

SKELETON ECOSYSTEM

SMART CONTRACT AUDIT



Decentream
DCM
BEP 20

0xfc6a90c7e72f911686d84f26b0c60e77064555bd



Table of Contents

Table of Contents	1
Disclaimer	2
Overview	3
Creation/Audit Date	3
Verified Socials	3
Contract Functions Analysis	4
Contract Safety and Weakness	8
Detected Vulnerability Description	10
Contract Flow Graph	11
Contract Interaction Graph	12
Inheritance Graph	13
Contract Descriptions	14
Audit Scope	24

Global Disclaimer

This document serves as a disclaimer for the crypto smart contract audit conducted by Skeleton Ecosystem. The purpose of the audit was to review the codebase of the smart contracts for potential vulnerabilities and issues. It is important to note the following:

Limited Scope: The audit is based on the code and information available up to the audit completion date. It does not cover external factors, system interactions, or changes made after the audit. The audit itself can not guarantee 100% safety and can not detect common scam methods like farming and developer sell-out.

No Guarantee of Security: While we have taken reasonable steps to identify vulnerabilities, it is impossible to guarantee the complete absence of security risks or issues. The audit report provides an assessment of the contract's security as of the audit date.

Continued Development: Smart contracts and blockchain technology are evolving fields. Updates, forks, or changes to the contract post-audit may introduce new risks that were not present during the audit.

Third-party Code: If the smart contract relies on third-party libraries or code, those components were not thoroughly audited unless explicitly stated. Security of these dependencies is the responsibility of their respective developers.

Non-Exhaustive Testing: The audit involved automated analysis, manual review, and testing under controlled conditions. It is possible that certain vulnerabilities or issues may not have been identified.

Risk Evaluation: The audit report includes a risk assessment for identified vulnerabilities. It is recommended that the development team carefully reviews and addresses these risks to mitigate potential exploits.

Not Financial Advice: This audit report is not intended as financial or investment advice. Decisions regarding the use, deployment, or investment in the smart contract should be made based on a comprehensive assessment of the associated risks.

By accessing and using this audit report, you acknowledge and agree to the limitations outlined above. Skeleton Ecosystem and its auditors shall not be held liable for any direct or indirect damages resulting from the use of the audit report or the smart contract itself.

Please consult with legal, technical, and financial professionals before making any decisions related to the smart contract.

Overview

Contract Name	Decentreum
Ticker/Simbol	DCM
Blockchain	Binance Smart Chain BEP20
Contract Address	0xfc6a90c7e72f911686d84f26b0c60e77064555bd
Creator Address	0xB75d9546EcdAA7eeE091aabe45eF2B5236FBD4F7
Current Owner Address	0xB75d9546EcdAA7eeE091aabe45eF2B5236FBD4F7
Contract Explorer	https://bscscan.com/address/0xfc6a90c7e72f911686d84f26b0c60e77064555bd#code
Compiler Version	v0.8.7+commit.e28d00a7
License	MIT
Optimisation	Yes with 200 Runs
Total Supply	200,000,000 DCM
Decimals	9

Creation/Audit

Contract Deployed	20 Dec 2023
Audit Created	24 Dec 2023
Audit Update	V 1.0

Verified Socials

Website	https://decentreum.org/
Telegram	https://t.me/Decentreum
Twitter (X)	https://twitter.com/Decentreum

