



**SOLID**Proof  
*Bring trust into your projects*

**Blockchain Security | Smart Contract Audits | KYC  
Development | Marketing**

MADE IN GERMANY

# Unicrypt

-

## V2 ENMT TaxToken

# Audit

**Security Assessment**  
**22. June, 2023**

**For**



**UNICRYPT**®  
N E T W O R K



**SolidProof\_io**



**@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	26
Source Units in Scope	34
Critical issues	36
High issues	36
Medium issues	36
Low issues	36
Informational issues	37
Audit Comments	40
SWC Attacks	41

# 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	15. October 2022	<ul style="list-style-type: none"><li>• Layout project</li><li>• Automated-Security Testing</li></ul>
	16.-17. October 2022	<ul style="list-style-type: none"><li>• Code review</li><li>• Manual-Security Testing</li></ul>
	18.-19. October 2022	<ul style="list-style-type: none"><li>• Finishing audit</li></ul>
1.1	14. - 15. November 2022	<ul style="list-style-type: none"><li>• Reaudit</li></ul>
1.2	09. December 2022	<ul style="list-style-type: none"><li>• Small updates review</li><li>• Updating report</li></ul>
1.3	13. - 15. March 2023	<ul style="list-style-type: none"><li>• Reaudit</li></ul>
	22. June 2023	<ul style="list-style-type: none"><li>• All issues have been acknowledged by the unicrypt team</li></ul>

## **Network**

Ethereum (ERC20)

## **Website**

<https://unicrypt.network/>

## **Telegram**

[https://t.me/uncx\\_token](https://t.me/uncx_token)

## **Twitter**

[https://twitter.com/UNCX\\_token](https://twitter.com/UNCX_token)

## **Medium**

<https://unicrypt.medium.com/>



## Description

TBA

## Project Engagement

During the 12th of October 2022, **Unicrypt 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

v1.3

• TBA

# 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)
<b>Critical</b>	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.
<b>High</b>	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.
<b>Medium</b>	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.
<b>Low</b>	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.
<b>Informational</b>	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
@uniswap/lib/contracts/libraries/TransferHelper.sol	4
@uniswap/v2-core/contracts/interfaces/IUniswapV2Callee.sol	1
@uniswap/v2-core/contracts/interfaces/IUniswapV2Factory.sol	6
@uniswap/v2-core/contracts/interfaces/IUniswapV2Pair.sol	6
hardhat/console.sol	5



# Tested Contract Files

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

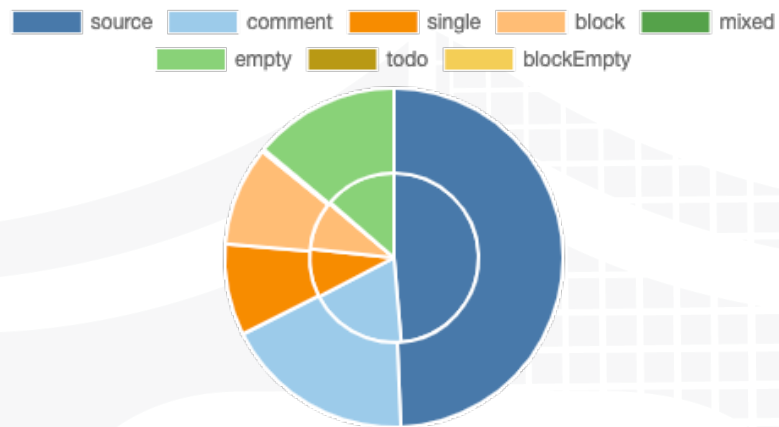
*A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.*

## v1.3

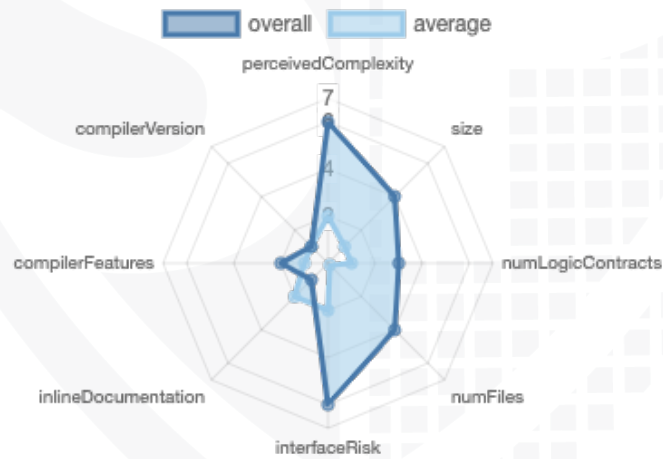
File Name	SHA-1 Hash
contracts/facets/AntiBot.sol	98ad58a80bb0aaf2871f1e7001735de9f27949fe
contracts/BuyBackWallet.sol	31173a0f571e96f03028569d7960e7c341e7f335
contracts/facets/Tax.sol	a3b7554e0c64b58262bbad573775226bffe7dac5
contracts/facets/Constructor.sol	c377f635835740d618b020c2e720058dfa4df6c7
contracts/facets/Storage.sol	f3d2da9616f81464aaa0a007eb93c4394342fa3a
contracts/facets/Multicall.sol	c2ff3f5f4ea08aa9f47026b4fb83213f980bd905
contracts/facets/Lossless.sol	b6180eccf843e7c1e7f838f35a5e9714817e5e25
contracts/facets/Wallets.sol	aef7deec00a0d0c6562e1d2051c307a41f188486
contracts/facets/Settings.sol	7ff8c5eb9e27f736014b1d9c644cd0098f291d56
contracts/FacetHelper.sol	a9c6306e0212bde84c83dc7ffd25bf7dd7cdc08
contracts/TaxToken.sol	77e18f1e36bf483414c2469e3dfe3b2a2a39738
contracts/FeeHelper.sol	9648534df6a81f7e93b3e5dce724b6cf8b5809f2
contracts/MintGenerator.sol	de2e4e76438e80c4e248e046cc81ce78bad5ed84
contracts/MintFactory.sol	66f7f112a50c505500330e32c8fc76d2830b45f3
contracts/TaxHelperUniswapV2.sol	8c40c9cbd233b6c5d23cb65165d26b8940c68560
contracts/LPWallet.sol	b835b362c0bfdcd40fbeb8187e9f346a5ad6e3b6
contracts/interfaces/IERC20.sol	4f02a422b8d0ebe0d3c2bc02461bbbc034286d5b
contracts/interfaces/ILosslessController.sol	d5a753d5bfc5598f8013c1c246ba37fe542508ae
contracts/interfaces/IFacetHelper.sol	a9a7f19c5d8439dd6daa4ce46d26b5a3cd87171b
contracts/interfaces/IUniswapV2Pair.sol	ccd8036e1ef9d2430f46a45fa801fc625dd80d8e
contracts/libraries/FullMath.sol	31b683e9e7e70a069d84e392c81093ddbc345b57
contracts/libraries/Context.sol	4465015f0682ad5930d21821c9d58be709195bfc
contracts/libraries/EnumerableSet.sol	9cdc08ba9455c2127e7c5d5651a036baab76f2c2
contracts/interfaces/IUniswapV2Factory.sol	a5d78edcba4e2228f92a4a0df03190c12d869184
contracts/libraries/Ownable.sol	0510660ea05a9ff29d6c9b87a4166c7a4eed2f8
contracts/libraries/Pausable.sol	b9ec1611b977ebcc3120e85cc10768dd192a7c78
contracts/libraries/ERC20.sol	68259afa71414e00c0afbe20cde382b556db6699
contracts/interfaces/IBuyBackWallet.sol	5df276446174391d0b00c2a7d25698d6441be04d
contracts/interfaces/ITaxToken.sol	e25accb168f50f19cd0fd6579b47caceb5ca6c50
contracts/interfaces/ILPWallet.sol	7c35ba43f899da2cf0345b3311b9bae5b65fa019
contracts/interfaces/IFeeHelper.sol	b565b226d1a2e5f80a78f5ac982e6a1d818398ac
contracts/interfaces/ISettings.sol	f76d561e54e059bd8c499fdaea6ac69307809aea
contracts/interfaces/IUniswapV2Router02.sol	9b9f4c23ac1e66692519984e3d449605afa8a3bc
contracts/interfaces/IUniswapV2Router01.sol	fc9a0f0007cb1ba6c3f8f3e63f0fa6280d4459d4
contracts/interfaces/IWallets.sol	824e9e9be847aec317932f57e63da03b842c80e4
contracts/interfaces/ITaxHelper.sol	f95d7952b05ae9588189c0195309df3f3eb80755
contracts/interfaces/IMintFactory.sol	b2f2e3a08a9e5431748dbe79ff3e03ab87c369b6

# Metrics

## Source Lines v1.3



## Risk Level v1.3



## Capabilities

### Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	16	2	15	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.*

Version	Public	Payable
1.0	330	9

Version	External	Internal	Private	Pure	View
1.0	191	252	18	13	181

### State Variables

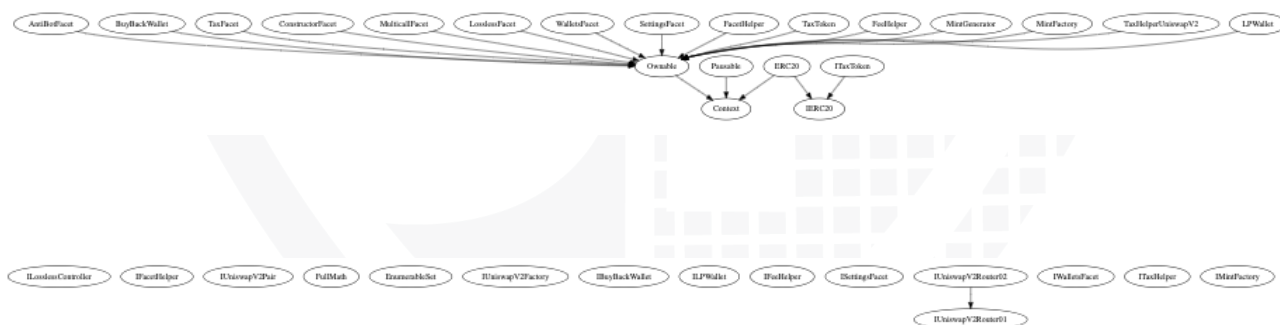
Version	Total	Public
1.0	41	9

### Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	0.8.17 ≥0.5.0 ≥0.6.2		yes	yes (11 asm blocks)	

Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	EC Recover	New/Create/Create2
1.0	yes		yes	yes		yes → NewContract:BuyBackWallet → NewContract:LPWallet → NewContract:TaxToken

## Inheritance Graph v1.3



CallGraph  
v1.3



## 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. Deployer cannot set fees
7. Deployer cannot blacklist/antisnipe addresses
8. Overall checkup (Smart Contract Security)



## Is contract an upgradeable

Name	
Is contract an upgradeable?	Yes

Comments:

### v1.0

- Since this contract is based on the diamond-3 pattern of Nick Mudge (For more information visit: <https://eips.ethereum.org/EIPS/eip-2535>, <https://github.com/mudgen/diamond-3>) parts of the project can be replaced by the owner. The team can also implement new functionalities after the deployment.

## Correct implementation of Token standard

ERC20				
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	✓	✓	✓



ERC721				
Function	Description	Exist	Tested	Verified
BalanceOf	Count all NFTs assigned to an owner	✓	✓	✓
OwnerOf	Find the owner of an NFT	✓	✓	✓
SafeTransferFrom	Transfers the ownership of an NFT from one address to another address	✓	✓	✓
SafeTransferFrom	See above - Difference is that this function has an extra data parameter	✓	✓	✓
TransferFrom	Transfer ownership of an NFT	✓	✓	✓
Approve	Change or reaffirm the approved address for an NFT	✓	✓	✓
SetApprovalForAll	Enable or disable approval for a third party ("operator") to manage all of `msg.sender`'s assets	✓	✓	✓
GetApproved	Get the approved address for a single NFT	✓	✓	✓
IsApprovedForAll	Query if an address is an authorized operator for another address	✓	✓	✓
SupportsInterface	Query if a contract implements an interface	✓	✓	✓
Name	Provides information about the name	✓	✓	✓
Symbol	Provides information about the symbol	✓	✓	✓
TokenURI	Provides information about the TokenUri	✓	✓	✓

## Write functions of contract v1.0

### AntiBot

```
setIncrement  
setEndDate  
setInitialMaxHold  
updateAntiBot  
antiBotCheck  
addMaxBalanceWhitelistedAddress  
removeMaxBalanceWhitelistedAddress  
updateMaxBalanceWhitelistBatch  
updateMaxBalanceAfterBuy  
addSwapWhitelistedAddress  
removeSwapWhitelistedAddress  
updateSwapWhitelistBatch  
setSwapWhitelistEndDate  
updateSwapWhitelisting  
swapWhitelistingCheck
```

### Constructor

```
constructorHandler
```

### Lossless

```
setLosslessAdmin  
transferRecoveryAdminOwnership  
acceptRecoveryAdminOwnership  
proposeLosslessTurnOff  
executeLosslessTurnOff  
executeLosslessTurnOn
```

### ERC20

```
transfer  
approve  
transferFrom  
increaseAllowance  
decreaseAllowance
```

### Ownable

```
renounceOwnership  
transferOwnership
```

### BuyBackWallet

```
sendEthToTaxHelper  
updateThreshold
```

### FacetHelper

```
addFacet  
addSelector  
removeSelector  
resetFacetStorage  
updateSettingsFacet  
updateLosslessFacet  
updateTaxFacet  
updateConstructorFacet  
updateWalletsFacet  
updateAntiBotFacet  
updateMulticallFacet
```

## Multicall

**multicallAdminUpdate**  
**multicallAntiBotUpdate**

## FeeHelper

**setGeneratorFee**  
**setFee**  
**setFeeAddress**

## Settings

**addLPToken**  
**removeLPToken**  
**togglePause**  
**addBlacklistedAddress**  
**removeBlacklistedAddress**  
**updateBlacklistBatch**  
**updateCustomTaxes**  
**updateTaxFees**  
**updateTransactionTaxAddress**  
**lockSettings**  
**updateSettings**  
**updatePairAddress**  
**updateTaxHelperIndex**

## LPWallet

**sendEthToTaxHelper**  
**transferBalanceToTaxHelper**  
**updateThreshold**

## MintFactory

**adminAllowTokenGenerator**  
**addTaxHelper**  
**updateTaxHelper**  
**registerToken**  
**updateFacetHelper**  
**updateFeeHelper**  
**updateLosslessController**

## MintGenerator

**createToken** 💰

## Tax

**handleTaxes**  
**\_transfer**  
**reflect**  
**excludeAccount**  
**includeAccount**  
**mint**  
**burn**

## TaxHelperUniswapV2

**initiateBuyBackTax** 💰  
**initiateLPTokenTax**  
**createLPToken**

## TaxToken

**transferOutBlacklistedFunds**  
**buyBackBurn**  
**transfer**  
**approve**  
**transferFrom**  
**increaseAllowance**  
**decreaseAllowance**

## Wallets

**createBuyBackWallet**  
**createLPWallet**  
**updateBuyBackWalletThreshold**  
**updateLPWalletThreshold**

## Deployer cannot mint any new tokens

Name	Exist	Tested	Status
Deployer cannot mint	✓	✓	✗

Comments:

**v1.0**

- Owner can mint new tokens



## Deployer cannot burn or lock user funds

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

Comments:

### v1.0

- Owner can lock user funds by
  - blacklisting addresses
  - Settings fees too high
- Tokens
  - can be burned by the owner
  - can be burned by msg.sender
  - Will be burned in the "initialBuyBackTax" function in the TaxHelperUniswapV2 contract L41

## Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	✓	✓	✗

Comments:

**v1.0**

- Owner can pause contract



## Deployer cannot set fees

Name	Exist	Tested	Status
Deployer cannot set fees over 25%	✓	✓	✗
Deployer cannot set fees to nearly 100% or to 100%	✓	✓	✗

Comments:

**v1.0**

- FeeHelper
  - Fees can be set without any limitations

## Deployer can blacklist/antisnipe addresses

Name	Exist	Tested	Status
Deployer cannot blacklist/antisnipe addresses	✓	✓	✗

Comments:

**v1.0**

- Only contracts can be blacklisted





## 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

## Lossless

- ✓  **setLosslessAdmin**
  - Ⓜ onlyRecoveryAdmin
- ✓  **transferRecoveryAdminOwnership**
  - Ⓜ onlyRecoveryAdmin
-  **acceptRecoveryAdminOwnership**
- ✓  **proposeLosslessTurnOff**
  - Ⓜ onlyRecoveryAdmin
- ✓  **executeLosslessTurnOff**
  - Ⓜ onlyRecoveryAdmin
- ✓  **executeLosslessTurnOn**
  - Ⓜ onlyRecoveryAdmin





## MintFactory

- ✓  **adminAllowTokenGenerator**
  - Ⓜ onlyOwner
- ✓  **addTaxHelper**
  - Ⓜ onlyOwner
- ✓  **updateTaxHelper**
  - Ⓜ onlyOwner
-  **registerToken**
- ✓  **updateFacetHelper**
  - Ⓜ onlyOwner
- ✓  **updateFeeHelper**
  - Ⓜ onlyOwner
- ✓  **updateLosslessController**
  - Ⓜ onlyOwner








## MintGenerator

-  **createToken** 

## TaxHelperUniswapV2

- ✓  **initiateBuyBackTax** 
  - Ⓜ isToken
- ✓  **initiateLPTokenTax**
  - Ⓜ isToken
-  **createLPToken**

## TaxToken

-  **transferOutBlacklistedFunds**
-  **buyBackBurn**
-  **transfer**
-  **approve**
-  **transferFrom**
-  **increaseAllowance**
-  **decreaseAllowance**

## AntiBot

## Settings

<ul style="list-style-type: none"> <li>setIncrement <ul style="list-style-type: none"> <li>onlyOwner</li> <li>antiBotsActive</li> </ul> </li> <li>setEndDate <ul style="list-style-type: none"> <li>onlyOwner</li> <li>antiBotsActive</li> </ul> </li> <li>setInitialMaxHold <ul style="list-style-type: none"> <li>onlyOwner</li> <li>antiBotsActive</li> </ul> </li> <li>updateAntiBot <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>antiBotCheck</li> <li>addMaxBalanceWhitelistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>removeMaxBalanceWhitelistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateMaxBalanceWhitelistBatch <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateMaxBalanceAfterBuy <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>addSwapWhitelistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>removeSwapWhitelistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateSwapWhitelistBatch <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>setSwapWhitelistEndDate <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateSwapWhitelisting <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>swapWhitelistingCheck</li> </ul>	<ul style="list-style-type: none"> <li>addLPToken <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>removeLPToken <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>togglePause <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>addBlacklistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> <li>canBlacklist</li> </ul> </li> <li>removeBlacklistedAddress <ul style="list-style-type: none"> <li>onlyOwner</li> <li>canBlacklist</li> </ul> </li> <li>updateBlacklistBatch <ul style="list-style-type: none"> <li>onlyOwner</li> <li>canBlacklist</li> </ul> </li> <li>updateCustomTaxes <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateTaxFees <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateTransactionTaxAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>lockSettings <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateSettings <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updatePairAddress <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> <li>updateTaxHelperIndex <ul style="list-style-type: none"> <li>onlyOwner</li> </ul> </li> </ul>
---	--

## FacetHelper

▼ 🔹 **addFacet**

🔒 onlyOwner

▼ 🔹 **addSelector**

🔒 onlyOwner

▼ 🔹 **removeSelector**

🔒 onlyOwner

▼ 🔹 **resetFacetStorage**

🔒 onlyOwner

▼ 🔹 **updateSettingsFacet**

🔒 onlyOwner

▼ 🔹 **updateLosslessFacet**

🔒 onlyOwner

▼ 🔹 **updateTaxFacet**

🔒 onlyOwner

▼ 🔹 **updateConstructorFacet**

🔒 onlyOwner

▼ 🔹 **updateWalletsFacet**

🔒 onlyOwner

▼ 🔹 **updateAntiBotFacet**

🔒 onlyOwner

▼ 🔹 **updateMulticallFacet**

🔒 onlyOwner

▼ 🔹 **handleTaxes**

▼ 🔹 **\_transfer**

▼ 🔹 **reflect**

▼ 🔹 **excludeAccount**

🔒 onlyOwner

▼ 🔹 **includeAccount**

🔒 onlyOwner

▼ 🔹 **mint**

🔒 onlyOwner

▼ 🔹 **burn**

## Constructor

▼ 🔹 **constructorHandler**

## Multicall

▼ 🔹 **multicallAdminUpdate**

🔒 onlyOwner

▼ 🔹 **multicallAntiBotUpdate**

🔒 onlyOwner

## Wallets

```
createBuyBackWallet
createLPWallet
updateBuyBackWalletThreshold
  onlyOwner
updateLPWalletThreshold
  onlyOwner
```

### BuyBackWallet

```
sendEthToTaxHelper
updateThreshold
  onlyOwner
```

### FeeHelper

```
setGeneratorFee
  onlyOwner
setFee
  onlyOwner
setFeeAddress
  onlyOwner
```

### LPWallet

```
sendEthToTaxHelper
transferBalanceToTaxHelper
updateThreshold
  onlyOwner
```

## Comments

- Deployer can set following state variables without any limitations
  - **AntiBot**
    - maxBalanceAfterBuy
    - antiBotSettings.initialMaxHold
    - antiBotSettings.increment
  - **Multicall**
    - fees.transactionTax.buy
    - fees.transactionTax.sell

- fees.buyBackTax
    - fees.holderTax
    - fees.lpTax
    - antiBotSettings.increment
    - antiBotSettings.initialMaxHold
  - **Settings**
    - taxHelperIndex
      - Max to  $2^8 - 1$
  - **BuyBackWallet**
    - threshold
  - **FacetHelper**
    - isFacet
    - facetsList
    - selectorToFacet
    - selectorsList
  - **FeeHelper**
    - SETTINGS.FEE
    - SETTINGS.GENERATOR\_FEE
  - **LPWallet**
    - threshold
    -
- Deployer can enable/disable following state variables
- **AntiBot**
    - swapWhitelistingSettings.isActive
    - antiBotSettings.isActive
    - swapWhitelistlist
    - maxBalanceWhitelistlist
  - **Lossless**
    - isLosslessTurnOffProposed
    - isLosslessOn
  - **Multicall**
    - taxSettings.transactionTax
    - taxSettings.holderTax
    - taxSettings.buyBackTax
    - taxSettings.lpTax
    - taxSettings.canMint
    - taxSettings.canPause
    - taxSettings.canBlacklist
    - taxSettings.maxBalanceAfterBuy
    - isLocked.transactionTax
    - isLocked.holderTax
    - isLocked.buyBackTax
    - isLocked.lpTax

- isLocked.canMint
  - isLocked.canPause
  - isLocked.canBlacklist
  - isLocked.maxBalanceAfterBuy
  - antiBotSettings.isActive
  - swapWhitelistingSettings.isActive
- **Settings**
  - taxSettings.transactionTax
  - taxSettings.holderTax
  - taxSettings.buyBackTax
  - taxSettings.lpTax
  - taxSettings.canMint
  - taxSettings.canPause
  - taxSettings.canBlacklist
  - taxSettings.maxBalanceAfterBuy
  - isLocked.transactionTax
  - isLocked.holderTax
  - isLocked.buyBackTax
  - isLocked.lpTax
  - isLocked.canMint
  - isLocked.canPause
  - isLocked.canBlacklist
  - isLocked.maxBalanceAfterBuy
  - blacklist
  - isPaused
  - lpTokens
- **Tax**
  - \_isExcluded
  - \_excluded
- Deployer can set following addresses/string
  - **Lossless**
    - recoveryAdmin
    - recoveryAdminCandidate
    - recoveryAdminKeyHash
    - admin
  - **Settings**
    - pairAddress
    - transactionTaxWallet
  - **FacetHelper**
    - facets.Multicall
    - facets.AntiBot
    - facets.Wallets
    - facets.Constructor

- facets.Settings
  - facets.Lossless
  - facets.Tax
- **FeeHelper**
  - SETTINGS.FEE\_ADDRESS
- **MintFactory**
  - LosslessController
  - FeeHelper
  - FacetHelper
  - taxHelpersData.Address
  - taxHelpers
  - tokenGenerators
- Existing Modifiers
  - **TaxHelperUniswapV2**
    - isToken
  - **Antibot**
    - antiBotIsActive
  - **Lossless**
    - onlyRecoveryAdmin
  - **Settings**
    - canBlacklist
  - **Ownable**
    - onlyOwner
  - **Pausable**
    - whenNotPaused
    - whenPaused
- The project is a diamond-3 structured. That means, that the owner can upgrade contracts on the fly.
- Tax
  - Owner can mint new tokens
- Wallets
  - Anybody is able to call “createBuyBackWallet” and “createLPWallet”
    - This function returns only the address of the new created wallets but it will not set a state variable in the storage
  - Owner can update buyback/lp wallets from the facet
- MintFactory
  - Can add new taxHelper
- FacetHelper
  - Owner can reset facet storage and remove all selector and facet list






















































**Please check if an OnlyOwner or similar restrictive modifier has been forgotten.**



# Source Units in Scope

## v1.3

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/facets/AntiBot.sol	1	————	184	184	144	7	111	————
	contracts/BuyBackWallet.sol	1	————	63	63	43	3	36	
	contracts/facets/Tax.sol	1	————	353	353	281	23	175	————
	contracts/facets/Constructor.sol	1	————	188	188	165	9	95	————
	contracts/facets/Storage.sol	————	————	310	310	89	142	————	————
	contracts/facets/Multicall.sol	1	————	200	200	157	13	76	————
	contracts/facets/Lossless.sol	1	————	76	76	56	4	42	
	contracts/facets/Wallets.sol	1	————	48	48	32	3	48	
	contracts/facets/Settings.sol	1	————	226	226	190	4	131	————
	contracts/FacetHelper.sol	1	————	346	327	199	82	151	
	contracts/TaxToken.sol	1	————	499	499	382	31	360	
	contracts/FeeHelper.sol	1	————	55	55	38	3	22	————
	contracts/MintGenerator.sol	1	————	47	45	22	8	34	
	contracts/MintFactory.sol	1	————	181	181	109	35	84	————
	contracts/TaxHelperUniswapV2.sol	1	————	116	116	92	6	107	
	contracts/LPWallet.sol	1	————	74	74	51	3	45	
	contracts/interfaces/IERC20.sol	————	1	79	28	17	58	13	
	contracts/interfaces/ILosslessController.sol	————	1	24	7	3	1	25	————
	contracts/interfaces/IFacetHelper.sol	————	1	70	17	7	17	39	————
	contracts/interfaces/IUniswapV2Pair.sol	————	1	52	7	5	————	55	————
	contracts/libraries/FulMath.sol	1	————	126	118	57	59	104	
	contracts/libraries/Context.sol	1	————	26	26	10	13	1	————
	contracts/libraries/EnumerableSet.sol	1	————	357	357	118	196	49	
	contracts/interfaces/IUniswapV2Factory.sol	————	1	17	6	4	————	17	————
	contracts/libraries/Ownable.sol	1	————	70	70	27	34	24	————
	contracts/libraries/Pausable.sol	1	————	91	91	29	51	16	————
	contracts/libraries/ERC20.sol	1	————	305	305	90	179	73	————
	contracts/interfaces/IBuyBackWallet.sol	————	1	19	10	3	3	11	————
	contracts/interfaces/ITaxToken.sol	————	1	19	12	4	3	9	————
	contracts/interfaces/ILPWallet.sol	————	1	21	10	3	3	13	————
	contracts/interfaces/IFeeHelper.sol	————	1	22	9	3	3	15	————
	contracts/interfaces/ISettings.sol	————	1	13	10	3	3	7	————
	contracts/interfaces/IUniswapV2Router02.sol	————	1	44	6	4	————	16	
	contracts/interfaces/IUniswapV2Router01.sol	————	1	95	4	3	————	48	
	contracts/interfaces/IWallets.sol	————	1	16	10	3	3	9	————
	contracts/interfaces/TaxHelper.sol	————	1	23	10	3	3	9	————
	contracts/interfaces/IMintFactory.sol	————	1	43	16	8	3	29	————
	Totals	21	15	4498	4074	2454	1008	2099	

## Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalised lines of the source unit (e.g. normalises functions spanning multiple lines)
nSLOC	normalised 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

## Critical issues

**No critical issues**

## High issues

**No high issues**

## Medium issues

**No medium issues**

## Low issues

**Low issues acknowledged**

Issue	File	Type	Line	Description	Status
#1	TaxHelperUniswapV2	Missing Zero Address Validation (missing-zero-check)	69, 70	Check that the address is not zero	Acknowledged
#2	TaxToken	Missing Zero Address Validation (missing-zero-check)	59	Check that the address is not zero	Acknowledged
#3	Settings	Missing Zero Address Validation (missing-zero-check)	219	Check that the address is not zero	Acknowledged
#4	UniswapV2Router02	Missing Zero Address Validation (missing-zero-check)	25, 27	Check that the address is not zero	Acknowledged

#5	UniswapV2Router01	Missing Zero Address Validation (missing-zero-check)	21, 22	Check that the address is not zero	Acknowledged
#6	TaxHelperUniswapV2	State variable visibility is not set	23-25	It is best practice to set the visibility of state variables explicitly	Acknowledged
#7	Multicall	Variable is not defined	137-140	Make sure to check whether s.lpWallet is set before calling updateThreshold of it.	Acknowledged
#8	Multicall	Missing parameter in the MulticallAdminUpdateParams	32	The multicall struct does not have a property for the lp wallet and buy back wallet.  See Issue one line above	Acknowledged

## Informational issues

### Informational issues acknowledged

Issue	File	Type	Line	Description	Status
#1	LPWallet	Error message is missing	55	Provide an error message for require statement	Acknowledged
#2	MintFactory	Error message is missing	157, 167, 177	Provide an error message for require statement	Acknowledged
#3	Settings	Error message is missing	95, 129	Provide an error message for require statement	Acknowledged
#4	AntiBot	Error message is missing	65, 120	Provide an error message for require statement	Acknowledged
#5	Constructor	Error message is missing	114	Provide an error message for require statement	Acknowledged
#6	Tax	Error message is missing	56, 145	Provide an error message for require statement	Acknowledged

#7	FullM ath	Error message is missing	34, 43, 122	Provide an error message for require statement	Ackno wledge d
#8	All	NatSpec documentation missing	-	If you started to comment your code, also comment all other functions, variables etc.	Ackno wledge d
#9	Lossl ess	Set recoveryAdminC andidate to address zero after accepting	50	Don't forget to set the "recoveryAdminCandidate" to address zero after accepting the ownership	Ackno wledge d
#10	AntiB ot	Visibility first	32	The visibility modifier "internal" should come before other modifiers. We recommend you to put internal before the view key here.	Ackno wledge d
#11	IUnis wapV 2Fact ory	SPDX License is missing	See descripti on	Add a SPDX License at the top of source file	Ackno wledge d
#12	IUnis wapV 2Pair	SPDX License is missing	See descripti on	Add a SPDX License at the top of source file	Ackno wledge d
#13	IUnis wapV 2Rou ter01	SPDX License is missing	See descripti on	Add a SPDX License at the top of source file	Ackno wledge d
#14	IUnis wapV 2Rou ter02	SPDX License is missing	See descripti on	Add a SPDX License at the top of source file	Ackno wledge d

## Acknowledged by Unicrypt team

### Low Issues

**#1-#2:** These checks are not needed, as the addresses are all defined by the Unicrypt team previously.

**#3:** UpdatePairAddress could potentially use a check, but we check on the front end already. Also, the Pair address is set to zero address on arbitrum using camelot, and then updated immediately after. No check is needed in this case.

**#4-#5:** Uniswap router is not our code, this was only used for local testing.

**#6:** Doesn't change anything, addressed..

**#7-#8:** These variables are all defined and used upon token creation.

### Informational Issues

**#1-#6:** While true that we can add more error messages for each require statement, I am not for redeploying for these errors. These require statements are for specific things, like if they try blacklisting the fee address for example. Addressed.

**#7:** This is a library we are using, pretty sure it's being called by uniswap routers for local testing. So no changes will be made.

**#8:** While we could, we will not proceed with this one. Addressed.

**#9:** While this makes sense, this is lossless code, and we should not modify it as it is intentionally written this way by their devs. Have tested myself, and everything works with the recovery admin function. Have tested multiple changes.

**#10:** Something to note moving forward, addressed.

**#11-#14:** We have the code flattened when verifying so they are all covered by the licensing.

## Audit Comments

We recommend you use the special form of comments (NatSpec Format, Follow the link for more information <https://docs.soliditylang.org/en/latest/natspec-format.html>) for your contracts to provide rich documentation for functions, return variables, and more. This helps investors to make clear what those variables, functions, etc. do.

### 15. November 2022:

- We recommend you to follow the terms of the diamond-3 pattern
  - This project is a modified diamond-3 pattern
- Read the whole report and modifiers section for more information

### 09. December 2022:

- Read the whole report and modifiers section for more information

### 13. March 2023:

- Changes of the new version of the project
  - The Architecture of the project was changed. Contracts are not inheriting from Storage anymore. The storage contract was implemented like an Interface where the owner can pass the “storage” address to interact with it.
  - External/Public functions were prevented to call be require statements
  - More Events were added to the project
  - Files
    - TaxFacet
      - Functions removed
        - mint
    - MulticallFacet
      - Added LPWallet
  - Diamond-3 standards were implemented into the project from Nick Mudge
- Read whole report and modifiers section for more information

### 22. June 2023:

- All issues have been acknowledged by the unicrypt team.



## SWC Attacks

ID	Title	Relationships	Status
<a href="#">SW C-1 36</a>	Unencrypted Private Data On-Chain	<a href="#">CWE-767: Access to Critical Private Variable via Public Method</a>	PASSED
<a href="#">SW C-1 35</a>	Code With No Effects	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-1 34</a>	Message call with hardcoded gas amount	<a href="#">CWE-655: Improper Initialization</a>	PASSED
<a href="#">SW C-1 33</a>	Hash Collisions With Multiple Variable Length Arguments	<a href="#">CWE-294: Authentication Bypass by Capture-replay</a>	PASSED
<a href="#">SW C-1 32</a>	Unexpected Ether balance	<a href="#">CWE-667: Improper Locking</a>	PASSED
<a href="#">SW C-1 31</a>	Presence of unused variables	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-1 30</a>	Right-To-Left-Override control character (U+202E)	<a href="#">CWE-451: User Interface (UI) Misrepresentation of Critical Information</a>	PASSED
<a href="#">SW C-1 29</a>	Typographical Error	<a href="#">CWE-480: Use of Incorrect Operator</a>	PASSED
<a href="#">SW C-1 28</a>	DoS With Block Gas Limit	<a href="#">CWE-400: Uncontrolled Resource Consumption</a>	PASSED

<a href="#">SW C-1 27</a>	Arbitrary Jump with Function Type Variable	<a href="#">CWE-695: Use of Low-Level Functionality</a>	<b>PASSED</b>
<a href="#">SW C-1 25</a>	Incorrect Inheritance Order	<a href="#">CWE-696: Incorrect Behavior Order</a>	<b>PASSED</b>
<a href="#">SW C-1 24</a>	Write to Arbitrary Storage Location	<a href="#">CWE-123: Write-what-where Condition</a>	<b>PASSED</b>
<a href="#">SW C-1 23</a>	Requirement Violation	<a href="#">CWE-573: Improper Following of Specification by Caller</a>	<b>PASSED</b>
<a href="#">SW C-1 22</a>	Lack of Proper Signature Verification	<a href="#">CWE-345: Insufficient Verification of Data Authenticity</a>	<b>PASSED</b>
<a href="#">SW C-1 21</a>	Missing Protection against Signature Replay Attacks	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>
<a href="#">SW C-1 20</a>	Weak Sources of Randomness from Chain Attributes	<a href="#">CWE-330: Use of Insufficiently Random Values</a>	<b>PASSED</b>
<a href="#">SW C-11 9</a>	Shadowing State Variables	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>
<a href="#">SW C-11 8</a>	Incorrect Constructor Name	<a href="#">CWE-665: Improper Initialization</a>	<b>PASSED</b>
<a href="#">SW C-11 7</a>	Signature Malleability	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>

<a href="#">SW C-11 6</a>	Timestamp Dependence	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	<b>PASSED</b>
<a href="#">SW C-11 5</a>	Authorization through tx.origin	<a href="#">CWE-477: Use of Obsolete Function</a>	<b>PASSED</b>
<a href="#">SW C-11 4</a>	Transaction Order Dependence	<a href="#">CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</a>	<b>PASSED</b>
<a href="#">SW C-11 3</a>	DoS with Failed Call	<a href="#">CWE-703: Improper Check or Handling of Exceptional Conditions</a>	<b>PASSED</b>
<a href="#">SW C-11 2</a>	Delegatecall to Untrusted Callee	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	<b>PASSED</b>
<a href="#">SW C-11 1</a>	Use of Deprecated Solidity Functions	<a href="#">CWE-477: Use of Obsolete Function</a>	<b>PASSED</b>
<a href="#">SW C-11 0</a>	Assert Violation	<a href="#">CWE-670: Always-Incorrect Control Flow Implementation</a>	<b>PASSED</b>
<a href="#">SW C-1 09</a>	Uninitialized Storage Pointer	<a href="#">CWE-824: Access of Uninitialized Pointer</a>	<b>PASSED</b>
<a href="#">SW C-1 08</a>	State Variable Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>
<a href="#">SW C-1 07</a>	Reentrancy	<a href="#">CWE-841: Improper Enforcement of Behavioral Workflow</a>	<b>PASSED</b>
<a href="#">SW C-1 06</a>	Unprotected SELFDESTRUCT Instruction	<a href="#">CWE-284: Improper Access Control</a>	<b>PASSED</b>

<a href="#">SW</a> <a href="#">C-1</a> <a href="#">05</a>	Unprotected Ether Withdrawal	<a href="#">CWE-284: Improper Access Control</a>	<b>PASSED</b>
<a href="#">SW</a> <a href="#">C-1</a> <a href="#">04</a>	Unchecked Call Return Value	<a href="#">CWE-252: Unchecked Return Value</a>	<b>PASSED</b>
<a href="#">SW</a> <a href="#">C-1</a> <a href="#">03</a>	Floating Pragma	<a href="#">CWE-664: Improper Control of a Resource Through its Lifetime</a>	<b>PASSED</b>
<a href="#">SW</a> <a href="#">C-1</a> <a href="#">02</a>	Outdated Compiler Version	<a href="#">CWE-937: Using Components with Known Vulnerabilities</a>	<b>PASSED</b>
<a href="#">SW</a> <a href="#">C-1</a> <a href="#">01</a>	Integer Overflow and Underflow	<a href="#">CWE-682: Incorrect Calculation</a>	<b>PASSED</b>
<a href="#">SW</a> <a href="#">C-1</a> <a href="#">00</a>	Function Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>

*Solid  
Proofed*

**Blockchain Security | Smart Contract Audits | KYC  
Development | Marketing**

  
MADE IN GERMANY