CONSENSYS
Diligence
[🌐 📩 🔥]

Solidity Metrics for audit-thunder-loan

Table of contents

- Scope
  - Source Units in Scope
    - Deployable Logic Contracts
  - Out of Scope
    - Excluded Source Units
    - Duplicate Source Units
    - Doppelganger Contracts
- Report Overview
  - Risk Summary
  - Source Lines
  - Inline Documentation
  - Components
  - Exposed Functions
  - StateVariables
  - Capabilities
  - Dependencies
  - Totals

Scope

This section lists files that are in scope for the metrics report.

- **Project:** `audit-thunder-loan`
- **Included Files:**
  - `src/**/*.sol`
- **Excluded Paths:**
  - `**/node_modules`
  - `**/mock*`
  - `**/test*`
  - `**/migrations`
  - `**/Migrations.sol`
- **File Limit:** `2000`
  - **Exclude File list Limit:** `2000`
- **Workspace Repository:** `unknown ( main @ c96f6fe18a5946fab7d976fd87d69f4ec3c3f2e0 )`

Source Units in Scope

Source Units Analyzed: **8**
Source Units in Scope: **8** (**100%**)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
🔍	src/interfaces/ITSwapPool.sol	—	1	6	5	3	1	3	🔆
🔍	src/interfaces/IPoolFactory.sol	—	1	6	5	3	1	3	🔆
🔍	src/interfaces/IThunderLoan.sol	—	1	6	5	3	1	3	—
🔍	src/interfaces/IFlashLoanReceiver.sol	—	1	20	11	4	5	3	🔆
📝	src/protocol/OracleUpgradeable.sol	1	—	31	31	23	1	18	—
📝	src/protocol/ThunderLoan.sol	1	—	293	263	147	90	129	🌀
📝	src/protocol/AssetToken.sol	1	—	105	105	65	24	41	—
📝	src/upgradedProtocol/ThunderLoanUpgraded.sol	1	—	288	258	143	90	127	🌀
📝🔍	**Totals**	**4**	**4**	**755**	**683**	**391**	**213**	**327**	🌀🔆

Legend: [➕]

Deployable Logic Contracts

Total: 3

- 📝 `ThunderLoan`
- 📝 `AssetToken`
- 📝 `ThunderLoanUpgraded`

Out of Scope

Excluded Source Units

Source Units Excluded: **0**

[➖]

File
None

Duplicate Source Units

Duplicate Source Units Excluded: **0**

[➖]

File
None

Doppelganger Contracts

Doppelganger Contracts: **3**

[➖]

File	Contract	Doppelganger
src/interfaces/	ITSwapPool	(fuzzy) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49,

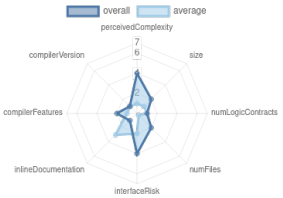
File	Contract	Doppelganger
ITSwapPool.sol		50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170
src/interfaces/IPoolFactory.sol	IPoolFactory	(fuzzy) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75
src/interfaces/IFlashLoanReceiver.sol	IFlashLoanReceiver	(fuzzy) 0, 1, 2

Report

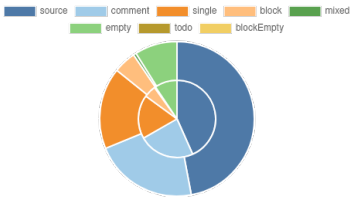
Overview

The analysis finished with `0` errors and `0` duplicate files.

Risk



Source Lines (sloc vs. nsloc)



Inline Documentation

- **Comment-to-Source Ratio:** On average there are `2.16` code lines per comment (lower=better).
- **ToDo's:** `0`

Components

📝Contracts	📚Libraries	🔍Interfaces	🎨Abstract
4	0	4	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.

