Quantstamp Security Assessment Certificate

January 21st 2022 — Quantstamp Verified

JPEG'd Part 3

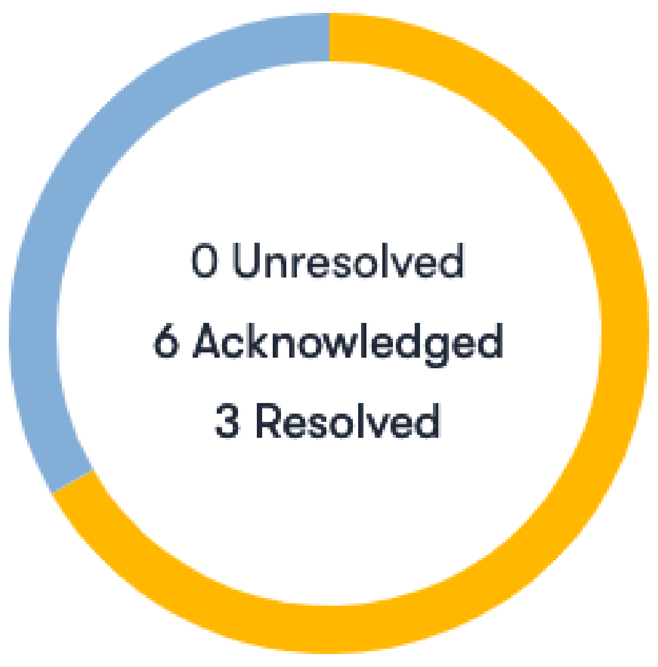
This audit report was prepared by Quantstamp, the leader in blockchain security.

Executive Summary

Type	NFT Lending
Auditors	Jose Ignacio Orlicki, Senior Engineer Cristiano Silva, Research Engineer Marius Guggenmos, Senior Research Engineer
Timeline	2021-12-13 through 2022-01-21
EVM	London
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	None
Documentation Quality	Medium
Test Quality	Medium
Source Code	

Repository	Commit
jpegd	679bb3c
jpegd	56d7ac1

Total Issues	**9** (3 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	**1** (1 Resolved)
Low Risk Issues	**5** (2 Resolved)
Informational Risk Issues	**3** (0 Resolved)
Undetermined Risk Issues	0 (0 Resolved)



High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
? Undetermined	The impact of the issue is uncertain.

Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

We have reviewed the code, documentation, and test suite and found several issues of various severities. Overall, we consider the code to be well-written but with insufficient documentation in the form of expected interaction diagrams, although inline comments and docstrings are extremely good and detailed. The test suite is very extensive but can be improved given the suggested changes from this report. We have outlined suggestions to better follow best practices, and recommend addressing all the findings to tighten the contracts for future deployments or contract updates. We recommend addressing all the **10** findings to harden the contracts for future deployments or contract updates. We recommend against deploying the code as-is.
Update: Quantstamp has audited the changes based on the commit for the `jpegd` repository (56d7ac1). Of the original 10 issues, all 9 active issues have been either fixed, acknowledged, or mitigated. The remaining issue was found to be a false positive.

ID	Description	Severity	Status
QSP-1	Farmed By Contracts	^ Medium	Mitigated
QSP-2	Anomalous Borrowing With Self-Transferred NFTs	⌄ Low	Fixed
QSP-3	Accidentally Renouncing The Ownership Is Possible	⌄ Low	Fixed
QSP-4	Rate `availableTokensRate` Not Enforced	⌄ Low	Acknowledged
QSP-5	DAO Can Revoke Its Role Admin's Role	⌄ Low	Acknowledged
QSP-6	Missing Input Validations	⌄ Low	Acknowledged
QSP-7	Interface Not Explicitly Implemented	○ Informational	Acknowledged
QSP-8	Pausable Feature Concerns	○ Informational	Acknowledged
QSP-9	Reentrancy Patterns	○ Informational	Acknowledged

Quantstamp Audit Breakdown

Quantstamp's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Methodology

The Quantstamp 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 Quantstamp 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 Quantstamp 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 analyzing a program to determine what inputs cause 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, and actionable recommendations to help you take steps to secure your smart contracts.

Toolset

The notes below outline the setup and steps performed in the process of this audit.

Setup

Tool Setup:

- Slither v0.8.0

Steps taken to run the tools:

1. Installed the Slither tool: `pip install slither-analyzer`
2. Run Slither from the project directory: `slither .`

Findings

QSP-1 Farmed By Contracts

Severity: Medium Risk

Status: Mitigated

File(s) affected: `./vaults/yVault/yVault.sol`, `./farming/yVaultLPFarming.sol`, `./farming/LPFarming.sol`

Description: A frequently observed pattern is using the function `isContract()` to avoid functionality from being accessed by other contracts. This function utilizes a specific opcode called `EXTCODESIZE` that only returns a zero-size code segment for non-contracts. One exception is that inside a constructor, the code segment is also empty. This enables auto-compounding from ephemeral contracts that have been built to specifically bypass this check using the `CREATE2` opcode with a fixed salt.

