



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Audit

Security Assessment
07. January, 2022

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	11
Scope of Work	13
Inheritance Graph	13
Verify Claims	14
Modifiers	21
CallGraph	23
Source Units in Scope	24
Critical issues	25
High issues	25
Medium issues	25
Low issues	25
Informational issues	25
Audit Comments	26
SWC Attacks	27

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	06. January 2022	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Binance Smart Chain (BEP20)

Website

<https://Oxpad.io/>

Telegram

<https://t.me/zeroXpad>

Twitter

<https://twitter.com/Oxpad>

Github

<https://github.com/Oxpad>

Medium

<https://medium.com/@0xPAD>

Description

Multichain launchpad and Decentralized Incubator Protocol.
Decentralizing seed funding and giving everyone early access to innovative projects

Project Engagement

During the 3rd of January 2022, **OxPad 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

- Staking
 - <https://bscscan.com/address/0x9CC09f444887Aaf1CC10115D15c232824De9Cd21#code>
- Sale
 - <https://bscscan.com/address/0x083AFDD00ab4aDD97e7f70f0d7FBdeAb8f6D4b7E#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)

Imported packages:

Sale

```
Context  
Ownable  
IERC20  
ReentrancyGuard  
Utils
```

Staking

```
Context  
Ownable  
IERC20  
IERC20_LP
```


Tested Contract Files

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

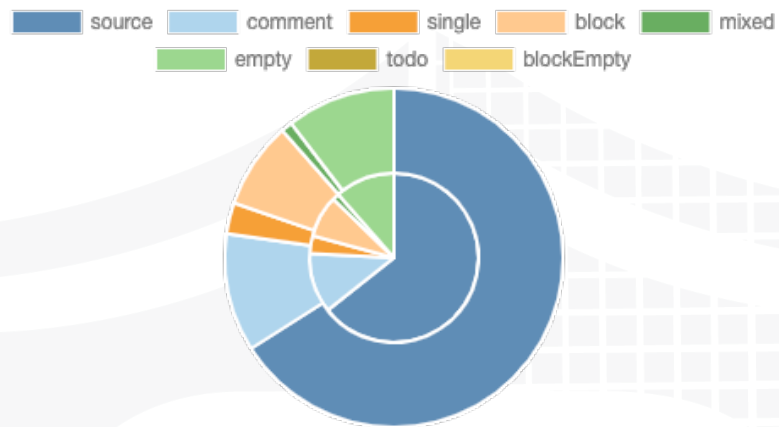
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

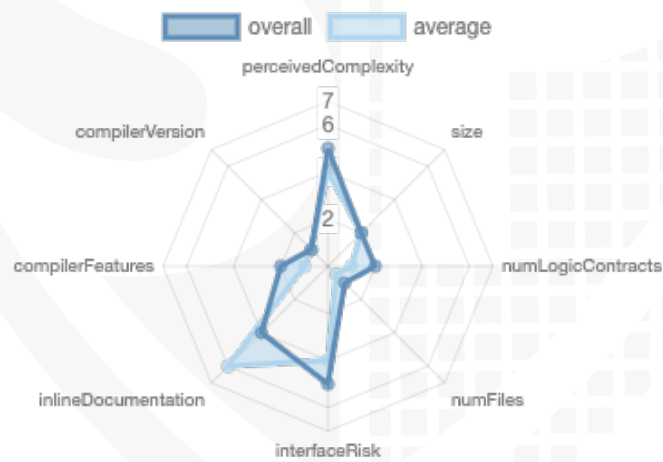
File Name	SHA-1 Hash
contracts/staking.sol	5f5d1601b7175ffb70a7b100381b5c740443c52a
contracts/sale.sol	887bff193d9b05ac985f466a83436fbaa2ab818d

Metrics

Source Lines v1.0



Risk Level v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	3	0	3	5

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	107	1

Version	External	Internal	Private	Pure	View
1.0	99	75	2	0	58

State Variables

Version	Total	Public
1.0	39	0

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	0.8.0		yes	**** (0 asm blocks)	

