SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Audit

Security Assessment

25. January, 2022

For

CULT.DAO

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 24
Critical issues 25
High issues 25
Medium issues 25
Low issues 25
Informational issues 26
Commented Code exist 27
Audit Comments 28
SWC Attacks 29

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	25. January 2022	• Layout project • Automated- /Manual-Security Testing • Summary

Network
Binance Smart Chain (BEP20)

Website
https://cultdao.io/

Telegram
https://t.me/cultdao

Twitter
https://twitter.com/wearecultdao

Medium
https://wearecultdao.medium.com/

Discord
https://discord.com/invite/hHDBvNnXqe

Reddit
http://reddit.com/r/cultdao/

Description

The purpose of CULT is to empower and fund those building and contributing towards our decentralized future. Our society is built to make it as difficult as possible to break away from societal, economic and other norms,

Project Engagement

During the 25th of January 2022, **CultDAO 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/cultdao-developer/cultdao
  - Commit: 003fc9119cd0fce1a56c3b53157d706c77800b5a

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-upgradeable/access/OwnableUpgradeable.sol	3
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	5
@openzeppelin/contracts-upgradeable/proxy/utils/UUPSUpgradeable.sol	5
@openzeppelin/contracts-upgradeable/security/PausableUpgradeable.sol	3
@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	2
@openzeppelin/contracts-upgradeable/token/ERC20/IERC20Upgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20VotesCompUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20VotesUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/draft-ERC20PermitUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/utils/SafeERC20Upgradeable.sol	1
@openzeppelin/contracts-upgradeable/utils/math/SafeMathUpgradeable.sol	4

Tested Contract Files

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

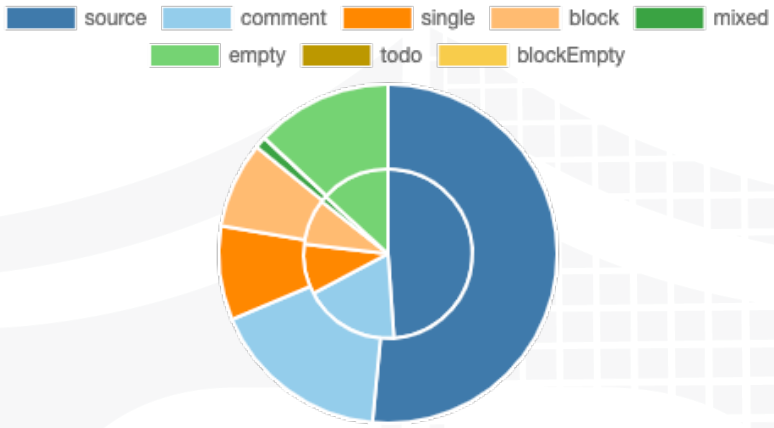
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

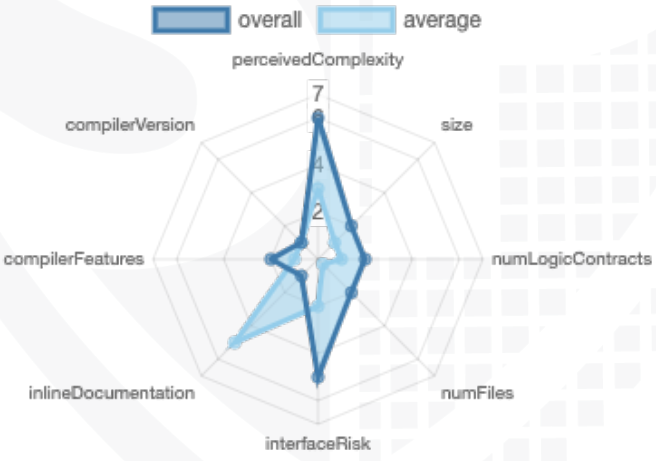
File Name	SHA-1 Hash
contracts/treasury.sol	f1a563489f19b6d44dd6206ed23389391649ecfc
contracts/dcult.sol	7f48779286bef63b631be4d46e4df82fbbdd2cc8
contracts/cult.sol	34bdad1e1cdc3737bce26970ceda92b6369e2f68
contracts/GovernorBravoInterfaces.sol	af29733fb1be18fad38c5f48efef618a4627153e
contracts/timelock.sol	a90b6764254751beac08ea4a4324c9f0d2884604
contracts/governance.sol	6e2ab39b2022697419b07d7883d772fe2e38d3f8

Metrics

Source Lines
v1.0



Risk Level
v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	9	0	7	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	73	5

Version	External	Internal	Private	Pure	View
1.0	49	82	2	7	21

State Variables

Version	Total	Public
1.0	60	59

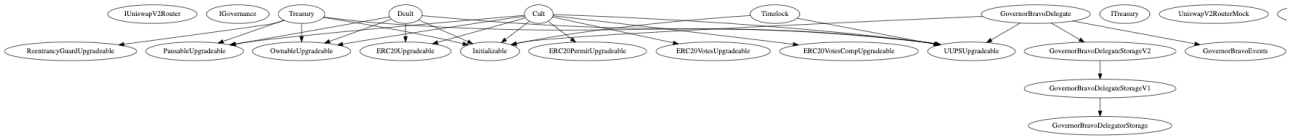
Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	`0.8.2` `^0.8.2`	`ABIEncoderV2`	`yes`	`yes` (1 asm blocks)	

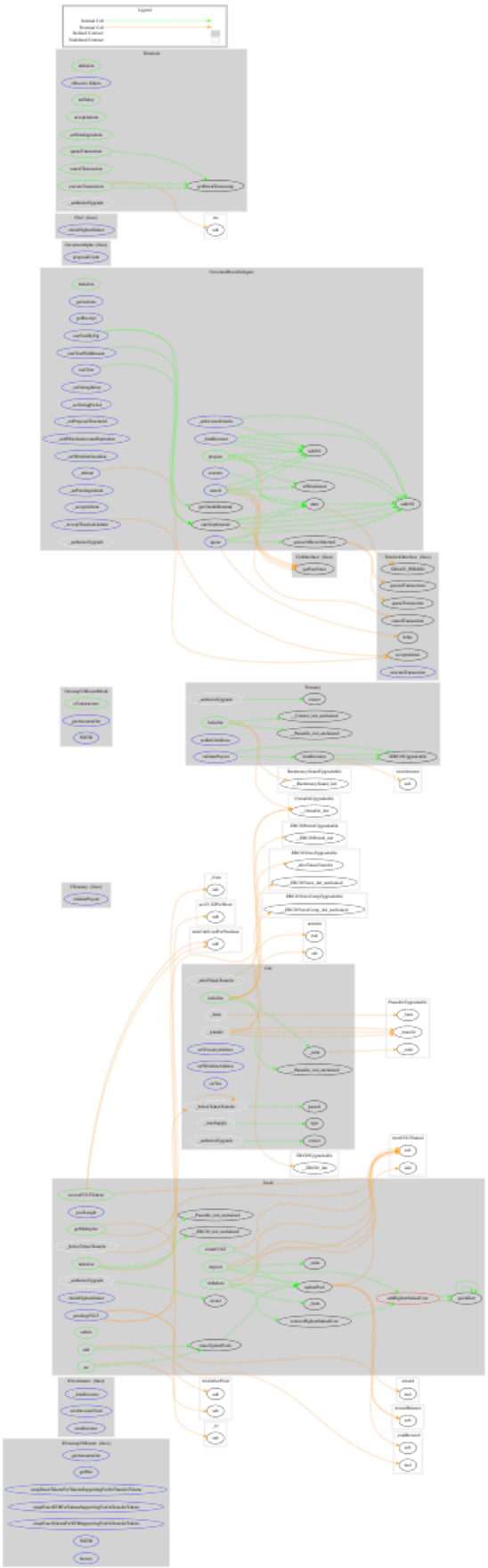
Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	ECRecover	New/Create/Create2
1.0	yes			yes	yes	

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).

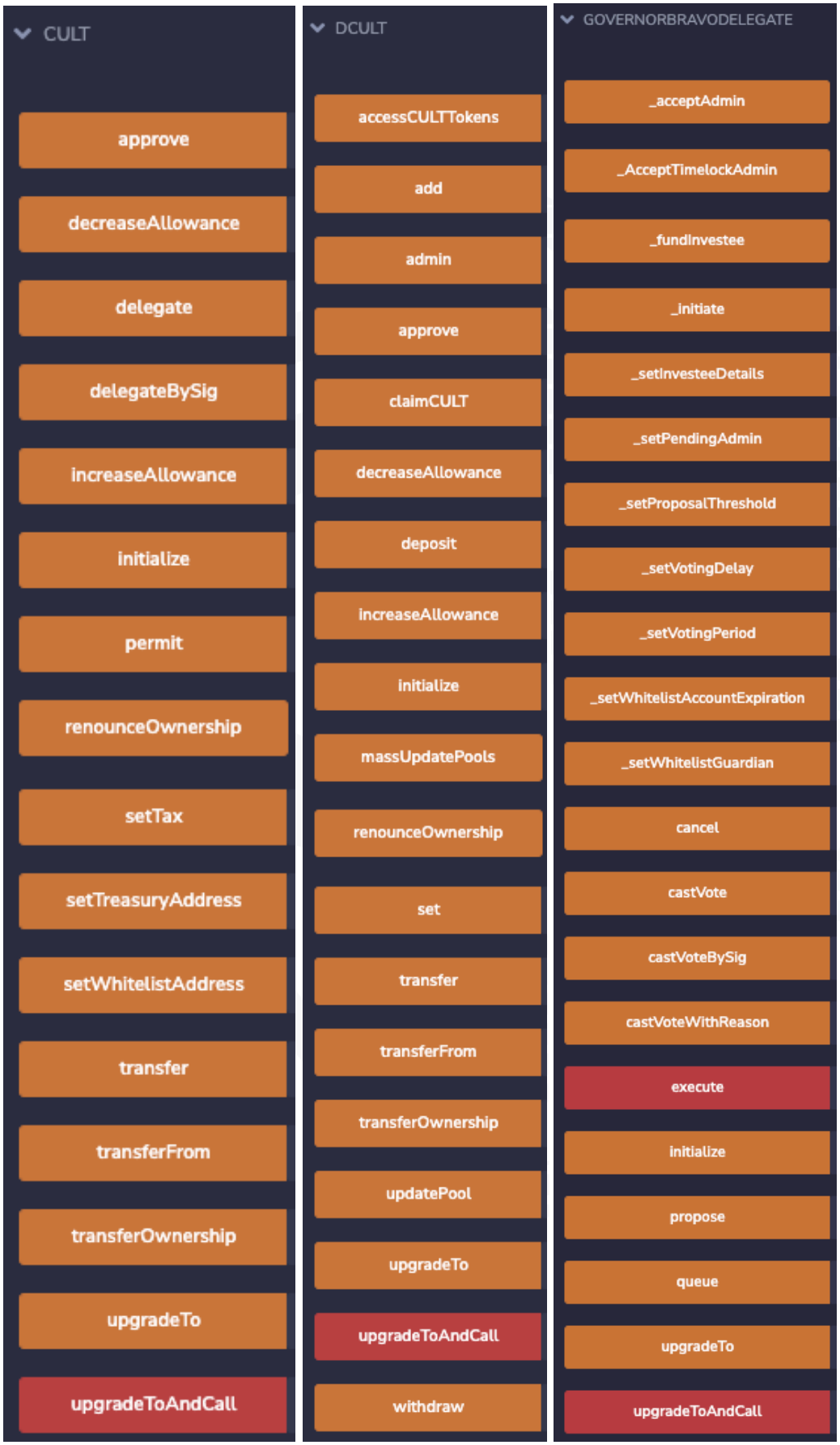
We will verify the following claims:

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

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 v1.0



TIMELOCK
acceptAdmin
cancelTransaction
executeTransaction
initialize
queueTransaction
setDelay
setPendingAdmin
upgradeTo
upgradeToAndCall
TREASURY
initialize
renounceOwnership
setDAOAddress
transferOwnership
upgradeTo
upgradeToAndCall
validatePayout

Deployer cannot mint any new tokens

Name	Exist	Tested	Status
Deployer cannot mint	✓	✓	✓
Max / Total Supply	Can set while deploying		

Deployer cannot burn or lock user funds

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

Comments:

v1.0

- Deployer can lock user funds if address sender or receiver is not whitelisted address by setting tax amount to high value (e.g. 1000)

Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	✓	✓	✗

Comments:

v1.0

- Contract can be paused

Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

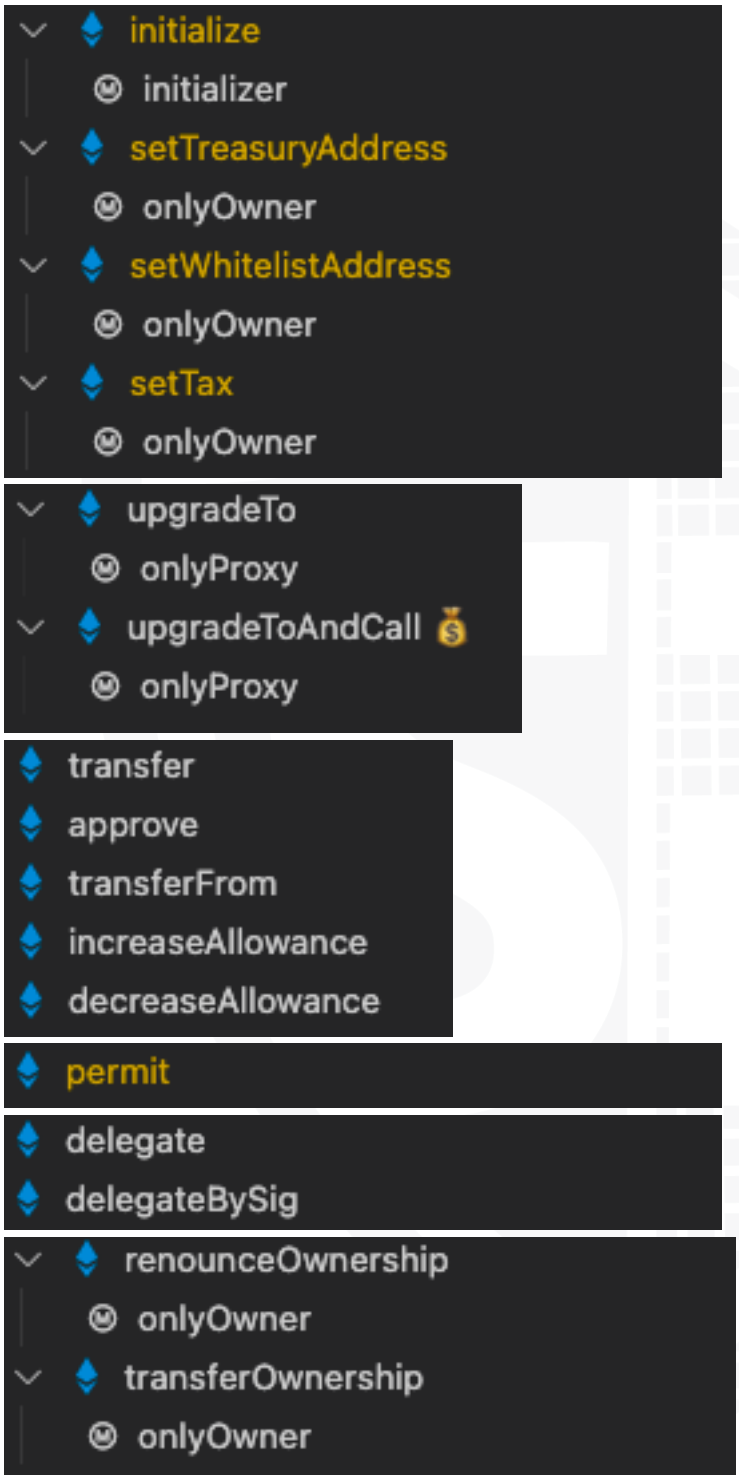
Legend

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

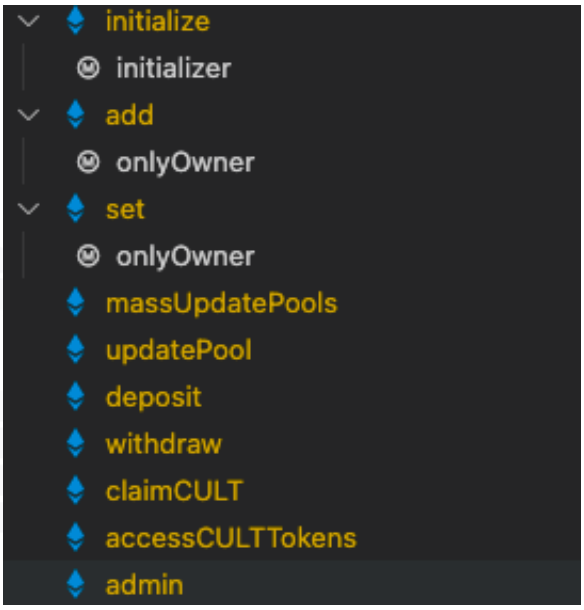
Modifiers and public functions

v1.0

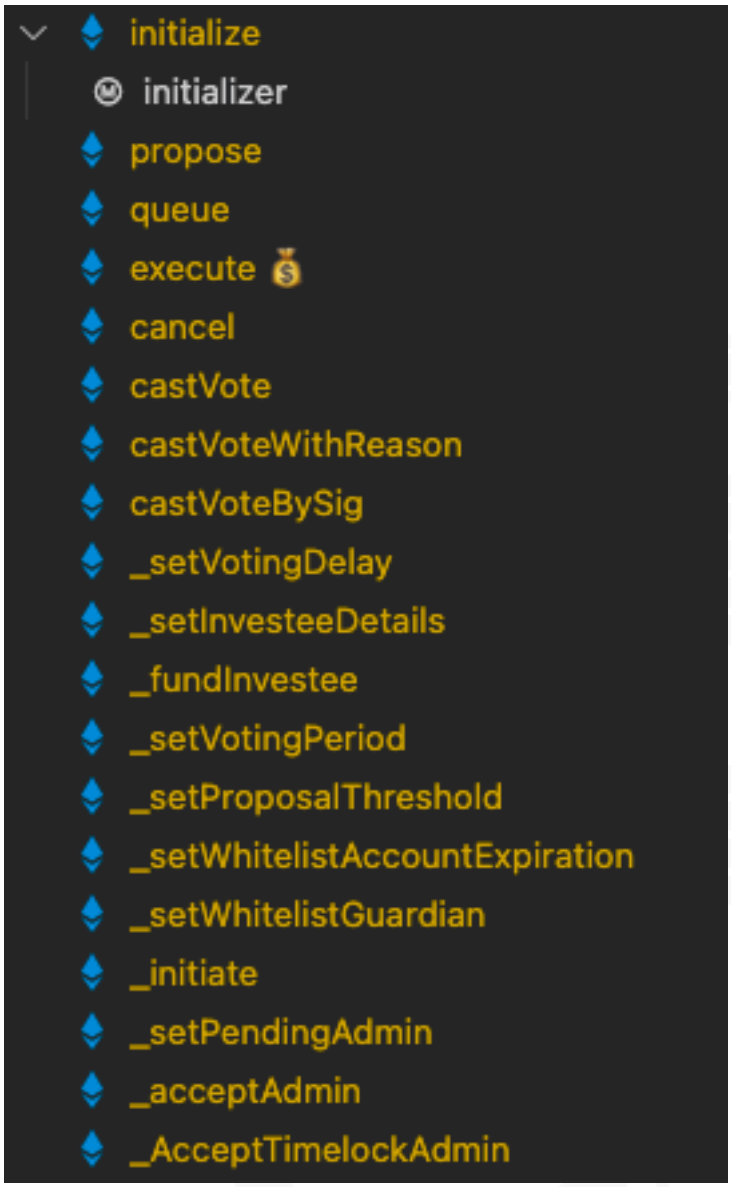
Cult



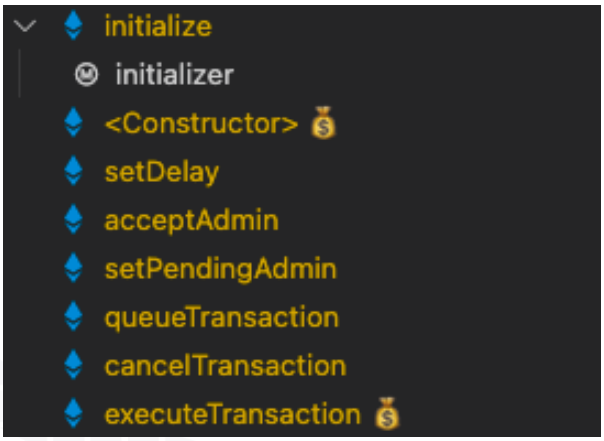
DCult



Governance



Timelock



Comments

- Deployer can set following state variables without any limitations
  - Cult
    - tax
    - poolInfo[_pid].allocPoint

- Deployer can enable/disable following state variables
  - Cult
    - whitelistedAddress[_whitelist]

- Cult
  - Exclude old treasury address from whitelistedAddress while setting new treasury address
- DCult
  - While deposit contract will mint new tokens
  - While withdraw contract will burn tokens

    - accessCULTTokens function can only be called from the admin address
    - Only Admin can set new admin address
- Governance
    - Only admin address can call following functions
        - _setVotingDelay
        - _setInvesteeDetails
        - _setVotingPeriod
        - _setProposalThreshold
        - _setWhitelistAccountExpiration
        - _setWhitelistGuardian
        - _initiate
        - _setPendingAdmin
    - Only treasury address can call following functions
        - _fundInfestee
    - Only whitelistGuardian address can call following functions
        - _setWhitelistAccountExpiration
    - Only pendingAdmin can call following functions
        - _acceptAdmin
        - _AcceptTimelockAdmin
- Timelock
    - Only admin address can call following functions
        - queueTransaction
        - cancelTransaction
        - executeTransaction
    - Only contract itself can call following functions
        - setDelay
    - Only pendingAdmin can call following functions
        - acceptAdmin
    - If admin is initialized only contract itself can call setPendingAdming otherwise admin has to call setPendingAdmin function
- Treasury
    - onlyAdmin can call following functions
        - setDAOAddress

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/treasury.sol	1	2	111	59	50	1	84	
	contracts/dcult.sol	1	———	398	377	261	89	203	
	contracts/cult.sol	1	1	106	83	68	1	64	———
	contracts/GovernorBravoInterfaces.sol	4	4	207	191	76	62	49	
	contracts/timelock.sol	1	———	122	122	89	2	81	
	contracts/governance.sol	1	———	489	489	265	155	237	
	Totals	**9**	**7**	**1433**	**1321**	**809**	**310**	**718**	

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	GovernorBravoInterfaces	A floating pragma is set	1	The current pragma Solidity directive is „“^0.8.4””.
#2	DCult	Missing Zero Address Validation (missing-zero-check)	374, 83	Check that the address is not zero
#3	Governance	Missing Zero Address Validation (missing-zero-check)	425, 399, 65	Check that the address is not zero
#4	Timelock	Missing Zero Address Validation (missing-zero-check)	87, 28, 55	Check that the address is not zero
#5	Treasury	Missing Zero Address Validation (missing-zero-check)	74, 75, 92	Check that the address is not zero
#6	Cult	Missing Events Arithmetic	79	Emit an event for critical parameter changes

#7	DCult	Missing Events Arithmetic	360	Emit an event for critical parameter changes
#8	Governance	Missing Events Arithmetic	412	Emit an event for critical parameter changes

Informational issues

Issue	File	Type	Line	Description
#1	Treasury	State variables that could be declared constant (constable-states)	70	Add the `constant` attributes to state variables that never change
#2	Governance	Unused return values	166	Ensure that all the return values of the function calls are used and handle both success and failure cases if needed by the business logic
#3	Governane	SPDX-License-Identifier is missing	-	Provide a SPDX-License-Identifier in source code
#4	GovernorBravorInterfaces	SPDX-License-Identifier is missing	-	Provide a SPDX-License-Identifier in source code
#5	Timelock	SPDX-License-Identifier is missing	-	Provide a SPDX-License-Identifier in source code
#6	Governance	Misspelling	Lines next to misspelling word	Change: - contructor to constructor line: 58 - timlock to timelock line: 462 - transfering to transferring line: 463 Make sure to change variable/functions etc. everywhere else if you changed it

#7	DCult	Misspelling	Lines next to misspelling word	Change: - poitns to points line: 68 - vairables to variables line: 151 - highes to highest line: 189, 194 - fuction to function line: 195 - hisghest to highest line: 337 Make sure to change variable/functions etc. everywhere else if you changed it
#8	DCult	Naming convention	Lines next to word	Use mixedCase for public state/local variables Change: - adminaddr to adminAddress line: 56, 91, 361, 375, 376 - _adminaddr to _adminAddress line: 83, 91, 374, 376 - higheststaker to highestStaker line: 239, 241, 242, 243, 245, 250, 252, 255, 257, 258, 262, 277, 280, 281 Make sure to change variable/functions etc. everywhere else if you changed it

Commented Code exist

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

File	Line	Comment
Governance	94	// require(initialProposalId != 0, "GovernorBravo::propose: Governor Bravo not active");

Recommendation
Remove the commented code, or address them properly.

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.

25. January 2022:
- Read whole report 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	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