Recommendation: Consider documenting this exception, as some auto-farming strategies won't be avoided.

Update: Documented in this PR.

QSP-2 Anomalous Borrowing With Self-Transferred NFTs

Severity: Low Risk

Status: Fixed

File(s) affected: `./vaults/NFTVault.sol`

Description: If an attacker transfers on its own NFTs to the `NFTVault` contract, there is a potential for anomalous borrowing of PUSD for this user as the debt position will be accounted but then the position cannot be repaid with `repay()` or closed with `close()` as `positionOwner[_nftIndex] == address(0)`. The root cause is that `_openPosition()` is never called in this scenario. Because the attacker transferred the NFTs to the `NFTVault` before calling `borrow()` then condition `positionOwner[_nftIndex] == address(0)` is good, condition `nftContract.ownerOf(_nftIndex) == address(this)` is good, giving the user an expected borrowing power for the PUSD. Also, the default value of the `Enum BorrowType` is the first value of an enumeration that has index 0 (`NOT_CONFIRMED`), which is good for the anomalous scenario to be completed. This scenario has low financial impact because it only affects financially a user depositing NFTs in a bizarre or accidental interaction outside of the recommended interaction.

Recommendation: Check `nftContract.ownerOf(_nftIndex) == address(this)` and `positionOwner[_nftIndex] != address(0)` at the same time as a valid precondition for `borrow()`. Also, consider using a separate bool for structs as Solidity does not has special `null` or `nil` values as declared in the documentation.

```
The concept of “undefined” or “null” values does not exist in Solidity, but newly declared variables always have a default value dependent on its type. To handle any unexpected values, you should use the revert function to
revert the whole transaction, or return a tuple with a second bool value denoting success.
```

Update: Fixed in this PR.

QSP-3 Accidentally Renouncing The Ownership Is Possible

Severity: Low Risk

Status: Fixed

File(s) affected: `farming/yVaultLPFarming.sol`, `vaults/yVault/yVault.sol`

Description: Many contracts inherit from some form of `Ownable`, which means the `renounceOwnership` function is available to call which would leave the contract in an unrecoverable state.

Recommendation: Override the `renounceOwnership` function and make it revert. Otherwise, document this feature.

Update: Fixed in this PR.

QSP-4 Rate `availableTokensRate` Not Enforced

Severity: Low Risk

Status: Acknowledged

File(s) affected: `vaults/yVault/yVault.sol`

Description: The rate `availableTokensRate` is supposed to control the ratio of how much should be held in the vault to make small withdrawals cheap. Since `earn()` can be called by anyone, tokens can repeatedly be transferred to the strategy.

Recommendation: Properly enforce the rate by taking the balance of the vault and the strategy into consideration and return only the surplus.

Update: Acknowledged that this is part of the design. The detailed response from the team was that "*The availableTokensRate variable has been implemented only as a gas-saving measure and since calling earn() repeatedly doesn't compromise the functionality of the contract in any way we decided to leave everything as is.*".

QSP-5 DAO Can Revoke Its Role Admin's Role

Severity: Low Risk

Status: Acknowledged

File(s) affected: `./vaults/yVault/yVault.sol`

Description: Similar to contract ownerships, the DAO admin can revoke its own permissions to be DAO role admin (`DAO_ROLE`) or other roles, such as Liquidator (`LIQUIDATOR_ROLE`) role admin. This can leave the `NFTVault` with limited functionality, including the limitation to allow new liquidators if existing liquidator bots have issues or need to be upgraded.

Recommendation: Document this feature of role admin renouncing its admin role as part of the future deployment plan, or override this function and revert to disable it for the role admin.

Update: Acknowledged that this is part of the design. The detailed response from the team was that "*This is by design as the DAO needs to be able to transfer/revoke roles.*".

QSP-6 Missing Input Validations

Severity: Low Risk

Status: Acknowledged

File(s) affected: `YVaultLPFarming.sol`

Description: The parameters of type `address` should be checked to be non-zero, before being assigned to state variables. These sanity checks on input addresses can avoid confusion in general and in, some cases, serious problems. Also, in the case of `pendingReward(user)` checking that `user != address(0)` can help avoid confusion on the UI development (leading to some minor financial loss).

Recommendation: Add checks for all parameters of type `address`.