🌐Public	💰Payable
38	0

External	Internal	Private	Pure	View
27	31	0	0	18

StateVariables

Total	🌐Public
14	4

Capabilities

Solidity Versions observed	🧪 Experimental Features	💰 Can Receive Funds	🖥 Uses Assembly	💣 Has Destroyable Contracts
`0.8.20`				

📤 Transfers ETH	⚡ Low-Level Calls	👥 DelegateCall	🧮 Uses Hash Functions	🔖 ECRecover	🌀 New/Create/Create2
					yes → `NewContract:AssetToken`

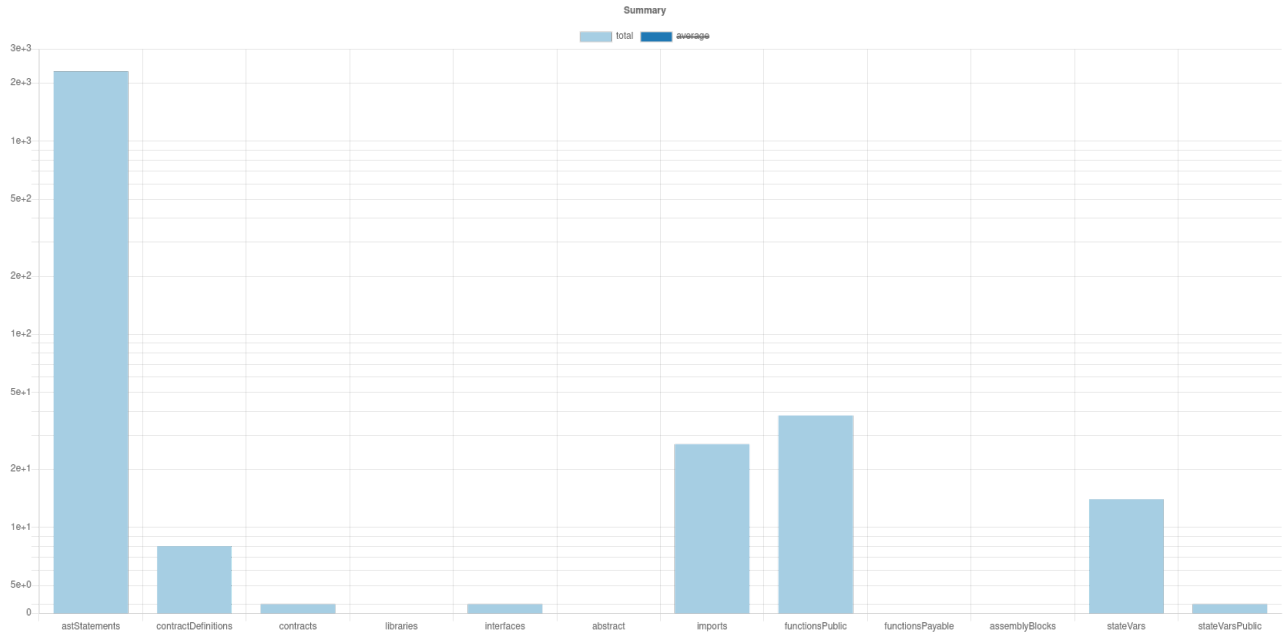
♻️ TryCatch	Σ Unchecked

Dependencies / External Imports

Dependency / Import Path	Count
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	3
@openzeppelin/contracts-upgradeable/proxy/utils/UUPSUpgradeable.sol	2
@openzeppelin/contracts/token/ERC20/ERC20.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	3
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	2
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	3
@openzeppelin/contracts/utils/Address.sol	2

