

SKELETON ECOSYSTEM

SMART CONTRACT AUDIT



Decentra Ecosystem

DCE

ERC20

0xf2c5780e2DDA407781c0C5ECCC9320D5988eA0A6



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	7
Detected Vulnerability Description	11
Contract Flow Graph	14
Contract Interaction Graph	15
Inheritance Graph	16
Contract Descriptions	17
Audit Scope	21

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	DecentraEcosystem
Ticker/Symbol	DCE
Blockchain	ETHEREUM ERC20
Contract Address	0xf2c5780e2DDA407781c0C5ECCC9320D5988eA0A6
Creator Address	0xbcB64f4FF2C7BdEEd5Ff14e2Ef2FEfa041481C0F
Current Owner Address	0x00
Contract Explorer	https://etherscan.io/token/0xf2c5780e2DDA407781c0C5ECCC9320D5988eA0A6#code
Compiler Version	v0.8.19+commit.7dd6d404
License	MIT
Optimisation	Yes with 9999 Runs
Total Supply	1,000,000 DCE
Decimals	9




Creation/Audit

Contract Deployed	31.07.2024
Audit Created	14.08.2024
Audit Update	V 1.0

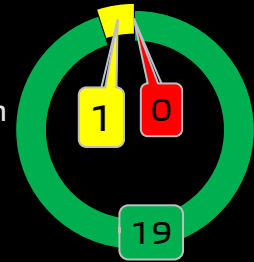
Verified Socials

Website	https://decentra.network
Telegram	https://t.me/DecentraERC20
Twitter (X)	https://twitter.com/DecentraERC20











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		0x00 Sometimes referred to as the "zero address" or "dead address" and is not owned by anyone.
Buy Tax	5 %	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	5 %	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		Liquidity status on 14.08.2024 100% of LP token are Burned.
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		No 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>Contract renounced, function can not be triggered by owner.</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>No 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

Removing Risk of contract function based on renounced ownership

Transaction Receipt Event Logs

236 **Address** Decentra Ecosystem: DCE Token   

Name OwnershipTransferred (index_topic_1 address previousOwner, index_topic_2 address newOwner) [View Source](#)

Topics 0 0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0

1: previousOwner Dec ▾ ⇒ 0x8bcB64f4FF2C7BdEEd5Ff14e2Ef2FEfa041481C0F

2: newOwner Dec ▾ ⇒ 0x00

Data 0x

Following detected contract functions serve as informational purposes about the contract. The owner has no more authorisation to trigger functions.

⚠ Whitelist (Set Zero Fee wallets)

Contract renounced, function can not be triggered by owner.

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

```

395 ftrace | funcSig
396 function excludeFromFees(
397     address account!,
398     bool excluded!
399 ) external onlyOwner {
400     _isExcludedFromFees[account!] = excluded!;
401     emit ExcludeFromFees(account!, excluded!);
402 }
403
404 ftrace | funcSig
405 function isExcludedFromFees(address account!) public view returns (bool) {
406     return _isExcludedFromFees[account!];
407 }
  
```

Contract Security

Total Findings: 6

- High 0
- Medium 0
- Low 3
- Info 3



■ **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: (3)**

- Missing Events
- Approve Front Running Attack (Sandwich Bots)
- Outdated Compiler Version

 **Informational severity issues: (3)**

- Public Functions Should be Declared External
- State Variables Should be Declared Constant
- Precision Loss During Division By Large Numbers

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

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	low	low
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	low	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.

⚠ Outdated Compiler Version

Item: 1	Location:	Line 21	Severity:	■ Low
---------	-----------	---------	-----------	-------

Function	Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version. The following outdated versions were detected: /dce.sol - 0.8.19
Remedation	It is recommended to use a recent version of the Solidity compiler that should not be the most recent version, and it should not be an outdated version as well. Using very old versions of Solidity prevents the benefits of bug fixes and newer security checks. Consider using the solidity version v0.8.25, which patches most solidity vulnerabilities.