Update: Acknowledged that this is part of the design. The detailed response from the team was that "*The only function affected by this is pendingReward(user) which is a frontend function. Calling it with address(0) would just return 0*".

QSP-7 Interface Not Explicitly Implemented

Severity: Informational

Status: Acknowledged

File(s) affected: `vaults/yVault/strategies/StrategyPUSDConvex.sol`

Description: The `StrategyPUSDConvex` contract implements the `IStrategy` interface but does not specify this explicitly. Not doing so might lead to small deviations in the signatures of what a caller expects and what the contract actually does.

Recommendation: Explicitly implement the interface `IStrategy`.

Update: Acknowledged by the JPEG'd team.

QSP-8 Pausable Feature Concerns

Severity: Informational

Status: Acknowledged

File(s) affected: `StableCoin.sol`

Description: Some third-party custodians consider `Pausable` token features a red flag as they cannot always control when to transfer back the tokens under custody to their clients.

Recommendation: Document this feature and research which centralized exchanges or custodians you want to interact with, if applicable.

Update: Acknowledged by the JPEG'd team.

QSP-9 Reentrancy Patterns

Severity: Informational

Status: Acknowledged

File(s) affected: `TokenSale.sol`, `NFTVault.sol`, `LPFarming.sol`, `yVaultLPFarming.sol`, `Controller.sol`

Description: Potential reentrancy patterns have been observed in the code. These include situations where external contracts are called before changing the internal state or emitting logging events. The codes detailed change state variables after external calls. The details have been included in the *Automated Analyses* section of this report and are not considered to be good blockchain security practices.

Recommendation: Apply Checks-Effect-Interactions pattern to avoid this kind of security best practices red flags.

Update: Acknowledged that these reentrancy patterns are not exploitable on their own. The detailed response from the team was that "*All the reentrancy patterns in the codebase are non-exploitable and have been introduced by design to save some gas on failing transactions*"

Automated Analyses

Slither

Slither has detected many results out of which the majority have been mostly filtered out as false positives and the rest have been integrated into the findings from this report. We include some non-exploitable reentrancy patterns we have observed.

```
1- Reentrancy in TokenSale.allocateTokensForSale(uint256) (contracts/sale/TokenSale.sol#141-149):
   External calls:
   - IERC20(saleToken).safeTransferFrom(msg.sender,address(this),_amount) (contracts/sale/TokenSale.sol#145)
   State variables written after the call(s):
   - availableTokens = _amount (contracts/sale/TokenSale.sol#146)

2- Reentrancy in LPFarming.deposit(uint256,uint256) (contracts/farming/LPFarming.sol#212-227):
   External calls:
   - pool.lpToken.safeTransferFrom(msg.sender,address(this),_amount) (contracts/farming/LPFarming.sol#223)
   State variables written after the call(s):
   - user.amount = user.amount + _amount (contracts/farming/LPFarming.sol#224)

3- Reentrancy in YVaultLPFarming.deposit(uint256) (contracts/farming/yVaultLPFarming.sol#98-110):
   External calls:
   - vault.safeTransferFrom(msg.sender,address(this),_amount) (contracts/farming/yVaultLPFarming.sol#104)
   State variables written after the call(s):
   - balanceOf[msg.sender] += _amount (contracts/farming/yVaultLPFarming.sol#106)
   - totalStaked += _amount (contracts/farming/yVaultLPFarming.sol#107)

4- Reentrancy in NFTVault.finalizePendingNFTValueETH(uint256) (contracts/vaults/NFTVault.sol#338-359):
   External calls:
   - jpegLocker.lockFor(msg.sender,_nftIndex,toLockJpeg) (contracts/vaults/NFTVault.sol#353)
   State variables written after the call(s):
   - pendingNFTValueETH[_nftIndex] = 0 (contracts/vaults/NFTVault.sol#358)

5- Reentrancy in NFTVault.repurchase(uint256) (contracts/vaults/NFTVault.sol#854-888):
   External calls:
   - stablecoin.transferFrom(msg.sender,position.liquidator,debtAmount + penalty) (contracts/vaults/NFTVault.sol#874-878)
   State variables written after the call(s):
   - positionOwner[_nftIndex] = address(0) (contracts/vaults/NFTVault.sol#881)
   - delete positions[_nftIndex] (contracts/vaults/NFTVault.sol#882)
```

```
6- Reentrancy in Controller.setStrategy(IERC20,IStrategy) (contracts/vaults/yVault/Controller.sol#82-98):
   External calls:
   - _current.withdrawAll() (contracts/vaults/yVault/Controller.sol#94)
   - _current.withdraw(address(jpeg)) (contracts/vaults/yVault/Controller.sol#95)
   State variables written after the call(s):
   - strategies[_token] = _strategy (contracts/vaults/yVault/Controller.sol#97)
```

Code Documentation

- The natspec of the function `liquidate` in `jpegd-liquidator/solidity/contracts/Liquidator.sol` specifies that it reverts when there are not enough funds when in reality it does not.