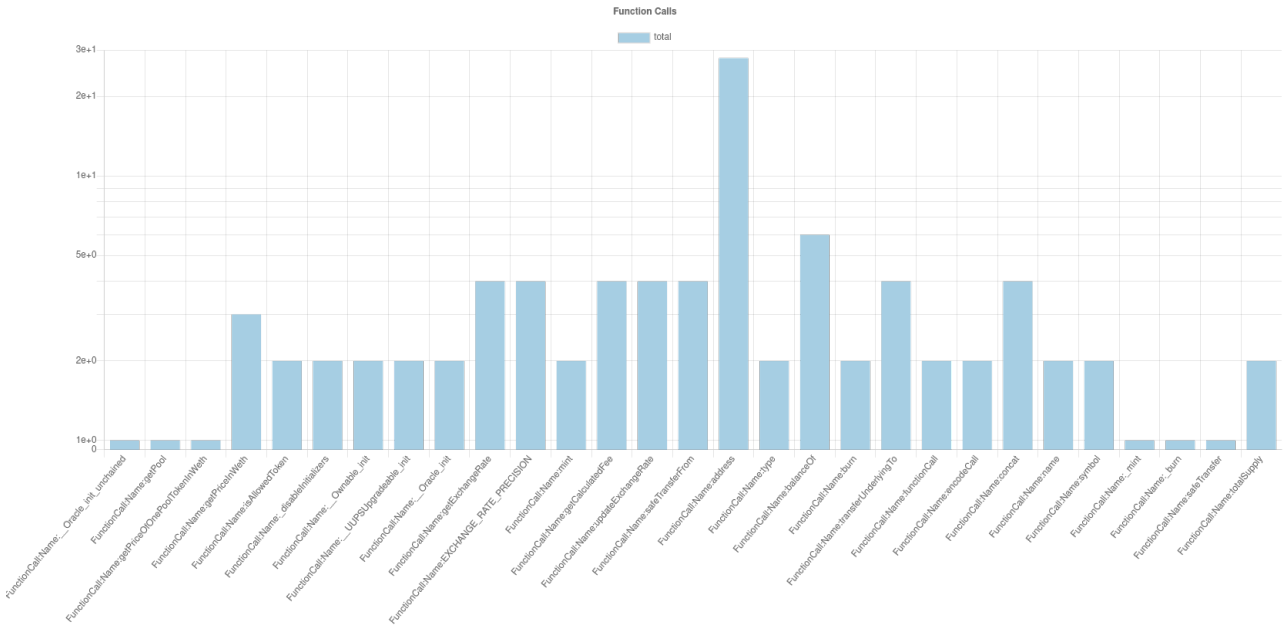
Totals

Summary

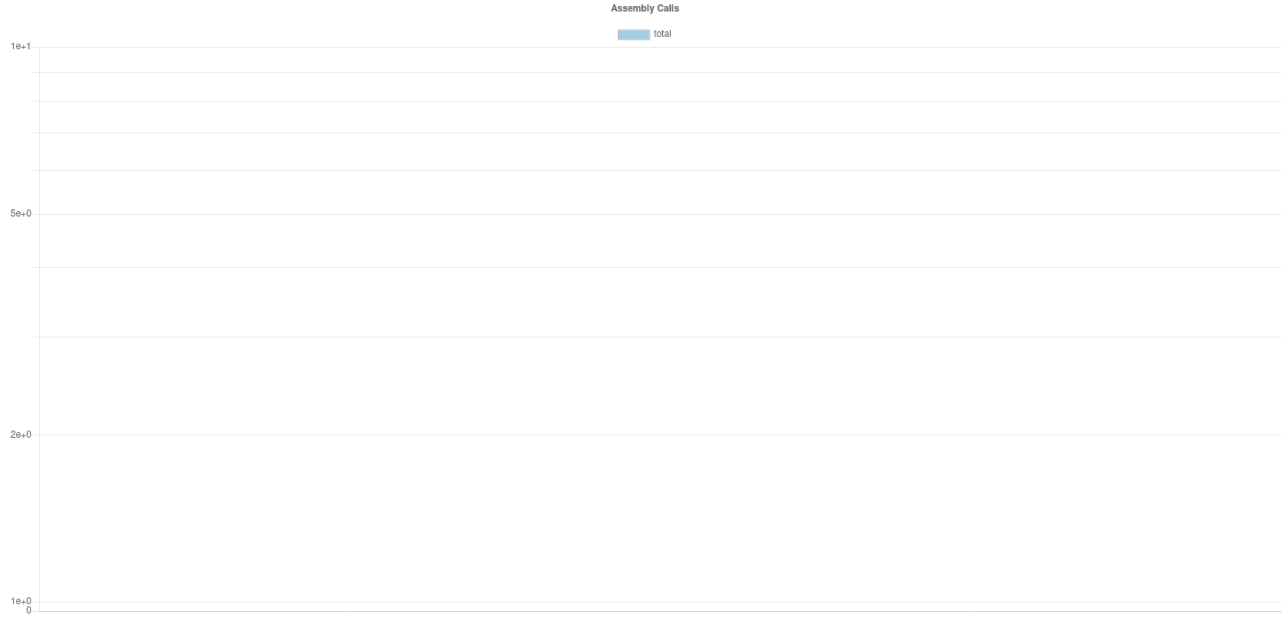


AST Node Statistics

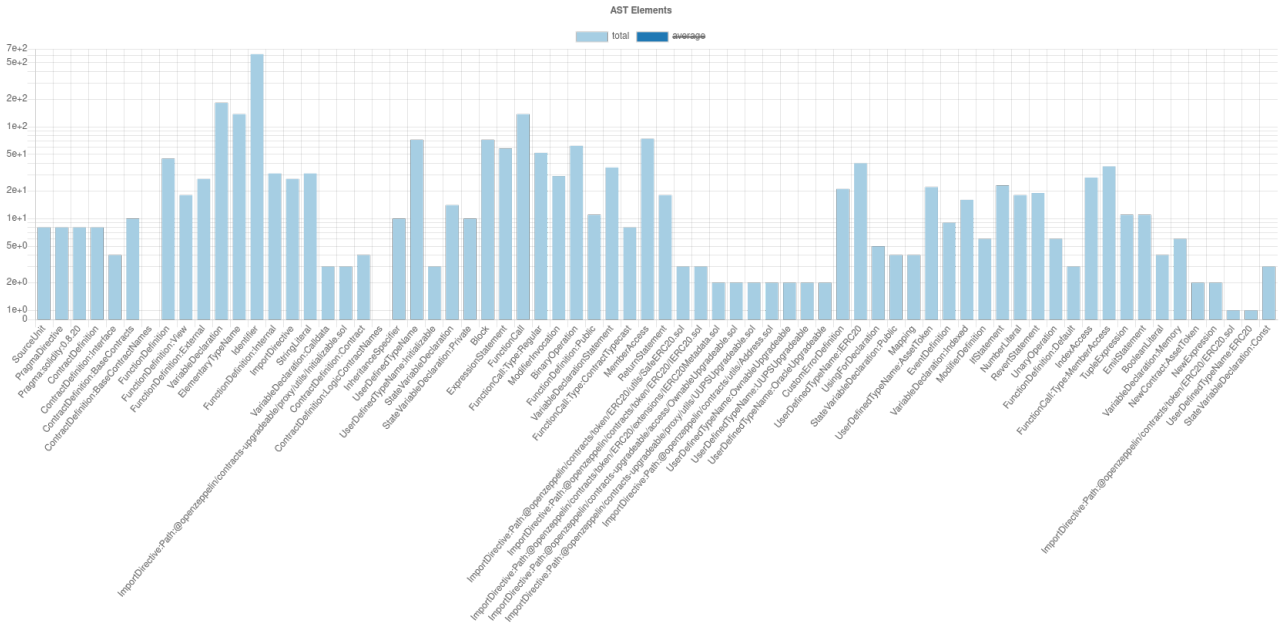
Function Calls



Assembly Calls

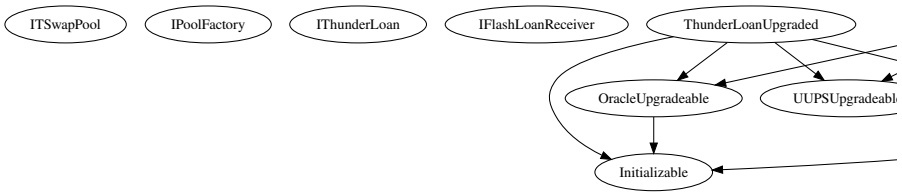


AST Total



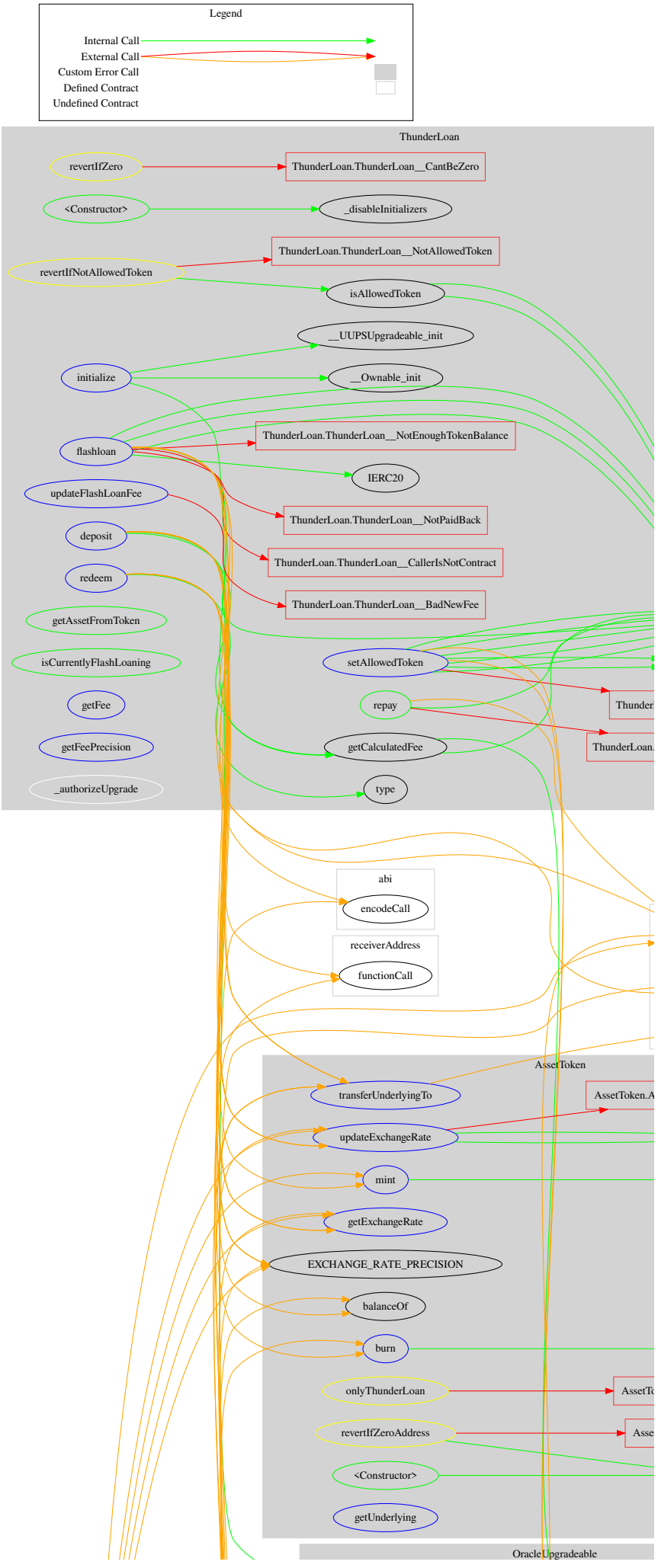
Inheritance Graph

