



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

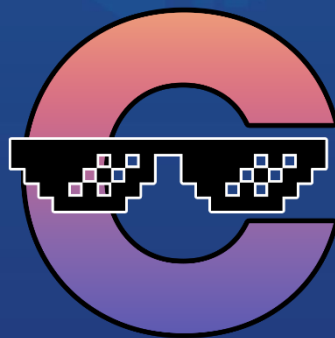
Culture FI

Audit

Security Assessment

30.May,2023

For



SolidProof.io



[@solidproof_io](https://t.me/solidproof_io)

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	21
Source Units in Scope	22
Critical issues	23
High issues	23
Medium issues	23
Low issues	23
Informational issues	23
Audit Comments	24
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	30.May,2023	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network
Ethereum Network (ETH)

Website
<https://culturefi.io>

Twitter
<https://twitter.com/Thecultureindex>

Telegram
<https://t.me/culturefi>



Description

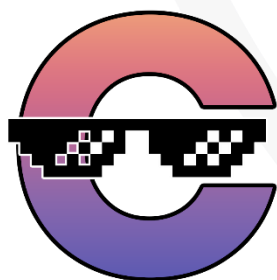
In the ETH ecosystem, When you connect to the **CULTURE** platform, you'll be greeted with an intuitive and user-friendly dashboard that serves as your gateway to the exciting world of meme coins. The dashboard provides a comprehensive overview of your portfolio, market trends, and the latest updates in the meme coin space. It's designed to give you a seamless and informative experience as you navigate through various features and functionalities.

You can easily track the current value of your tokens, view your staking progress, and monitor the overall performance of your investments. The overview section serves as a central hub to keep you updated on your \$CULTURE journey.

Project Engagement

During the 30th of May 2023, **Culture** team engaged Solidproof.io to audit the smart contracts that they created. The engagement was technical in nature and focused on identifying the security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Links

v1.0

<https://etherscan.io/token/0xC2892325A2C6a817e9A1F4dD4a14B3F553bdA572>

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 analyzing 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:



```
> IERC20  
> Context  
> Ownable  
> SafeMath  
> BaseToken  
> StandardToken
```


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.

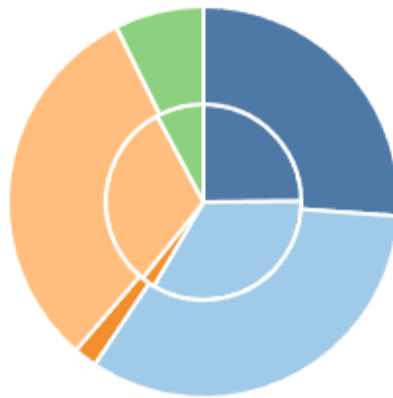
v1.0

File Name	SHA-1 Hash
contracts/StandardToken.sol	139d7c567b73f15bc8939f98a02170cd313f0321

Metrics

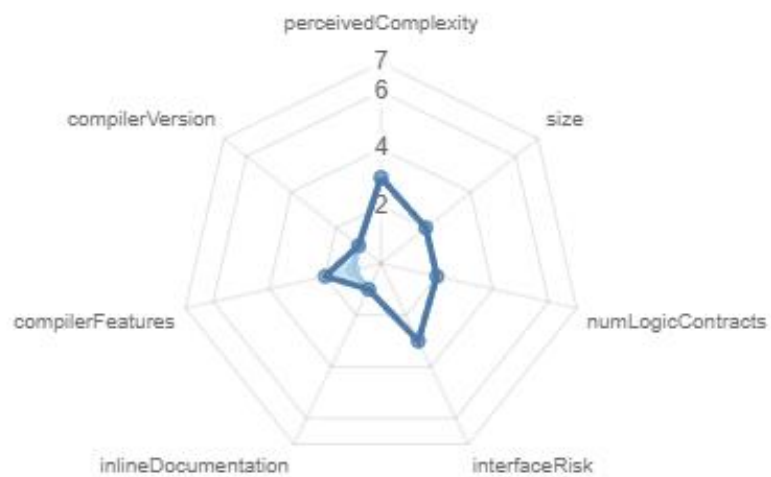
Source Lines v1.0

source comment single block mixed
empty todo blockEmpty



Risk Level v1.0

overall average



Capabilities

Components

 Contracts	 Libraries	 Interfaces	 Abstract
1	1	1	3

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
20	1







External	Internal	Private	Pure	View
6	39	1	13	12


StateVariables

Total	 Public
8	1

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
=0.8.4		yes		

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

 TryCatch	Σ Unchecked
	yes

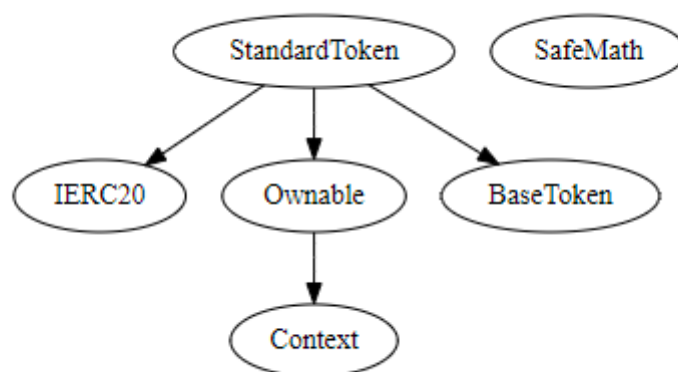
Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	0.8.4		Yes		

Version	Transfers ETH	Low-Level Calls	Delegate Call	Uses Hash Functions	EC Recover	New/Create/Create2
1.0	Yes					