    `This function reverts when there's not enough PUSD in this contract`

Adherence to Best Practices

- Use `immutable` for members that are only ever set in the constructor (`vault` in farming/yVaultLPFarming.sol) **Fixed** in PR

Test Results

Test Suite Results

The number of tests climbed to 119 test cases. We consider the testing suite very complete and extensive, although reported issues in this report must be considered to add news test cases. Detailed output is included below.

```
$ yarn test
yarn run v1.22.10
$ hardhat test
No need to generate any newer typings.

  Controller
     ✓ should return the correct JPEG balance (66ms)
     ✓ should allow the vault to withdraw jpeg (119ms)
     ✓ should allow admins to set the fee address (21ms)
     ✓ should allow strategists to set vaults for tokens (27ms)
     ✓ should allow admins to approve and revoke strategies (52ms)
     ✓ should allow strategists to set strategies (78ms)
     ✓ should deposit tokens into the strategy when calling earn (53ms)
     ✓ should allow strategists to withdraw all tokens from a strategy (63ms)
     ✓ should allow strategists to withdraw tokens (26ms)
     ✓ should allow strategists to withdraw tokens from a strategy (51ms)
     ✓ should allow vaults to withdraw tokens from a strategy (69ms)

  CryptoPunksHelper
     ✓ should not allow the owner to renounce ownership (7ms)
     ✓ should return the owner of this contract when the nft is owned by the helper (27ms)
     ✓ should return the nft owner in all other cases (18ms)
     ✓ should only allow the owner to call transferFrom and safeTransferFrom (25ms)
     ✓ should revert if neither the contract or the precompute address hold the nft (779ms)
     ✓ should keep the nft if the recipient is the owner (446ms)
     ✓ should send the nft if the recipient is anyone besides the owner (442ms)
     ✓ should allow the owner to send nfts (48ms)
     ✓ can't precompute with the 0 address or the contract as the owner (10ms)

  FungibleAssetVaultForDAO
     ✓ should be able to update creditLimitRate (126ms)
     ✓ should be able to deposit assets (167ms)
     ✓ should be able to borrow assets (155ms)
     ✓ should be able to repay assets (217ms)
     ✓ should be able to withdraw assets (137ms)

  JPEG
     ✓ should allow the minter to mint tokens (18ms)
     ✓ shouldn't allow users to mint tokens (15ms)

  JPEGLock
     ✓ should not allow the owner to renounce ownership (5ms)
     ✓ Only owner can lock tokens (46ms)
     ✓ Cannot unlock before 1 year (74ms)
     ✓ Only position owner can unlock after 1 year (67ms)

  JPEGStaking
     ✓ stake should not work with invalid parameters (21ms)
     ✓ stake should work (36ms)
     ✓ unstake should not work with invalid parameters (12ms)
     ✓ unstake should work (69ms)

  LPFarming
     ✓ should not allow the owner to renounce ownership (4ms)
     ✓ only owner can add pools (62ms)
     ✓ only owner can update pool configuration (61ms)
     ✓ should not allow an epoch with invalid parameters (28ms)
     ✓ should update epoch (88ms)
     ✓ should not emit tokens outside of an epoch (115ms)
     ✓ should not assing rewards in between epochs (113ms)
     ✓ should not allow non whitelisted contracts to farm (52ms)
     ✓ should not allow 0 token deposits or withdrawals (28ms)
     ✓ should work for zero allocations (58ms)
     ✓ should allow whitelisted contracts to farm (85ms)
1:
owner reward:  50000
alice reward:  0
bob reward:  0
2:
owner reward:  16716
alice reward:  33333
bob reward:  0
3:
owner reward:  41762
alice reward:  50053
bob reward:  8333
4:
owner reward:  71787
alice reward:  60069
bob reward:  18341
5:
owner reward:  96847
alice reward:  8343
bob reward:  35027
6:
owner reward:  126872
alice reward:  8351
bob reward:  55044
7:
owner reward:  139432
alice reward:  8351
bob reward:  37519
     ✓ users can deposit/withdraw/claim (8922ms)

  NFTVault
     ✓ should be able to borrow (229ms)
     ✓ should be able to borrow with insurance (112ms)
     ✓ should be able to repay (388ms)
     ✓ should be able to close position (285ms)
     ✓ should be able to liquidate borrow position without insurance (583ms)
     ✓ should be able to liquidate borrow position with insurance (291ms)
     ✓ should be able to repurchase (296ms)
     ✓ should allow the liquidator to claim an nft with expired insurance (304ms)
     ✓ get ape punk + open position + borrow 600ETH (102ms)
     ✓ get punk + increase debt limit to 50000ETH + open position + borrow 6000ETH (212ms)
     ✓ organization is deducted from debt (62ms)
     ✓ insurance fee is deducted from debt (67ms)
     ✓ collect mints interest and send to dao (265ms)
     ✓ should allow the dao to override floor price (128ms)
     ✓ should allow the dao to set nftType (86ms)
     ✓ should allow the dao to set the value of an nft type (64ms)
     ✓ should be able to update borrowAmountCap (52ms)
     ✓ should be able to update debtInterestApr (61ms)
     ✓ should be able to update creditLimitRate (104ms)
```

```
    ✓ should be able to update liquidationLimitRate (100ms)
    ✓ should be able to update organizationFeeRate (59ms)
    ✓ should be able to update insurancePurchaseRate (63ms)
    ✓ should be able to update insuranceLiquidationPenaltyRate (72ms)

  PreJPEG
    ✓ should mint PreJPEG tokens on new vesting (35ms)
    ✓ should burn all tokens on revoke (50ms)
    ✓ should burn tokens on release (64ms)
    ✓ should not allow transfers (37ms)

  Stablecoin
    ✓ MINTER can mint tokens (39ms)
    ✓ PAUSER can pause token transfer (68ms)
    ✓ PAUSER can unpause token transfer (82ms)

  StrategyPUSDConvex
    ✓ should return the correct name (5ms)
    ✓ should return the correct JPEG balance (44ms)
    ✓ should allow the DAO to change controller (20ms)
    ✓ should allow the DAO to change usdc vault (18ms)
    ✓ should deposit want on convex (35ms)
    ✓ should allow the controller to withdraw JPEG (2987ms)
    ✓ should allow the controller to withdraw non strategy tokens (1261ms)
    ✓ should allow the controller to withdraw want (192ms)
    ✓ should allow the controller to call withdrawAll (120ms)
    ✓ should add liquidity with pusd when harvest is called and curve has less pusd than usdc (18789ms)
    ✓ should add liquidity with usdc when harvest is called and curve has less usdc than pusd (742ms)
    ✓ should revert on deploy with bad arguments (603ms)

  TokenSale
    ✓ should return the correct tokens when calling getSupportedTokens (3ms)
    ✓ should return the correct oracles when calling getTokenOracles (4ms)
    ✓ should return the correct oracle when calling getOracle (4ms)
    ✓ should allow the owner to allocate tokens (42ms)
    ✓ should allow the owner to set the sale schedule (68ms)
    ✓ should allow users to deposit (331ms)
    ✓ should allow the owner to finalize the raise (205ms)
    ✓ should allow the owner to enable withdrawals (94ms)
    ✓ should allow users to withdraw (265ms)
    ✓ should allow the owner to transfer the raise to treasury (257ms)

  TokenVesting
    ✓ should allow members of the vesting_controller role to vest tokens (76ms)
    ✓ shouldn't allow to release vested tokens before vesting starts (30ms)
    ✓ should allow users to release (73ms)
    ✓ should not emit tokens during the cliff period (35ms)
    ✓ should allow to claim all the tokens after vesting is over (62ms)
    ✓ should allow the owner to revoke tokens (120ms)

  yVault
    ✓ should have the same decimals as the deposit token (22ms)
    ✓ should return the correct JPEG balance (15ms)
    ✓ should allow the farm to withdraw JPEG (57ms)
    ✓ should allow users to deposit (93ms)
    ✓ should mint the correct amount of tokens (106ms)
    ✓ should deposits tokens into the strategy when calling earn (77ms)
    ✓ should withdraw the correct amount of tokens (184ms)
    ✓ should not allow non whitelisted contracts to deposit and withdraw (24ms)
    ✓ should allow whitelisted contracts to deposit/withdraw (82ms)

  yVaultLPFarming