Contract Function Analysis



Pass



Attention Item

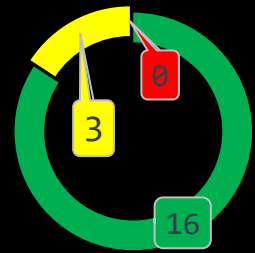


Risky Item



Pass

Attention

Risk



Contract Verified		The contract source code is uploaded to blockchain explorer and is open source, so everybody can read it.
Contract Ownership		0xB75d9546EcdAA7eeE091aabe45eF2B5236FBD4F7
Buy Tax	10 %	Shows the taxes for purchase transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Sell Tax	10 %	Shows the taxes for sell transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Honeypot Analyse		Holder is able to buy and sell. If honeypot: The contract blocks sell transfer from holder wallet. Multiple events may cause honeypot. Trading disabled, extremely high tax
Liquidity Status		LP Lock Status on 23.12.2023: 100.00% Pinklock for 92 days.
Trading Disable Functions		No Trading suspendable function found. If a suspendable code is included, the token maybe neither be bought or sold (honeypot risk). If contract is renounced this function can't be used
Set Fees function		Fee Setting function found. The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).
Proxy Contract		Not a proxy contract!
Mint Function		No Mint Function detected Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token. Owner can mint new tokens and sell.

Balance Modifier Function		<p>No Balance Modifier function found.</p> <p>If there is a function for this, the contract owner can have the authority to modify the balance of tokens at other addresses. For example revoke the bought tokens from the holders wallet. Common form of scam: You buy the token, but it's disappearing from your wallet.</p>
Blacklist Function		<p>No Blacklist Setting function found.</p> <p>If there is a blacklist, some addresses may not be able to trade normally. Example: you buy the token and right after your Wallet getting blacklisted. Like so you will be unable to sell. Honeypot Risk.</p>
Whitelist Function		<p>Whitelist Setting function found.</p> <p>If there is a function for this Developer can set zero fee or no max wallet size for addresses (for example team wallets can trade without fee. Can cause farming)</p>
Hidden Owner Analysis		<p>No Hidden or multi owner with authorisation</p> <p>For contract with a hidden owner, developer can still manipulate the contract even if the ownership has been abandoned.</p>
Retrieve Ownership Function		<p>No Functions found which can retrieve ownership of the contract.</p> <p>If this function exists, it is possible for the project owner to regain ownership even after relinquishing it. Also known as fake renounce.</p>
Self Destruct Function		<p>No Self Destruct function found.</p> <p>If this function exists and is triggered, the contract will be destroyed, all functions will be unavailable, and all related assets will be erased.</p>
Specific Tax Changing Function		<p>No Specific Tax Changing Functions found.</p> <p>If it exists, the contract owner may set a very outrageous tax rate for assigned address to block it from trading. Can assign all wallets at once!</p>
Trading Cooldown Function		<p>No Trading Cooldown Function found. If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying. Like a temporary honeypot.</p>
Max Transaction and Holding Modify Function		<p>Max Transaction and Holding Modify function found</p> <p>If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot</p>
Transaction Limiting Function		<p>No Transaction Limiter Function Found.</p> <p>The number of overall token transactions may be limited (honeypot risk)</p>

Details of Risk - Attention Items

Set Fee

The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded

```
808     ftrace | funcSig
809     function setBuyTaxes(
810         uint256 newLiquidityTax!,
811         uint256 newMarketingTax!,
812         uint256 newTeamTax!
813     ) external onlyOwner {
814         _buyLiquidityFee = newLiquidityTax!;
815         _buyMarketingFee = newMarketingTax!;
816         _buyTeamFee = newTeamTax!;
817
818         totalTaxIfBuying = _buyLiquidityFee.add(_buyMarketingFee).add(
819             _buyTeamFee
820         );
821     }
822
823     ftrace | funcSig
824     function setSellTaxes(
825         uint256 newLiquidityTax!,
826         uint256 newMarketingTax!,
827         uint256 newTeamTax!
828     ) external onlyOwner {
829         _sellLiquidityFee = newLiquidityTax!;
830         _sellMarketingFee = newMarketingTax!;
831         _sellTeamFee = newTeamTax!;
832
833         totalTaxIfSelling = _sellLiquidityFee.add(_sellMarketingFee).add(
834             _sellTeamFee
835         );
836     }
```