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

1.0	yes					
-----	-----	--	--	--	--	--



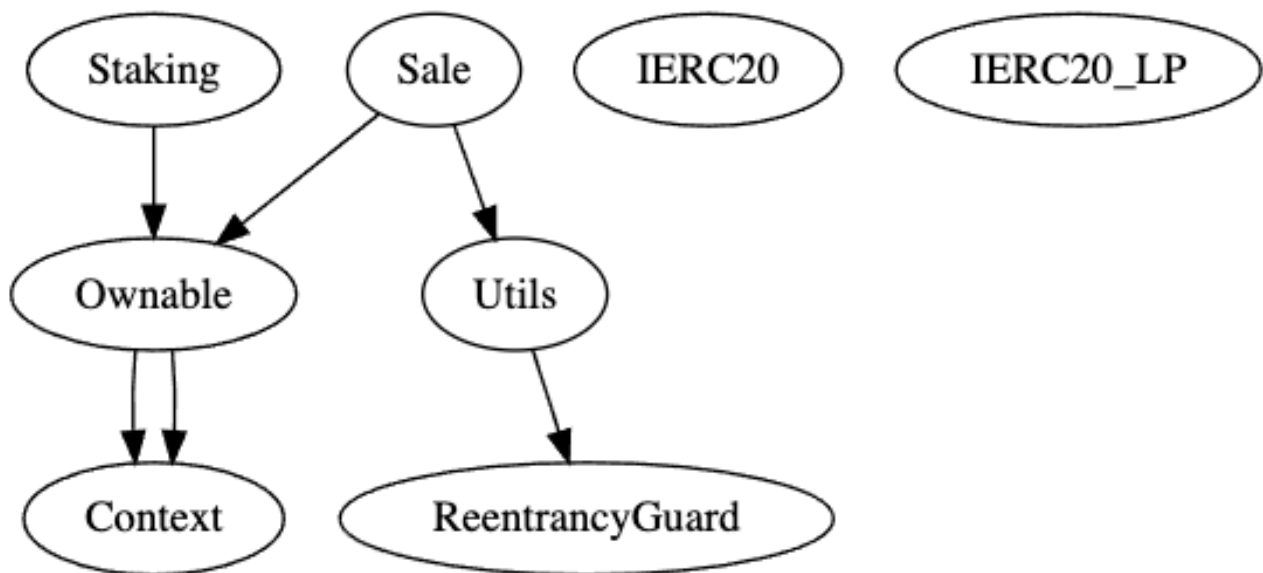
Scope of Work

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



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	✓	✓	✓

Write functions of contract Sale

1. addPaymentProfile

2. addToManagers

3. addToWhitelist

4. addToWhitelistMultiple

5. adminWithdraw

6. purchase

7. removeFromManagers

8. removeFromWhitelist

9. removeFromWhitelistMultiple

10. renounceOwnership

11. setAssetsReceiverAddress

12. setBatchLimit

13. setEndTime

14. setMaxTokenAmount

15. setPaymentProfileCurrency

16. setPaymentProfileName

17. setPaymentProfileStatus

18. setPaymentProfileUsdRate

19. setPaymentProfileWeight

20. setSaleOver

21. setSalePoolSize

22. setStartTime

23. setTokenAddress

24. setTokenUsdRate

25. setWhitelistEndTime

26. setWhitelistMode

27. setWithdrawalAvailable

28. transferOwnership

29. withdrawAllTokens

30. withdrawTokens

Staking

1. adminAddDepositProfile

2. adminSetDepositApr

3. adminSetDepositCurrency

4. adminSetDepositLink

5. adminSetDepositLockTime

6. adminSetDepositName

7. adminSetDepositRate

8. adminSetDepositStatus

9. adminSetDepositTax

10. adminSetDepositWeight

11. adminSetOxpadContract

12. adminSetSafeMode

13. adminWithdrawOxpad

14. adminWithdrawToken

15. reStake

16. renounceOwnership

17. stake

18. transferOwnership

19. unStake

20. withdrawYield

Deployer cannot mint any new tokens

Name	Exist	Tested	Verified
Deployer cannot mint	—	—	—

Max / Total Supply: 13.000.000.000.000.000.000.000.000

Comment

v1.0

- Deployer can set pool size



Deployer cannot burn or lock user funds

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

Comments:

v1.0

- Deployer can lock user funds
 - By setting whitelistMode to true and address not included into whitelist mapping
 - Deactivate active state from payment profiles to false
 - By setting _startTime higher than block.timestamp
 - By setting maxTokenAmount to 1
 - By setting _withdrawalAvailable to false

Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	—	—	—



Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

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

Modifiers

Sale

[purchaseAllowed](#)

`purchase` 💰

[onlyManager](#)

```
addPaymentProfile
setPaymentProfileUsdRate
setPaymentProfileWeight
setPaymentProfileName
setPaymentProfileCurrency
setPaymentProfileStatus
setBatchLimit
setTokenUsdRate
setSalePoolSize
addToWhitelist
addToWhitelistMultiple
removeFromWhitelist
removeFromWhitelistMultiple
setMaxTokenAmount
setStartTime
setWhitelistEndTime
setEndTime
setWithdrawalAvailable
setTokenAddress
setSaleOver
setWhitelistMode
```

[onlyOwner](#)

```
setAssetsReceiverAddress
addToManagers
removeFromManagers
adminWithdraw
```

Comments

- Deployer can set following state variables without any limitations
 - States of paymentProfiles
 - _batchLimit
 - _tokenUsdRate
 - variable must be at least 1
 - salePoolSize
 - Variable must be at least _totalPaidTokenAmount
 - _maxTokenAmount
 - _whitelistEndTime
 - _endTime
- Deployer can enable/disable following state variables
 - _whitelist
 - _saleOver
 - _withdrawalAvailable
 - _managers

Staking

```
adminAddDepositProfile
adminSetDepositApr
adminSetDepositTax
adminSetDepositRate
adminSetDepositWeight
adminSetDepositLockTime
adminSetDepositName
adminSetDepositCurrency
adminSetDepositLink
adminSetDepositStatus
adminWithdrawToken
adminWithdrawOxpad
adminSetOxpadContract
adminSetSafeMode
```







Comments

- Deployer can set following state variables without any limitations
 - States of depositProfiles
- Deployer can enable/disable following state variables
 - _safeMode



Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/staking.sol	3	2	675	578	447	70	247	
	contracts/sale.sol	5	1	701	634	460	109	286	
	Totals	8	3	1376	1212	907	179	533	

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

Issue	File	Type	Line	Description
#1	Staking, Sale	Contract doesn't import npm packages from source (like OpenZeppelin etc.)	-	We recommend to import all packages from npm directly without flatten the contract. Functions could be modified or can be susceptible to vulnerabilities
#2	Sale	State variable visibility is not set	241	It is best practice to set the visibility of state variables explicitly

Informational issues

Issue	File	Type	Line	Description
#1	Sale	Functions that are not used	23	Remove unused functions
#2	Staking	Format source code	-	Format source code of sol file for better readability
#3	Staking	Comments	-	Comment everything else if you started to comment something
#4	Sale	Require statements messages	-	Start error messages with an uppercase word

Audit Comments

06. January 2022:

- Deployer can lock user funds
- Read whole report for more information



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	NOT 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 words "SolidProof" in a white, handwritten-style script. The "P" is 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.

SolidProof

Blockchain Security | Smart Contract Audits | KYC

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

MADE IN GERMANY