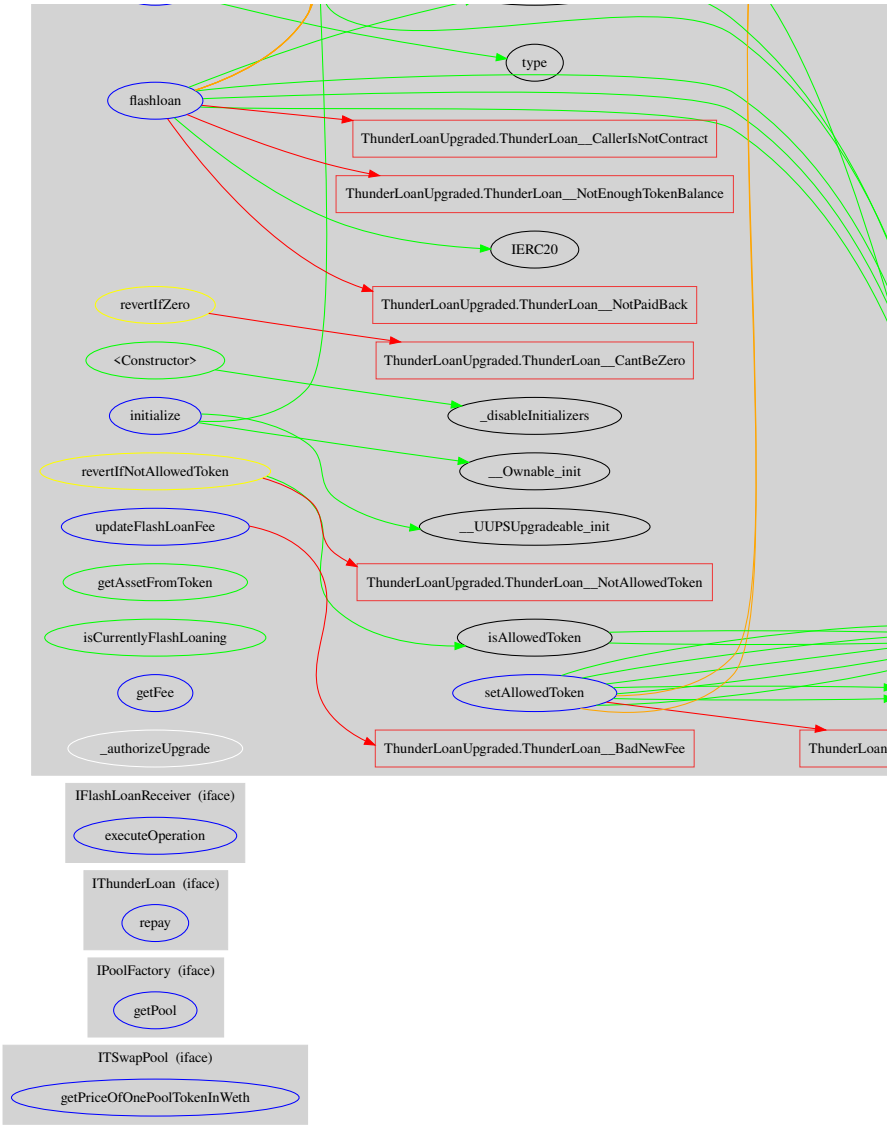
[➖]



CallGraph

[➖]


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
ThunderLoan
revertIfZero
ThunderLoan.ThunderLoan__CantBeZero
<Constructor>
_disableInitializers
ThunderLoan.ThunderLoan__NotAllowedToken
revertIfNotAllowedToken
isAllowedToken
__UUPSUpgradeable_init
initialize
__Ownable_init
ThunderLoan.ThunderLoan__NotEnoughTokenBalance
flashloan
IERC20
updateFlashLoanFee
ThunderLoan.ThunderLoan__NotPaidBack
deposit
ThunderLoan.ThunderLoan__CallerIsNotContract
redeem
ThunderLoan.ThunderLoan__BadNewFee
getAssetFromToken
isCurrentlyFlashLoaning
setAllowedToken
repay
getFee
getFeePrecision
getCalculatedFee
_authorizeUpgrade
type
abi
encodeCall
receiverAddress
functionCall
AssetToken
transferUnderlyingTo
updateExchangeRate
mint
getExchangeRate
EXCHANGE_RATE_PRECISION
balanceOf
burn
onlyThunderLoan
revertIfZeroAddress
<Constructor>
getUnderlying
OracleUpgradeable



Contract Summary

[➖]

Files Description Table

File Name	SHA-1 Hash
src/interfaces/ITSwapPool.sol	4e149e38fec54f837e35d376c3015ba13e5fd753
src/interfaces/IPoolFactory.sol	489f639fb9212a413e53369cf9a15f82e696da12
src/interfaces/IThunderLoan.sol	cda5f9f2e87e20802542339a5434f8cb6bab0472
src/interfaces/IFlashLoanReceiver.sol	ed29a80d39ee95dc3d7249b71ded9addf356d725
src/protocol/OracleUpgradeable.sol	8ed0a9b120e96c5b7bafb857705b6bef458f54d2
src/protocol/ThunderLoan.sol	64ceb5b0e8ecfa992b33c82a4d0f634bf7b58a43
src/protocol/AssetToken.sol	0a173de7b044f0561af60fda7a44a97629a5ac67
src/upgradedProtocol/ThunderLoanUpgraded.sol	de4ad4e345e0c2a51e27765bea04f383a60ccf2a

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
ITSwapPool	Interface			
└	getPriceOfOnePoolTokenInWeth	External ❗		NO ❗
IPoolFactory	Interface			

Contract	Type	Bases		
└	getPool	External ❗		NO ❗
IThunderLoan	Interface			
└	repay	External ❗	🛑	NO ❗
IFlashLoanReceiver	Interface			
└	executeOperation	External ❗	🛑	NO ❗
OracleUpgradeable	Implementation	Initializable		
└	*Oracle*init	Internal 🔒	🛑	onlyInitializing
└	*Oracle*init_unchained	Internal 🔒	🛑	onlyInitializing
└	getPriceInWeth	Public ❗		NO ❗
└	getPrice	External ❗		NO ❗
└	getPoolFactoryAddress	External ❗		NO ❗
ThunderLoan	Implementation	Initializable, OwnableUpgradeable, UUPSUpgradeable, OracleUpgradeable		
└		Public ❗	🛑	NO ❗
└	initialize	External ❗	🛑	initializer
└	deposit	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	redeem	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	flashloan	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	repay	Public ❗	🛑	NO ❗
└	setAllowedToken	External ❗	🛑	onlyOwner
└	getCalculatedFee	Public ❗		NO ❗
└	updateFlashLoanFee	External ❗	🛑	onlyOwner
└	isAllowedToken	Public ❗		NO ❗
└	getAssetFromToken	Public ❗		NO ❗
└	isCurrentlyFlashLoaning	Public ❗		NO ❗
└	getFee	External ❗		NO ❗
└	getFeePrecision	External ❗		NO ❗
└	_authorizeUpgrade	Internal 🔒	🛑	onlyOwner
AssetToken	Implementation	ERC20		
└		Public ❗	🛑	ERC20 revertIfZeroAddress revertIfZeroAddress
└	mint	External ❗	🛑	onlyThunderLoan
└	burn	External ❗	🛑	onlyThunderLoan
└	transferUnderlyingTo	External ❗	🛑	onlyThunderLoan
└	updateExchangeRate	External ❗	🛑	onlyThunderLoan
└	getExchangeRate	External ❗		NO ❗
└	getUnderlying	External ❗		NO ❗
ThunderLoanUpgraded	Implementation	Initializable, OwnableUpgradeable, UUPSUpgradeable, OracleUpgradeable		
└		Public ❗	🛑	NO ❗
└	initialize	External ❗	🛑	initializer
└	deposit	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	redeem	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	flashloan	External ❗	🛑	revertIfZero revertIfNotAllowedToken
└	repay	Public ❗	🛑	NO ❗
└	setAllowedToken	External ❗	🛑	onlyOwner
└	getCalculatedFee	Public ❗		NO ❗
└	updateFlashLoanFee	External ❗	🛑	onlyOwner
└	isAllowedToken	Public ❗		NO ❗
└	getAssetFromToken	Public ❗		NO ❗
└	isCurrentlyFlashLoaning	Public ❗		NO ❗
└	getFee	External ❗		NO ❗
└	_authorizeUpgrade	Internal 🔒	🛑	onlyOwner

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Thinking about smart contract security? We can provide training, ongoing advice, and smart contract auditing. Contact us.