⚠ Whitelist Function

If there is a function for this, Developer can set zero fee or no max wallet size for addresses (for example team wallets can trade without fee. Can cause farming)

```

792     }
793
794     ftrace | funcSig
795     function setIsTxLimitExempt(address holder!, bool exempt!)
796     |
797     |   external
798     |   |
799     |   |   onlyOwner
800     |   |
801     |   {
802     |     |   _isTxLimitExempt[holder!] = exempt!;
803     |   }
804
805     ftrace | funcSig
806     function setIsExcludedFromFee(address account!, bool newValue!)
807     |
808     |   public
809     |   |
810     |   |   onlyOwner
811     |   |
812     |   {
813     |     |   _isExcludedFromFee[account!] = newValue!;
814     |   }
  
```

⚠ Max Transaction and Holding Modify Function

If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot

```

846     |   _teamShare
847     |   );
848     |   }
849
850     ftrace | funcSig
851     function setMaxTxAmount(uint256 maxTxAmount!) external onlyOwner {
852     |   |   _maxTxAmount = maxTxAmount!;
853     |   }
  
```

```

863     |   }
864
865     ftrace | funcSig
866     function setWalletLimit(uint256 newLimit!) external onlyOwner {
867     |   |   _walletMax = newLimit!;
868     |   }
  
```


Contract Security

Total Findings: 6


 High 0


 Medium


 Low 4


 Info 2



 **High Severity Issues:** High possibility to cause problems, need to be resolved.

 **Medium Severity Issue:** Will likely cause problems, recommended to resolve.


 **Low Severity Issues:** Won't cause problems, but for improvement purposes could be adjusted.

 **Informational Severity Issues:** Not harmful in any way, information for the developer team.

Contract Security


List of Found Issues

 **High severity Issues: (0)**

 **Medium severity issues: (0)**

 **Low severity issues: (4)**

- Missing Events
- Long Number Literals
- Outdated Compiler Version
- Floating Pragma

 **Informational severity issues: (2)**

- Public Functions Should be Declared External
- Variables never used

Contract Weakness Classisication

THE SMART CONTRACT WEAKNESS CLASSIFICATION REGISTRY (SWC REGISTRY) IS AN IMPLEMENTATION OF THE WEAKNESS CLASSIFICATION SCHEME PROPOSED IN EIP-1470. IT IS LOOSELY ALIGNED TO THE TERMINOLOGIES AND STRUCTURE USED IN THE COMMON WEAKNESS ENUMERATION (CWE) WHILE OVERLAYING A WIDE RANGE OF WEAKNESS VARIANTS THAT ARE SPECIFIC TO SMART CONTRACTS.

ID	Description	AI	Manual	Result
SWC-100	Function Default Visibility	Passed	Passed	Passed
SWC-101	Integer Overflow and Underflow	Passed	Passed	Passed
SWC-102	Outdated Compiler Version	Low	Passed	Passed
SWC-103	Floating Pragma	Low	Passed	Passed
SWC-104	Unchecked Call Return Value	Passed	Passed	Passed
SWC-105	Unprotected Ether Withdrawal	Passed	Passed	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed	Passed	Passed
SWC-107	Reentrancy	Passed	Passed	Passed
SWC-108	State Variable Default Visibility	Passed	Passed	Passed
SWC-109	Uninitialized Storage Pointer	Passed	Passed	Passed
SWC-110	Assert Violation	Passed	Passed	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed	Passed	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed	Passed	Passed
SWC-113	DoS with Failed Call	Passed	Passed	Passed
SWC-114	Transaction Order Dependence	Passed	Passed	Passed
SWC-115	Authorization through tx.origin	Passed	Passed	Passed
SWC-116	Block values as a proxy for time	Passed	Passed	Passed
SWC-117	Signature Malleability	Passed	Passed	Passed
SWC-118	Incorrect Constructor Name	Passed	Passed	Passed
SWC-119	Shadowing State Variables	Passed	Passed	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed	Passed	Passed

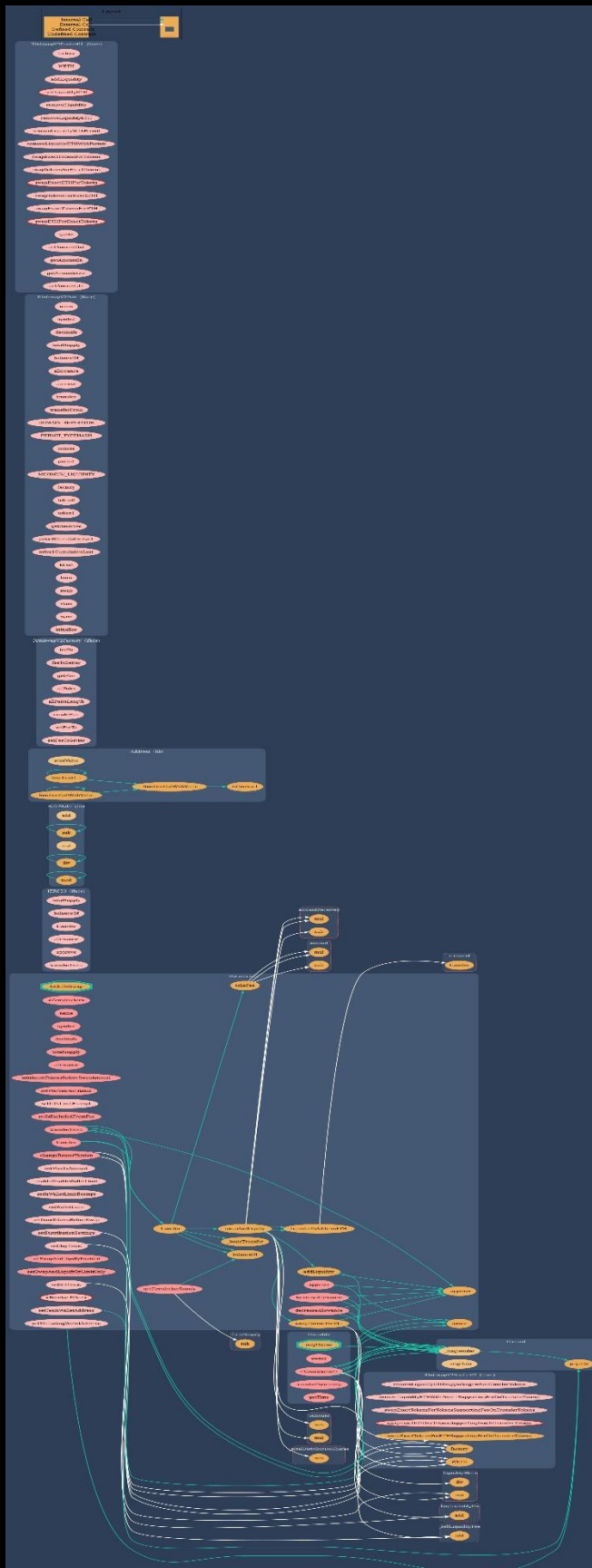
SWC-121	Missing Protection against Signature Replay Attacks	Passed	Passed	Passed
SWC-122	Lack of Proper Signature Verification	Passed	Passed	Passed
SWC-123	Requirement Violation	Passed	Passed	Passed
SWC-124	Write to Arbitrary Storage Location	Passed	Passed	Passed
SWC-125	Incorrect Inheritance Order	Passed	Passed	Passed
SWC-126	Insufficient Gas Griefing	Passed	Passed	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed	Passed	Passed
SWC-128	DoS With Block Gas Limit	Passed	Passed	Passed
SWC-129	Typographical Error	Passed	Passed	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed	Passed	Passed
SWC-131	Presence of unused variables	Passed	Passed	Passed
SWC-132	Unexpected Ether balance	Passed	Passed	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed	Passed	Passed
SWC-134	Message call with hardcoded gas amount	Passed	Passed	Passed
SWC-135	Code With No Effects	Passed	Passed	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed	Passed	Passed

Detected High and Medium Severity Vulnerability Description.



No High and Medium Severity Issues Found

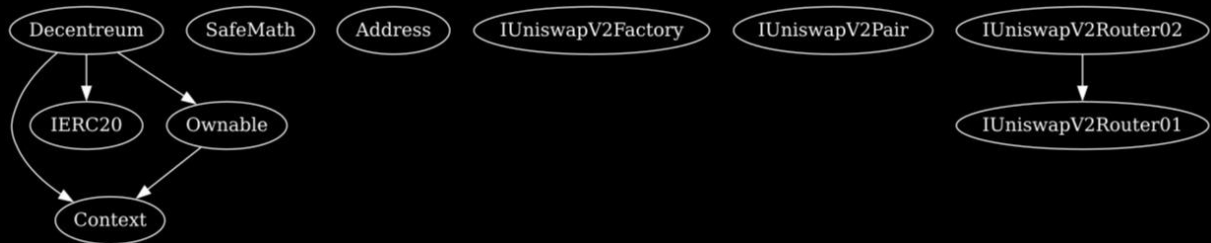
Contract Flow Graph



























Contract Interaction Graph
















































Inheritance Graph
























































































Contract Functions



Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
L	_msgSender	Internal 		
L	_msgData	Internal 		
IERC20	Interface			
L	totalSupply	External 		NO 
L	balanceOf	External 		NO 
L	transfer	External 		NO 
L	allowance	External 		NO 
L	approve	External 		NO 
L	transferFrom	External 		NO 
SafeMath	Library			
L	add	Internal 		
L	sub	Internal 		
L	sub	Internal 		
L	mul	Internal 		
L	div	Internal 		
L	div	Internal 		
L	mod	Internal 		
















L	mod	Internal 🔒		
Address	Library			
L	isContract	Internal 🔒		
L	sendValue	Internal 🔒	⚙️	
L	functionCall	Internal 🔒	⚙️	
L	functionCall	Internal 🔒	⚙️	
L	functionCallWithValue	Internal 🔒	⚙️	
L	functionCallWithValue	Internal 🔒	⚙️	
L	_functionCallWithValue	Private 🔒	⚙️	
Ownable	Implementation	Context		
L		Public 🚫	⚙️	NO 🚫
L	owner	Public 🚫		NO 🚫
L	transferOwnership	Public 🚫	⚙️	onlyOwner
L	getTime	Public 🚫		NO 🚫
IUniswapV2Factory	Interface			
L	feeTo	External 🚫		NO 🚫
L	feeToSetter	External 🚫		NO 🚫
L	getPair	External 🚫		NO 🚫
L	allPairs	External 🚫		NO 🚫
L	allPairsLength	External 🚫		NO 🚫



















L	createPair	External 		NO 
L	setFeeTo	External 		NO 
L	setFeeToSetter	External 		NO 
IUniswapV2Pair	Interface			
L	name	External 		NO 
L	symbol	External 		NO 
L	decimals	External 		NO 
L	totalSupply	External 		NO 
L	balanceOf	External 		NO 
L	allowance	External 		NO 
L	approve	External 		NO 
L	transfer	External 		NO 
L	transferFrom	External 		NO 
L	DOMAIN_SEPARATOR	External 		NO 
L	PERMIT_TYPEHASH	External 		NO 
L	nonces	External 		NO 
L	permit	External 		NO 
L	MINIMUM_LIQUIDITY	External 		NO 
L	factory	External 		NO 
L	token0	External 		NO 
L	token1	External 		NO 

L	getReserves	External 		NO 
L	price0CumulativeLast	External 		NO 
L	price1CumulativeLast	External 		NO 
L	kLast	External 		NO 
L	burn	External 		NO 
L	swap	External 		NO 
L	skim	External 		NO 
L	sync	External 		NO 
L	initialize	External 		NO 
IUniswapV2Router01	Interface			
L	factory	External 		NO 
L	WETH	External 		NO 
L	addLiquidity	External 		NO 
L	addLiquidityETH	External 		NO 
L	removeLiquidity	External 		NO 
L	removeLiquidityETH	External 		NO 
L	removeLiquidityWithPermit	External 		NO 
L	removeLiquidityETHWithPermit	External 		NO 
L	swapExactTokensForTokens	External 		NO 

L	swapTokensForExactTokens	External 		NO 
L	swapExactETHForTokens	External 		NO 
L	swapTokensForExactETH	External 		NO 
L	swapExactTokensForETH	External 		NO 
L	swapETHForExactTokens	External 		NO 
L	quote	External 		NO 
L	getAmountOut	External 		NO 
L	getAmountIn	External 		NO 
L	getAmountsOut	External 		NO 
L	getAmountsIn	External 		NO 
IUniswapV2Router02	Interface	IUniswapV2Router01		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External 		NO 
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External 		NO 
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External 		NO 
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External 		NO 

	rtngFeeOnTran sferTokens			
L	swapExactTokesForETHSupportingFeeOnTransferTokens	External !		NO!
Decentreum	Implementation	Context, IERC20, Ownable		
L		Public !		NO!
L	name	Public !		NO!
L	symbol	Public !		NO!
L	decimals	Public !		NO!
L	totalSupply	Public !		NO!
L	balanceOf	Public !		NO!
L	allowance	Public !		NO!
L	increaseAllowance	Public !		NO!
L	decreaseAllowance	Public !		NO!
L	minimumTokensBeforeSwapAmount	Public !		NO!
L	approve	Public !		NO!
L	_approve	Private !		
L	setMarketPairStatus	Public !		onlyOwner
L	setIsTxLimitExempt	External !		onlyOwner

L	setIsExcludedFromFee	Public ⓘ		onlyOwner
L	setBuyTaxes	External ⓘ		onlyOwner
L	setSellTaxes	External ⓘ		onlyOwner
L	setDistributionSettings	External ⓘ		onlyOwner
L	setMaxTxAmount	External ⓘ		onlyOwner
L	enableDisableWalletLimit	External ⓘ		onlyOwner
L	setIsWalletLimitExempt	External ⓘ		onlyOwner
L	setWalletLimit	External ⓘ		onlyOwner
L	setNumTokensBeforeSwap	External ⓘ		onlyOwner
L	setMarketingWalletAddress	External ⓘ		onlyOwner
L	setTeamWalletAddress	External ⓘ		onlyOwner
L	setSwapAndLiquifyEnabled	Public ⓘ		onlyOwner
L	setSwapAndLiquifyByLimitOnly	Public ⓘ		onlyOwner
L	getCirculatingSupply	Public ⓘ		NO ⓘ
L	transferToAddressETH	Private 🔒		
L	changeRouterVersion	Public ⓘ		onlyOwner
L		External ⓘ		NO ⓘ

L	transfer	Public 		NO 
L	transferFrom	Public 		NO 
L	_transfer	Private 		
L	_basicTransfer	Internal 		
L	swapAndLiquify	Private 		lockTheSwap
L	swapTokensFor Eth	Private 		
L	addLiquidity	Private 		
L	takeFee	Internal 		



Function
can modify
state



Function
is payable

Audit Scope

Audit Method.

Our smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. Goal: discover errors, issues and security vulnerabilities in the code. Findings getting reported and improvements getting suggested.

Automatic and Manual Review

We are using automated tools to scan functions and weaknesses of the contract. Transfers, integer over-undeflow checks such as all CWE events.

Tools we use:

Visual Studio Code

CWE

SWC

Solidity Scan

SVD

In manual code review our auditor looking at source code and performing line by line examination. This method helps to clarify developer's coding decisions and business logic.

Skeleton Ecosystem

<https://skeletonecosystem.com>

<https://github.com/SkeletonEcosystem/Audits>