    ✓ should allow users to deposit tokens (74ms)
    ✓ should allow users to withdraw (101ms)
    ✓ should allow users to claim (293ms)
    ✓ should not allow non whitelisted contracts to farm (68ms)
    ✓ should allow whitelisted contracts to farm (88ms)

·--------------------------------------------------------------------|---------------------------|-------------|------------------------------·
|                        Solc version: 0.8.0                         ·  Optimizer enabled: true  ·  Runs: 1000 ·  Block limit: 30000000 gas   │
·····································································|···························|·············|·······························
|  Methods                                                                                                                                    │
···························|········································|·············|·············|·············|···············|··············
|  Contract                ·  Method                                ·  Min        ·  Max        ·  Avg        ·  # calls      ·  usd (avg)   │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  approveStrategy                       ·      47274  ·      47286  ·      47285  ·           34  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  earn                                  ·          -  ·          -  ·      60063  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  grantRole                             ·          -  ·          -  ·      51735  ·           37  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  inCaseStrategyTokensGetStuck          ·      61329  ·      62283  ·      61806  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  inCaseTokensGetStuck                  ·          -  ·          -  ·      57198  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  revokeStrategy                        ·          -  ·          -  ·      25413  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  setFeeAddress                         ·          -  ·          -  ·      26623  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  setStrategy                           ·      49694  ·      90709  ·      50911  ·           34  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  setVault                              ·          -  ·          -  ·      47374  ·           22  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  withdraw                              ·          -  ·          -  ·      65402  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  Controller              ·  withdrawAll                           ·      69055  ·      88956  ·      79006  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  CryptoPunks             ·  getPunk                               ·          -  ·          -  ·      73143  ·            6  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  CryptoPunks             ·  transferPunk                          ·          -  ·          -  ·      65051  ·            4  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20PresetMinterPauser  ·  grantRole                             ·      58688  ·      59102  ·      59004  ·          120  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20PresetMinterPauser  ·  revokeRole                            ·      34783  ·      35199  ·      34982  ·           48  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Upgradeable        ·  approve                               ·          -  ·          -  ·      59963  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Upgradeable        ·  transfer                              ·      51268  ·      65613  ·      57937  ·           10  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Upgradeable        ·  transferFrom                          ·     131290  ·     140678  ·     135984  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  borrow                                ·      99346  ·     133546  ·     117998  ·           11  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  deposit                               ·      57348  ·     102545  ·      91522  ·           11  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  repay                                 ·      59168  ·      63866  ·      62300  ·            3  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  setCreditLimitRate                    ·      37105  ·      39976  ·      38062  ·            3  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  setDebtInterestApr                    ·          -  ·          -  ·      37184  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  setLiquidationLimitRate               ·          -  ·          -  ·      39994  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC20Vault              ·  withdraw                              ·      63933  ·      99261  ·      81597  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  ERC721                  ·  safeTransferFrom                      ·          -  ·          -  ·      84572  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEG                    ·  approve                               ·      46783  ·      46819  ·      46804  ·           35  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEG                    ·  grantRole                             ·          -  ·          -  ·      51807  ·           39  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEG                    ·  mint                                  ·      72822  ·     107022  ·      99247  ·           11  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEG                    ·  transfer                              ·      52024  ·      56800  ·      56000  ·            6  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEGLock                ·  lockFor                               ·          -  ·          -  ·     133714  ·            3  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEGLock                ·  transferOwnership                     ·          -  ·          -  ·      28791  ·           23  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEGLock                ·  unlock                                ·          -  ·          -  ·      67020  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEGStaking             ·  stake                                 ·          -  ·          -  ·     170847  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  JPEGStaking             ·  unstake                               ·          -  ·          -  ·     107339  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  add                                   ·      82477  ·     142070  ·     118298  ·           13  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  claim                                 ·     107516  ·     143716  ·     125616  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  claimAll                              ·     138298  ·     155398  ·     146848  ·            2  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  deposit                               ·      99135  ·     126476  ·     112668  ·           10  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  newEpoch                              ·      42639  ·     147178  ·     110751  ·            8  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  set                                   ·      36322  ·      44411  ·      41715  ·            3  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  setContractWhitelisted                ·          -  ·          -  ·      46644  ·            1  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  LPFarming               ·  withdraw                              ·      52460  ·     106937  ·      85044  ·            4  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  MockV3Aggregator        ·  updateAnswer                          ·      78889  ·     120737  ·     102681  ·            8  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  NFTVault                ·  borrow                                ·     144550  ·     429919  ·     403893  ·           15  ·           -  │
···························|········································|·············|·············|·············|···············|··············
|  NFTVault                ·  claimExpiredInsuranceNFT              ·          -  ·          -  ·     104676  ·            1  ·           -  │
```

```
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  closePosition                       ·          -  ·          -  ·      91412  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  collect                             ·      76009  ·      87411  ·      83610  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  disableFloorOverride                ·          -  ·          -  ·      36042  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  finalizePendingNFTValueETH          ·          -  ·          -  ·     227849  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  liquidate                           ·     169865  ·     189478  ·     184575  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  overrideFloor                       ·          -  ·          -  ·      58673  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  repay                               ·      91862  ·     108686  ·      99699  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  repurchase                          ·          -  ·          -  ·     129909  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setBorrowAmountCap                  ·          -  ·          -  ·      36478  ·            2  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setInsuranceLiquidationPenaltyRate  ·          -  ·          -  ·      37249  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setInsurancePurchaseRate            ·          -  ·          -  ·      37227  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setNFTType                          ·          -  ·          -  ·      64964  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setNFTTypeValueETH                  ·          -  ·          -  ·      37147  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setOrganizationFeeRate              ·          -  ·          -  ·      37242  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  NFTVault                  ·  setPendingNFTValueETH               ·          -  ·          -  ·      62529  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  PreJPEG                   ·  grantRole                           ·          -  ·          -  ·      51785  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  PreJPEG                   ·  release                             ·          -  ·          -  ·     148585  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  PreJPEG                   ·  revoke                              ·          -  ·          -  ·     110845  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  PreJPEG                   ·  vestTokens                          ·          -  ·          -  ·     256003  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  approve                             ·      46807  ·      47095  ·      46857  ·           13  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  grantRole                           ·     101252  ·     118736  ·     109410  ·           89  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  mint                                ·          -  ·          -  ·      73544  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  pause                               ·          -  ·          -  ·      47185  ·            2  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  revokeRole                          ·          -  ·          -  ·      46965  ·           24  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  transfer                            ·      32492  ·      49592  ·      41254  ·           10  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StableCoin                ·  unpause                             ·          -  ·          -  ·      25231  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex        ·  deposit                             ·          -  ·          -  ·      85978  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex        ·  grantRole                           ·          -  ·          -  ·      51743  ·           12  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex        ·  harvest                             ·     635854  ·     747869  ·     691862  ·            2  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex        ·  setController                       ·          -  ·          -  ·      29385  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex        ·  setUSDCVault                        ·          -  ·          -  ·      29386  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC20                 ·  approve                             ·      46747  ·      46807  ·      46792  ·           34  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC20                 ·  mint                                ·      56456  ·      73568  ·      72623  ·           73  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC20                 ·  setDecimals                         ·          -  ·          -  ·      26706  ·           12  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC20                 ·  transfer                            ·      54378  ·      54414  ·      54404  ·            5  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC721                ·  approve                             ·      48990  ·      49014  ·      49011  ·           14  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TestERC721                ·  mint                                ·      51930  ·      69030  ·      66461  ·           20  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  allocateTokensForSale               ·          -  ·          -  ·      90012  ·            7  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  deposit                             ·     133365  ·     135611  ·     134488  ·            8  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  depositETH                          ·      67137  ·     155537  ·      84817  ·            5  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  enableWithdrawals                   ·          -  ·          -  ·      48662  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  finalizeRaise                       ·          -  ·          -  ·     131273  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  setSaleSchedule                     ·      70599  ·      70611  ·      70609  ·            6  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  transferToTreasury                  ·          -  ·          -  ·     101861  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenSale                 ·  withdraw                            ·      78795  ·      80891  ·      79843  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenVesting              ·  grantRole                           ·          -  ·          -  ·      51712  ·            6  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenVesting              ·  release                             ·      91748  ·      97005  ·      94377  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenVesting              ·  revoke                              ·          -  ·          -  ·      74599  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  TokenVesting              ·  vestTokens                          ·     139456  ·     168992  ·     152623  ·            7  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  WETH                      ·  approve                             ·      46727  ·      46739  ·      46733  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  WETH                      ·  deposit                             ·          -  ·          -  ·      67962  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  approve                             ·          -  ·          -  ·      46774  ·            6  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  deposit                             ·      73973  ·     134896  ·     119511  ·            4  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  depositAll                          ·      75224  ·     136147  ·     119619  ·           11  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  earn                                ·      81967  ·     143030  ·     122676  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  setContractWhitelisted              ·          -  ·          -  ·      46677  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  setFarmingPool                      ·          -  ·          -  ·      46306  ·           19  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  transfer                            ·          -  ·          -  ·      47378  ·            2  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  withdraw                            ·      72492  ·     116159  ·      94348  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  withdrawAll                         ·      82058  ·     120272  ·      96449  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVault                    ·  withdrawJPEG                        ·      74897  ·     161247  ·     103680  ·            3  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVaultLPFarming           ·  claim                               ·     108258  ·     167348  ·     137803  ·            2  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVaultLPFarming           ·  deposit                             ·     131030  ·     167367  ·     138737  ·            5  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVaultLPFarming           ·  setContractWhitelisted              ·          -  ·          -  ·      46610  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  YVaultLPFarming           ·  withdraw                            ·          -  ·          -  ·      95191  ·            1  ·          -  |
·····························|······································|·············|·············|·············|···············|··············
|  Deployments                                                      ·                                         ·  % of limit   ·             |
····································································|·············|·············|·············|···············|··············
|  Controller                                                       ·    1690923  ·    1690935  ·    1690934  ·        5.6 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  CryptoPunks                                                      ·          -  ·          -  ·    1951136  ·        6.5 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  CryptoPunksHelper                                                ·          -  ·          -  ·    1172380  ·        3.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  FungibleAssetVaultForDAO                                         ·          -  ·          -  ·    1966477  ·        6.6 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  JPEG                                                             ·    2681099  ·    2721007  ·    2706671  ·          9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  JPEGLock                                                         ·     872481  ·     872493  ·     872492  ·        2.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  JPEGStaking                                                      ·          -  ·          -  ·    2672449  ·        8.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  LPFarming                                                        ·          -  ·          -  ·    1810376  ·          6 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  MockBooster                                                      ·          -  ·          -  ·     274014  ·        0.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  MockCurve                                                        ·          -  ·          -  ·     574348  ·        1.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  MockRewardPool                                                   ·     534810  ·     623360  ·     544477  ·        1.8 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  MockStrategy                                                     ·     566473  ·     566485  ·     566482  ·        1.9 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  MockV3Aggregator                                                 ·     537836  ·     537884  ·     537848  ·        1.8 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  NFTVault                                                         ·          -  ·          -  ·    4887472  ·       16.3 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  PreJPEG                                                          ·    3337959  ·    3337971  ·    3337968  ·       11.1 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  StableCoin                                                       ·          -  ·          -  ·    1991118  ·        6.6 %  ·          -  |
····································································|·············|·············|·············|···············|··············
|  StrategyPUSDConvex                                               ·          -  ·          -  ·    3513227  ·       11.7 %  ·          -  |
·································································|··············|··············|················|················|··············
|  TestERC20                                                     ·     2229578  ·     2229734  ·       2229652  ·         7.4 %  ·           -  |
·································································|··············|··············|················|················|··············
|  TestERC721                                                    ·           -  ·           -  ·       1467430  ·         4.9 %  ·           -  |
·································································|··············|··············|················|················|··············
|  TokenSale                                                     ·     2152437  ·     2152461  ·       2152459  ·         7.2 %  ·           -  |
·································································|··············|··············|················|················|··············
|  TokenVesting                                                  ·     1452520  ·     1452532  ·       1452531  ·         4.8 %  ·           -  |
·································································|··············|··············|················|················|··············
|  WETH                                                          ·           -  ·           -  ·        994443  ·         3.3 %  ·           -  |
·································································|··············|··············|················|················|··············
|  YVault                                                        ·     2431440  ·     2431452  ·       2431451  ·         8.1 %  ·           -  |
·································································|··············|··············|················|················|··············
|  YVaultLPFarming                                               ·           -  ·           -  ·       1250370  ·         4.2 %  ·           -  |
·----------------------------------------------------------------|--------------|--------------|----------------|----------------|-------------·

  119 passing (6m)

Failed to generate 3 stack traces. Run Hardhat with --verbose to learn more.
 ✓  Done in 338.67s.
```