⚠️ Approve of front running attack. Also known as Sandwich Bot attack. (2 Item)

Item: 1	Location:	Line 198-204	Severity: ■ Low
---------	-----------	--------------	--

Function	<p>The approve() method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account.</p> <p>This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account. Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function. The function approve can be front-run by abusing the _approve function.</p>
Remediation	<p>1.Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions.</p> <p>2.Use transaction taxes to prevent against front-run attack</p>

```

198      ftrace | funcSig
199      function approve(
200          address spender!,
201          uint256 amount!
202      ) public virtual override returns (bool) {
203          _approve(_msgSender(), spender!, amount!);
204          return true;
205      }
  
```

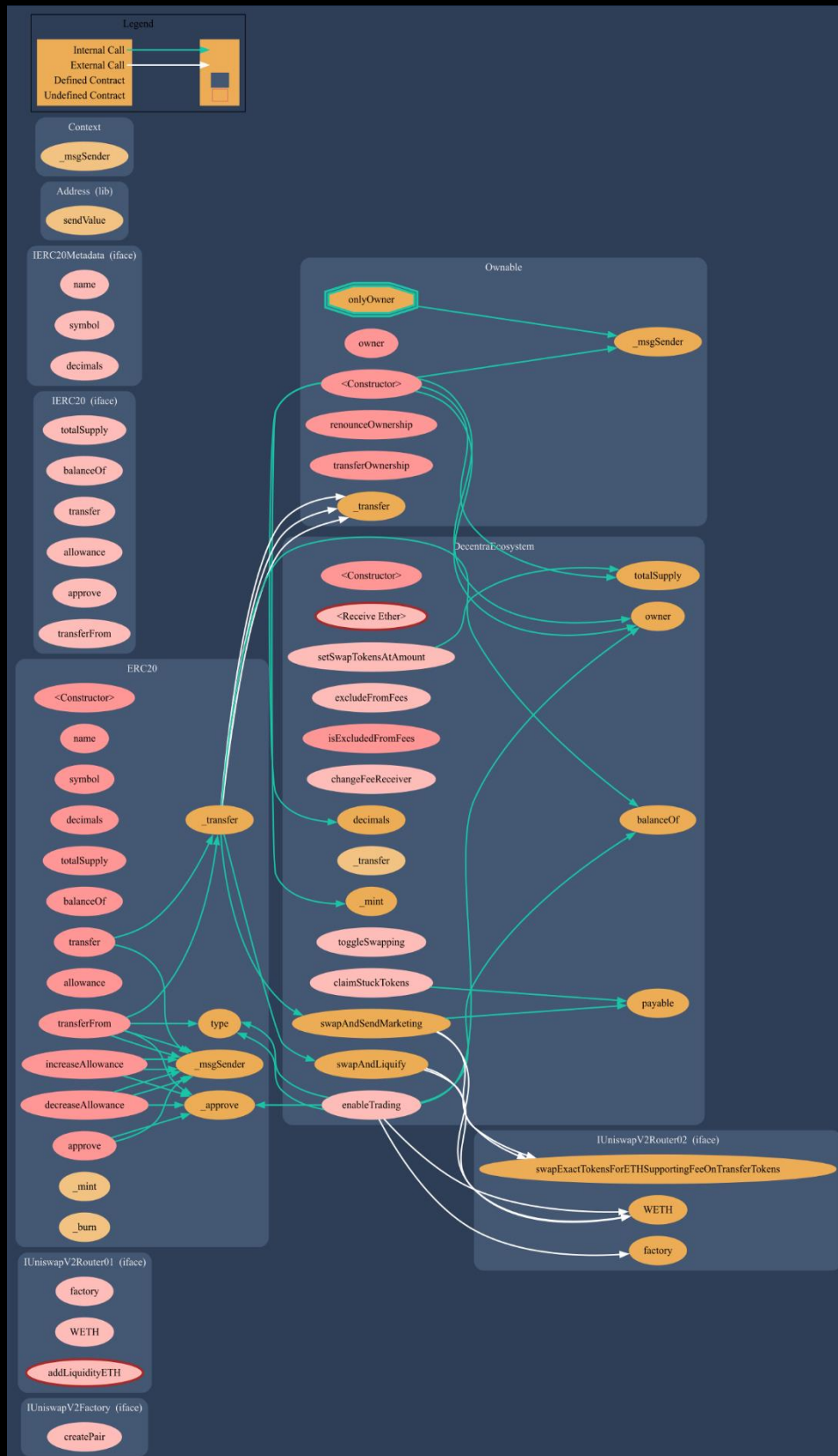
Item: 2	Location:	Line 206-225	Severity: ■ Low
---------	-----------	--------------	--

Function	<p>The TransferFrom() method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account.</p> <p>This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account. Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function. The function approve can be front-run by abusing the <code>_approve</code> function.</p>
Remedation	<ol style="list-style-type: none"> 1. Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions. 2. Use transaction taxes to prevent against front-run attack

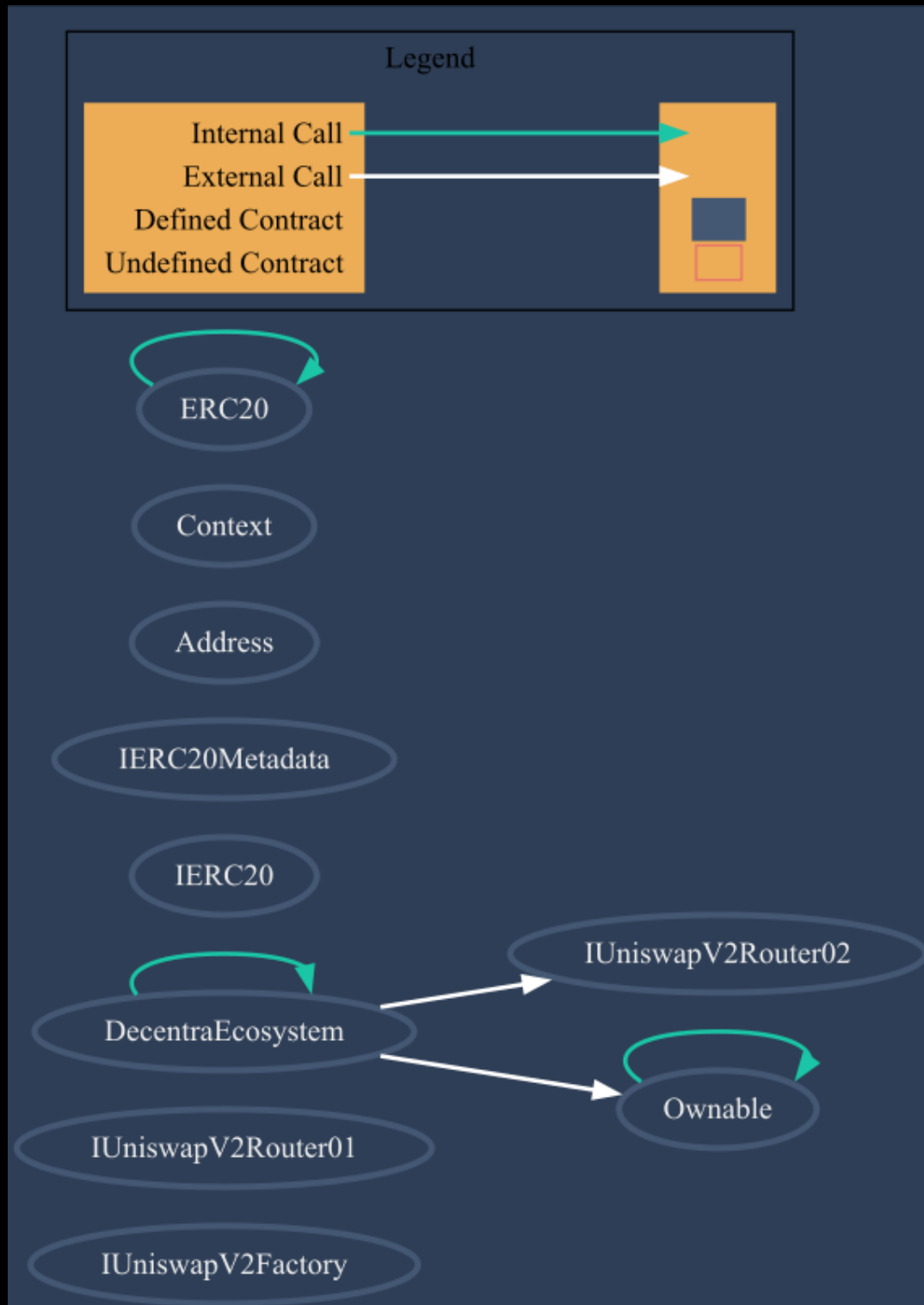
```

206  function transferFrom(
207      address sender!,
208      address recipient!,
209      uint256 amount!
210  ) public virtual override returns (bool) {
211      uint256 currentAllowance = allowances[sender!][_msgSender()];
212      if (currentAllowance != type(uint256).max) {
213          require(
214              currentAllowance >= amount!,
215              "ERC20: transfer amount exceeds allowance"
216          );
217          unchecked {
218              _approve(sender!, _msgSender(), currentAllowance - amount!);
219          }
220      }
221
222      _transfer(sender!, recipient!, amount!);
223
224      return true;
225  }
226
  
```

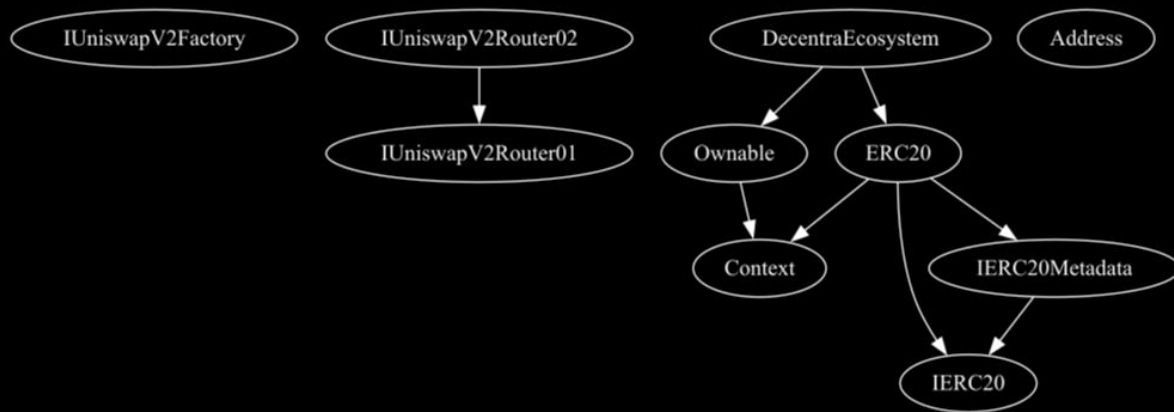
Contract Flow Graph





























Contract Interaction Graph



























Inheritance Graph





Contract Functions

Contract	Type	Bases		
		Visibility	Mutability	Modifiers
IUniswapV2Factory	Interface			
	createPair	External 		NO 
IUniswapV2Router01	Interface			
	factory	External 		NO 
	WETH	External 		NO 
	addLiquidityETH	External 		NO 
IUniswapV2Router02	Interface	IUniswapV2Router01		
	swapExactTokensForETHSupportingFeeOnTransferTokens	External 		NO 
IERC20	Interface			
	totalSupply	External 		NO 
	balanceOf	External 		NO 
	transfer	External 		NO 
	allowance	External 		NO 
	approve	External 		NO 
	transferFrom	External 		NO 
IERC20Metadata	Interface	IERC20		

Contract	Type	Bases		
L	name	External ¶		NO¶
L	symbol	External ¶		NO¶
L	decimals	External ¶		NO¶
Address	Library			
L	sendValue	Internal 🔒	⚙️	
Context	Implementation			
L	_msgSender	Internal 🔒		
Ownable	Implementation	Context		
L		Public ¶	⚙️	NO¶
L	owner	Public ¶		NO¶
L	renounceOwnership	Public ¶	⚙️	onlyOwner
L	transferOwnership	Public ¶	⚙️	onlyOwner
ERC20	Implementation	Context, IERC20, IERC20/Metadata		
L		Public ¶	⚙️	NO¶
L	name	Public ¶		NO¶
L	symbol	Public ¶		NO¶
L	decimals	Public ¶		NO¶
L	totalSupply	Public ¶		NO¶
L	balanceOf	Public ¶		NO¶
L	transfer	Public ¶	⚙️	NO¶
L	allowance	Public ¶		NO¶

Contract	Type	Bases		
L	approve	Public !		NO!
L	transferFrom	Public !		NO!
L	increaseAllowance	Public !		NO!
L	decreaseAllowance	Public !		NO!
L	_transfer	Internal 		
L	_mint	Internal 		
L	_burn	Internal 		
L	_approve	Internal 		
DecentraEcosystem	Implementation	ERC20, Ownable		
L		Public !		ERC20
L		External !		NO!
L	claimStuckTokens	External !		onlyOwner
L	excludeFromFees	External !		onlyOwner
L	isExcludedFromFees	Public !		NO!
L	changeFeeReceiver	External !		onlyOwner
L	enableTrading	External !		onlyOwner
L	_transfer	Internal 		
L	setSwapTokensAtAmount	External !		onlyOwner
L	toggleSwapping	External !		onlyOwner
L	swapAndLiquify	Private 		

Contract	Type	Bases		
L	swapAndSendMarketing	Private 		



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>

