAddress
    - bomnft
    - lpMasterAddress
    - marketingWallet
    - teamWallet
    - techWallet

  - BOMNFT
    - lpAddress
    - lpinfo
    - baseURI

- *Existing Modifiers*
  - BOMToken
    - whenNotPaused
    - whenPaused

- Owner can withdraw contract balance to withdrawAddress
  - Withdraw address can be set to any address

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/BOMNFT.sol	2	1	219	213	165	12	177	💰💠
📝🔍🎨	contracts/BOMToken.sol	4	2	715	640	376	169	366	————
🔍	contracts/IERC20.sol	————	1	81	22	17	57	15	————
📝🔍🎨	**Totals**	**6**	**4**	**1015**	**875**	**558**	**238**	**558**	💰💠

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

Issue	File	Type	Line	Description
#1	BOMNFT	lpAddress must be restricted to owner	99	Everybody can set LP address from the contract with setLPpairaddress function

Medium issues

No medium issues

Low issues

Issue	File	Type	Line	Description
#1	BOMToken	A floating pragma is set	2	The current pragma Solidity directive is „“^0.8.7””.
#2	BOMNFT	A floating pragma is set	5	The current pragma Solidity directive is „“^0.8.1””.
#3	BOMToken	Missing Zero Address Validation (missing-zero-check)	174, 691, 671	Check that the address is not zero
#4	BOMToken	Local variables shadowing	651, 380	Rename the local variables that shadow another component
#5	BOMToken	Missing Events Arithmetic	709, 711, 121	Emit an event for critical parameter changes

Informational issues

Issue	File	Type	Line	Description
#1	BOMToken	Functions that are not used	222	Remove unused functions
#2	BOMNFT	Misspelling	See description	Change following words: - Auther L13 Make sure to change it everywhere else as well.
#3	BOMNFT	Error message is missing	114, 115, 126, 142, 143, 154, 172, 184, 198, 207, 212	Provide an error message for require statement
#4	BOMToken	Error message is missing	28, 36, 197-200, 273, 289, 290, 314, 422, 448, 449, 655, 656, 673, 678, 683	Provide an error message for require statement
#5	All	NatSpec documentation missing	-	If you started to comment your code, also comment all other functions, variables etc.
#6	BOMToken	Variable should not be 0	184	Prevent state variable to be 0 because you are dividing with it. Otherwise this will cause an error. If this variable is set to 0 the Matic price will also be 0 in L108, BOMNFT
#7	BOMToken	Zero variable	709	If variable is set to 0 it cannot be set upwards again
#8	BOMToken	Visibility order	43, 51	Visibility modifiers like “external, public, etc.” come first and after it the others.
#9	BOMToken	Unused event	76	Remove or emit event

#10	BOMNFT	Duplicate code	139, 113	We recommend you to create a function to use the same code because of repetition. Pay attention to the changes while comparing.

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information https://docs.soliditylang.org/en/v0.5.10/natspec-format.html) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

31. May 2022:

- LPPrice contract was not provided to solidproof
    - Do your own research here
- Read whole report and modifiers section for more information

SWC Attacks

ID	Title	Relationships	Status
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY