AUDITONE

Audit Report

Hedgey.

Core contract

05.06.2024

Table of Contents

CONTENTS

INTRODUCTION

Smart Contract Security Analysis Report

Note: This report may contain sensitive information on potential vulnerabilities and exploitation methods. This must be referred internally and should be only made available to the public after issues are resolved (to be confirmed prior by the client and AuditOne).

INTRODUCTION

Defsec, Minhquanym and X0f-unit, who are auditors at AuditOne, successfully audited the smart contracts (as indicated below) of Hedgey Finance. The audit has been performed using manual analysis. This report presents all the findings regarding the audit performed on the customer's smart contracts. The report outlines how potential security risks are evaluated. Recommendations on quality assurance and security standards are provided in the report.

01-PROJECT DESCRIPTION

Hedgey is a platform that helps decentralized autonomous organizations (DAOs) and onchain organizations distribute tokens securely and efficiently. It combines token streams, periodic release schedules, and administrative controls, such as revocability and optional governance rights, to automate token distribution to team members, contributors, investors, and the community.

The platform has been used by notable teams like Arbitrum DAO, Celo, Gitcoin, Gnosis, Shapeshift, Index Coop, and Collabland to streamline their token management processes. Hedgey's tools are available as free public goods on a self-service basis, optimized for various issuers and recipients.

Hedgey's core products include token vesting, investor lockups, and token claims. Token vesting plans feature flexible schedules, cliffs, and backdated start dates, and are fully onchain and revocable. Investor lockups allow tokens to be distributed to investors on predefined schedules, with options for transferability and voting rights. The token claims product supports large-scale token distributions, enabling users to review, analyze, and claim their tokens efficiently.

Built on robust smart contracts, Hedgey's platform ensures secure and trustless interactions, providing essential tools for onchain teams to manage their digital assets effectively and support their growth.

02-Project and Audit Information

Term	Description
Auditor	Defsec, Minhquanym and X0f-unit
Reviewed by	Luis Buendia and Gracious Igwe
Type	Finance
Language	Solidity
Ecosystem	EVM Compatible
Methods	Manual Review
Repository	https://github.com/hedgey-finance/Locked_VestingTokenPlans
Commit hash (at audit start)	7e178923bca6244161b71969c60d6936b95f1956
Commit hash (after resolution)	ede287900fe3f10c16b188add4a9f4823e55b7e0
Documentation	NA
Unit Testing	NA
Website	https://hedgey.finance/
Submission date	20/05/2024
Finishing date	03/06/2024

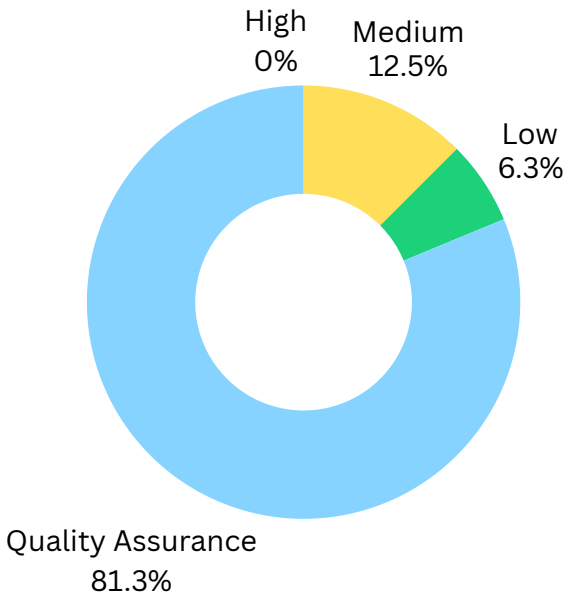
03-Contracts in Scope

Forwarder contracts path

- ERC721Delegate/ERC721Delegate.sol
- LockupPlans/TokenLockupPlans.sol
- LockupPlans/VotingTokenLockupPlans.sol
- LockupPlans/NonTransferable/TokenLockupPlans_Bound.sol
- Periphery/BatchPlanner.sol
- VestingPlans/TokenVestingPlans.sol
- VestingPlans/VotingTokenVestingPlans.sol
- libraries/TimelockLibrary.sol
- libraries/TransferHelper.sol
- sharedContracts/LockupStorage.sol
- sharedContracts/PlanDelegator.sol
- sharedContracts/URIAdmin.sol
- sharedContracts/VestingStorage.sol
- sharedContracts/VotingVault.sol

04-Executive summary

Hedgey Finance smart contracts were audited between 20-05-2024 and 03-06-2024 by Defec, Minhquanym and X0f-unit. Manual analysis was carried out on the code base provided by the client. The following findings were reported to the client. For more details, refer to the findings section of the report.



Issue Category	Issues Found	Resolved	Acknowledged
High	0	0	0
Medium	2	1	1
Low	1	1	0
Quality Assurance	13	3	10

05-Severity Definitions

Risk factor matrix	Low	Medium	High
Occasional	L	M	H
Probable	L	M	H
Frequent	M	H	H

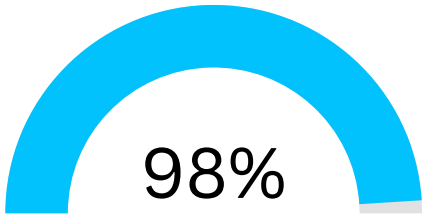
High: Funds or control of the contracts might be compromised directly. Data could be manipulated. We recommend fixing high issues with priority as they can lead to severe losses.

Medium: The impact of medium issues is less critical than high, but still probable with considerable damage. The protocol or its availability could be impacted, or leak value with a hypothetical attack path with stated assumptions.

Low: Low issues impose a small risk on the project. Although the impact is not estimated to be significant, we recommend fixing them on a long-term horizon. Assets are not at risk: state handling, function incorrect as to spec, issues with comments.

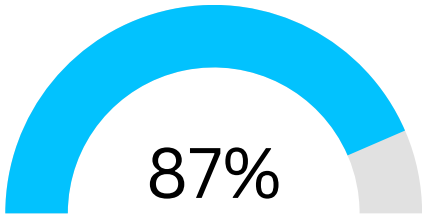
Quality Assurance: Informational and Optimization - Depending on the chain, performance issues can lead to slower execution or higher gas fees. For example, code style, clarity, syntax, versioning, off-chain monitoring (events etc.)

06-Audit Overview



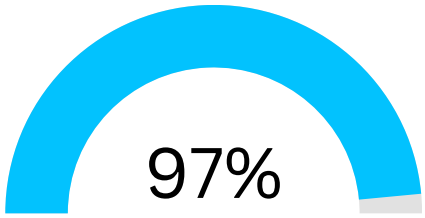
Security score

Security score is a numerical value generated based on the vulnerabilities in smart contracts. The score indicates the contract's security level and a higher score implies a lower risk of vulnerability.



Code quality

Code quality refers to adherence to standard practices, guidelines, and conventions when writing computer code. A high-quality codebase is easy to understand, maintain, and extend, while a low-quality codebase is hard to read and modify.



Documentation quality

Documentation quality refers to the accuracy, completeness, and clarity of the documentation accompanying the code. High-quality documentation helps auditors to understand business logic in code well, while low-quality documentation can lead to confusion and mistakes.

07-Findings

Finding: #1

Issue: BatchCreator and **DelegatedClaimCampaigns** are partially incompatible with Bound Lockup Plans.

Severity: Medium

Where: BatchCreator.createLockupPlansWithDelegation(), and **DelegatedClaimCampaigns._claimLockedAndDelegate()** functions.

Impact: The **BatchCreator** and **DelegatedClaimCampaigns** functions that include delegation after creation or claim cannot be used with Bound Lockup Plans. Since these tokens cannot be transferred, an incompatibility of this function arises, preventing non-transferable lockups from being created using a CSV upload, which is an undocumented incompatibility.

Description: The **createLockupPlansWithDelegation()** function is not compatible with **TokenLockupPlans_Bound** and **VotingTokenLockupPlans_Bound** plans. This is because the **createLockupPlansWithDeletation()** function mints the plan tokens to the **BatchCreator** contract, performs the requested delegations, and then transfers the token to the legitimate owner.
As expected, both of these plans will revert when they are transferred.

Recommendations: If full compatibility is desired, it is recommended to implement a special case in **_beforeTokenTransfer()** hook to allow the token transfer if the **msg.sender** or the owner of the token is **BatchCreator** or **DelegatedClaimCampaigns** contract.

Status: Resolved.

Finding: #2

Issue: transferAndDelegate() function will always revert

Severity: Medium

Where: VotingTokenLockupPlans.transferAndDelegate()

Impact: The **transferAndDelegate()** function from the **VotingTokenLockupPlans** contract is unusable.

Description: The **transferAndDelegate** function will never work in the **VotingTokenLockupPlans** contract.

This function should be called by the owner or by any user holding the **Delegator** role.

First of all, the Lock NFT is transferred to the new user, and after that, **_delegate()** function is called. In this function, a require statement calling **_isApprovedDelegatorOrOwner()** enforces that only an approved delegator or owner could perform the delegation. And since the token was already transferred in the previous step, **msg.sender** will not be the owner of the token anymore.

In addition, **getApprovedDelegator()** would also fail, since **_approvedDelegators[firstTokenId]** is also removed when transferring the token.

Recommendations: Alter the order of the calls, performing the delegation before transferring the token.

Status: Acknowledged.

Finding: #3

Issue: Incompatibility with Fee-On-Transfer tokens

Severity: Low

Where: TransferHelper.sol:L28,44

Impact: The plans would be locked if any token being used in a plan enables this feature.

Description: The **transferTokens()** and **withdrawTokens()** functions in **TransferHelper** contracts include a require statement that ensures that the total **amount** balance transferred has been received, reverting if a Fee-On-Transfer token is used or if the amount received is lower than the expected due to any reason.

This is behavior is described in the comments in **TransferHelper** contract from VestingLockups repository, but not in the one found in Locked_VestingTokenPlans.

However, certain tokens, such as USDT or USDC, already include Fee-On-Transfer mechanisms, only that they are currently set to 0. If any of these tokens enabled the fee-on-transfer functionality, any existing plan using these tokens would remain locked in the contract since the require statement of line 44 would always revert.

Recommendations: It is recommended to implement an emergency withdraw function in case tokens remain locked in the contract, similar to the emergency admin transfer feature from **TokenVestingPlans** contract.

Status: Resolved.

Finding: #4

Issue: Invert order of instructions to save gas

Severity: QA

Where:
- **TokenLockupPlan_Bound**:L29-30
- **VotingTokenLockupPlan_Bound**:L29-30

Impact: Performing additional checks for token ownership before reverting waste gas.

Description: For **TokenLockupPlan_Bound** and **VotingTokenLockupPlan_Bound**, tokens are not transferable. This is enforced in the **_beforeTokenTransfer()** hook, which will revert if (**from != address(0) && to != address(0)**), which means that it will only allow token transfers if it is a mint or a burn.

However, **super._beforeTokenTransfer()** is called before determining if it is a mint or a burn or if the transaction should revert, performing unnecessary checks that could have been avoided if the order of the instructions was inverted.

Recommendations: Invert the order of the instructions within **_beforeTokenTransfer()** to save gas if the revert condition is met.

Status: Acknowledged.

Finding: #5

Issue: Missing ETH Wrapping and Unwrapping Functionality in **TransferHelper** Library.

Severity: QA

Where: TransferHelper.sol#L8

Impact: The library fails to meet the expectations set by the specification, which states that it should handle ETH wrapping and unwrapping. This inconsistency can cause confusion and misunderstandings for developers relying on the library.

Description: The provided TransferHelper library includes functions for safely transferring ERC20 tokens using the transferTokens and withdrawTokens functions. However, the library lacks functionality for wrapping and unwrapping ETH (Ether) to and from WETH (Wrapped Ether), despite the specification mentioning the library's intention to handle ETH wrapping and unwrapping.

```
/// @notice Library to help safely transfer tokens and handle ETH wrapping and unwrapping of WETH
library TransferHelper {
  using SafeERC20 for IERC20;
```

Recommendations: Consider fixing the spec on the library.

Status: Resolved.

Finding: #6

Issue: Incomplete NATSPEC

Severity: QA

Where: Every scoped contract.

Impact: Incomplete NATSPEC reduces code readability and can affect UX.

Description: It has been detected that some functions (including public/external functions) are lacking of a proper NATSPEC documentation.

Recommendations: It is recommended to have a complete and detailed NATSPEC documentation, even for non-public functions, since it increases code readability.

Status: Unresolved.

Finding: #7

Issue: Revert Strings increase gas usage

Severity: QA

Where: Every revert string used in the scoped contracts.

Impact: The gas usage is increased and can be reduced.

Description: Since Solidity 0.8.4, custom errors can be used. Each custom error saves around 50 gas every time they are hit, since they avoid the need for allocating and storing the revert string.

Recommendations: Use custom errors instead of revert strings to save gas.

Status: Acknowledged.

Finding: #8

Issue: Redundant check can be removed to reduce gas usage

Severity: QA

Where: **PlanDelegator.sol**:L48

Impact: The gas usage is increased due to a redundant check in **approveSpenderDelegator()** function.

Description: The **approveSpenderDelegator()** function from **PlanDelegator** contract includes the following function call: **_approve(spender, planId, msg.sender);**

This _approve implementation includes the "**auth**" parameter, which if different from zero, will check that "**auth**" is indeed the owner or approved to operate on all tokens held by the owner. In this case, **msg.sender** is sent as **auth**. However, this check is already being performed in the lines above, so it's redundant:

```
function approveSpenderDelegator(address spender, uint256 planId) public virtual {
  address owner = ownerOf(planId);
  require(
    msg.sender == owner || (isApprovedForAllDelegation(owner, msg.sender) && isApprovedForAll(owner, msg.sender)
    '!ownerOperator'
  );
  require(spender != msg.sender, '!self approval');
  _approveDelegator(spender, planId);
  _approve(spender, planId, msg.sender);
}
```

Recommendations: Since the relevant ownership or approval checks have already been performed, **auth** can be set to **0** in the **_approve()** call to save some gas.

Status: Resolved.

Finding: #9

Issue: For loops gas optimizations

Severity: QA

Where: Every **for** loop in the scoped contracts.

Impact: By using a non-locked pragma version, contracts could be accidentally deployed using a different pragma, which could introduce bugs or different behaviors that could negatively affect the contracts.

Description: Multiple gas optimizations have been found in the **for** loop used in the scoped contracts:

1. uint256 index **i** is being checked while incremented: It is not necessary to use a safe increment on **i** if a **uint256** variable is used since the function will run out of gas way before overflowing.
2. Postfix operators (**i++**) are being used instead of prefix operators (**++i**).
3. The array length is read in every iteration instead of being cached outside the loop.
4. **i** is initialized to **0**.

Recommendations:

1. Increment **i** using **unchecked: unchecked {++i}**
2. Use prefix operators instead of postfix operators.
3. Cache the array length in a variable outside the loop as long as the size will not change during the loop.
4. Do not initialize the value of **i**, since **0** (or **false**) are the default values in Solidity.

Status: Resolved.

Finding: #10

Issue: Error-prone variable naming

Severity: QA

Where: TokenLockupPlans:L253-254

Impact: Using confusing variable names reduces code readability and understanding and makes debugging and using the code more difficult.

Description: The **_segmentPlan()** function from **TokenLockupPlans** and **VotingTokenLockupPlans** contracts uses two different variables, called **planAmount** and **plan.amount**. These variables are confusing and error-prone.

Recommendations: Variable names are recommended to be succinct and unique to avoid confusion and increase code readability. This has been observed many times along the codebase.

Status: Unresolved.

Finding: #11

Issue: Variable name not adhering to the naming convention

Severity: QA

Where: **BatchCreator**:L285

Impact: Using an inconsistent naming convention decreases code readability and understandability.

Description: The **transferableblocks** parameter from **BatchCreator.createVestingLockupPlans()** function does not adhere to the camelCase naming convention.

Recommendations: Adhere to a consistent naming convention (usually camelCase).

Status: Unresolved.

Finding: #12

Issue: Typos in comments

Severity: QA

Where: TokenLockupPlans:L22 (**Combingin Plans**)
That is only one example of the issue, but many more were identified along the code.

Impact: Typos in code comments can impact the readability and understanding of the code, potentially leading to confusion and misunderstandings for developers maintaining or reviewing the code in the future.

Description: Typos in the code comments were identified, which might impact the readability and understandability of the code.

Recommendations: It is recommended to fix the typos.

Status: Unresolved.

Finding: #13

Issue: Require statement is reverting without providing any reason

Severity: QA

Where: createPlan() function implementations.

Impact: Error debugging and logging capabilities are reduced if reverts provide no reason.

Description: It has been noted that the end validity check of a plan can revert without providing any reason: **require(valid);**. The rest of the require statements include an error message when reverting, but this does not.

Recommendations: To improve code uniformity, it is suggested to provide a revert reason.

Status: Unresolved.

Finding: #14

Issue: **uriAdmin** cannot be changed

Severity: QA

Where: **URIAdmin** contract

Impact: If the **uriAdmin** account gets compromised, deploying a new full set of contracts might be needed in case that **baseURI** has to be updated.

Description: The **uriAdmin** address is set at the constructor of each plan contract. This address cannot be changed, only deleted.

Recommendations: Implement a **uriAdmin** change function if needed.

Status: Acknowledged.

Finding: #15

Issue: Misleading comments

Severity: QA

Where:
- **DelegatedClaimCampaigns:**L161
- **TokenVestingPlans:**L18

Impact: Misleading comments might lead users or developers to make false assumptions about the code, that could lead to unexpected behaviors.

Description: The comments in **DelegatedClaimCampaigns.createLockedCampaign()** function states that **additionally it will check that the lockup details are valid, and perform an allowance increase to the contract for when tokens are claimed they can be pulled.**

However, it was observed that the allowance increases are performed in the claiming functions, not in the creation, and the remaining allowance is checked to be 0 at the end of these.

Another instance was detected in **TokenVestingPlans** contract, in which the following is stated: **3. Governance optimized for snapshot voting: These are built to allow beneficiaries to vote with their unvested tokens on snapshot, or delegate them to other delegates.** However, that is not exactly true, since users do not vote with their unvested tokens, but with the unclaimed ones (which include unvested and vested but unclaimed tokens).

Recommendations: Fix the code comments to adhere to the actual code logic implemented. It is important to update the comments when the code is changed, as well.

Status: Unresolved.

Finding: #16

Issue: Broken Invariant: The plan recipient can be set as the admin

Severity: QA

Where: **TokenVestingPlans** and **VotingTokenVestingPlans** contracts (**createPlan()** function).

Impact: Any **vestingAdmin** could create plans with himself as the recipient and transfer them at will.

Description: According to the documentation, each Token Vesting Plan is soul-bound, meaning that cannot be transferred by the beneficiary, only by the plan admin, which is set in the **vestingAdmin** parameter.

However, it was noted that when creating a plan, **vestingAdmin** is not being enforced to be different from the recipient, which might lead to scenarios in which plan recipients are able to transfer their own plans.

It has been observed that this check is actually enforced in the **changeVestingPlanAdmin()** function, but not when the plan is created.

Recommendations: Enforce that **recipient** and **vestingAdmin** addresses are different when creating a plan.

Status: Acknowledged.

08 - Disclaimer

The smart contracts provided to AuditOne have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions). The ethical nature of the project is not guaranteed by a technical audit of the smart contract. Any owner-controlled functions should be carried out by the responsible owner. Before participating in the project, all investors/users are recommended to conduct due research.

The focus of our assessment was limited to the code parts associated with the items defined in the scope. We draw attention to the fact that due to inherent limitations in any software development process and product, an inherent risk exists that even major failures or malfunctions can remain undetected. Further uncertainties exist in any software product or application used during the development, which cannot be free from any errors or failures. These preconditions can impact the system's code and/or functions and/or operation. We did not assess the underlying third-party infrastructure, which adds further inherent risks as we rely on correctly executing the included third-party technology stack itself. Report readers should also consider that over the life cycle of any software product, changes to the product itself or the environment in which it is operated can have an impact leading to operational behaviors other than initially determined in the business specification.

Contact

auditone.io

@auditone_team

hello@auditone.io

A trust layer of our
multi-stakeholder world.