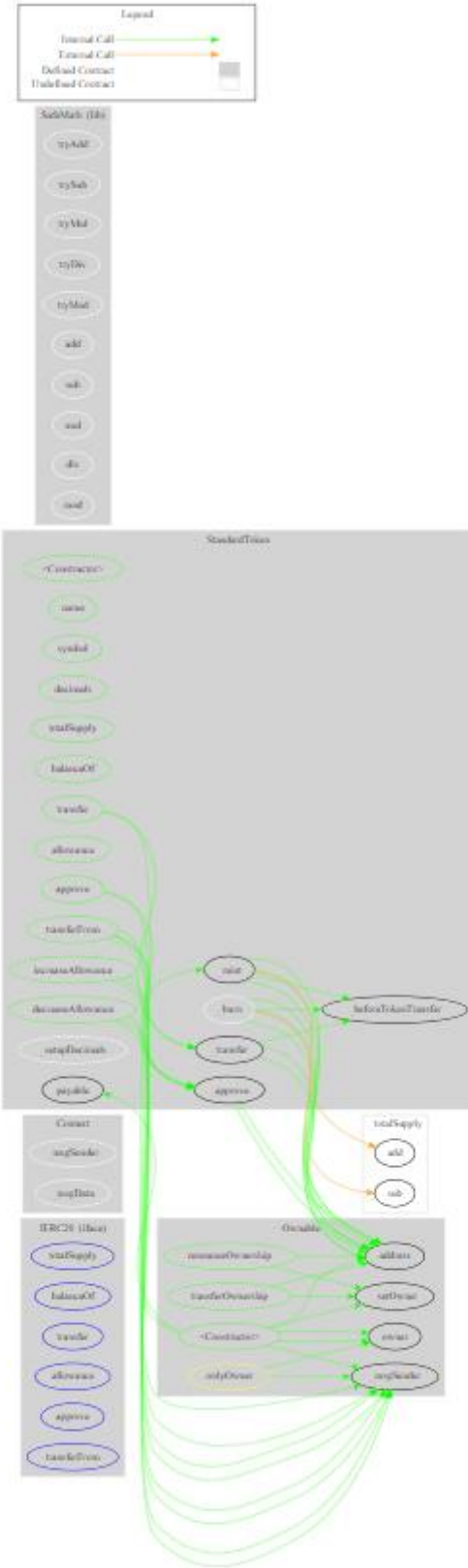
Inheritance Graph

v1.0



Call Graph

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



Is contract an upgradeable

Name	
Is contract an upgradeable?	No



Correct implementation of Token standard

ERC20				
Function	Description	Exist	Tested	Verified
totalSupply	Provides information about the total token supply	Yes	Yes	Yes
balanceOf	Provides account balance of the owner's account	Yes	Yes	Yes
transfer	Executes transfers of a specified number of tokens to a specified address	Yes	Yes	Yes
transferFrom	Executes transfers of a specified number of tokens from a specified address	Yes	Yes	Yes
approve	Allow a spender to withdraw a set number of tokens from a specified account	Yes	Yes	Yes
allowance	Returns a set number of tokens from a spender to the owner	Yes	Yes	Yes

Deployer cannot mint any new tokens

Name	Exist	Tested	Status
Deployer cannot mint	N/A	N/A	N/A
Max / Total Supply	42000000000000000000 0000000000000000		



Deployer cannot burn or lock user funds

Name	Exist	Tested	Status
Deployer cannot lock	N/A	N/A	N/A
Deployer cannot burn	N/A	N/A	N/A



Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	N/A	N/A	N/A



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

- ◆ <Constructor> 🏠
- ◆ transfer
- ◆ approve
- ◆ transferFrom
- ◆ increaseAllowance
- ◆ decreaseAllowance





















Ownership Privileges:

N/A

Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
   	contracts/StandardToken.sol	5	1	799	686	257	398	140	    
   	Totals	5	1	799	686	257	398	140	    

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

No Low issues

Informational issues

Issue	File	Type	Line	Description
#1	StandardToken.sol	Unused function	-	If you don't need to use any function, you can remove it for ex- _setUpDecimals is not called anywhere in the main contract.
#2	StandardToken.sol	Latest Solidity Version	-	You can also use the latest solidity version to avoid any exceptions.

Audit Comments

Here, some of the functions are unused we recommend you remove the unused code, so it will also help you to reduce the gas fee.
There are no Ownership privileges in the contract.

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	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	Authoriza tion through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SWC-114	Transacti on Order Depende nce	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	Delegate call to Untruste d Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-111	Use of Deprecat ed Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SWC-109	Uninitializ ed Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

<u>SWC-107</u>	Reentrancy	<u>CWE-841: Improper Enforcement of Behavioral Workflow</u>	PASSED
<u>SWC-106</u>	Unprotected SELFDESTRUCT Instruction	<u>CWE-284: Improper Access Control</u>	PASSED
<u>SWC-105</u>	Unprotected Ether Withdrawal	<u>CWE-284: Improper Access Control</u>	PASSED
<u>SWC-104</u>	Unchecked Call Return Value	<u>CWE-252: Unchecked Return Value</u>	PASSED
<u>SWC-103</u>	Floating Pragma	<u>CWE-664: Improper Control of a Resource Through its Lifetime</u>	PASSED
<u>SWC-102</u>	Outdated Compiler Version	<u>CWE-937: Using Components with Known Vulnerabilities</u>	PASSED
<u>SWC-101</u>	Integer Overflow and Underflow	<u>CWE-682: Incorrect Calculation</u>	PASSED
<u>SWC-100</u>	Function Default Visibility	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED



[SolidProof_io](https://twitter.com/SolidProof_io)



[@solidproof_io](https://t.me/@solidproof_io)

Solid
Proofed

Blockchain Security | Smart Contract Audits | KYC


MADE IN GERMANY