Code Coverage

The code coverage is overall very good, statement coverage is above 99%, branch coverage is above 95%, function coverage is above 98% and line coverage is above 99% also.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
escrow/	100	100	100	100	
NFTEscrow.sol	100	100	100	100	
farming/	99.32	98.39	100	100	
LPFarming.sol	100	100	100	100	
yVaultLPFarming.sol	98	95.83	100	100	
helpers/	100	83.33	100	100	
CryptoPunksHelper.sol	100	83.33	100	100	
lock/	100	100	100	100	
JPEGLock.sol	100	100	100	100	
sale/	100	100	100	100	
TokenSale.sol	100	100	100	100	
staking/	100	100	100	100	
JPEGStaking.sol	100	100	100	100	
tokens/	100	100	100	100	
JPEG.sol	100	100	100	100	
StableCoin.sol	100	100	100	100	
vaults/	98.82	88.89	98	99.22	
FungibleAssetVaultForDAO.sol	100	84.62	100	100	
NFTVault.sol	98.56	90.24	97.56	99.05	219,220
vaults/yVault/	100	100	100	100	
Controller.sol	100	100	100	100	
yVault.sol	100	100	100	100	
vaults/yVault/strategies/	100	98.44	100	100	
StrategyPUSDConvex.sol	100	98.44	100	100	
vesting/	100	100	100	100	
PreJPEG.sol	100	100	100	100	
TokenVesting.sol	100	100	100	100	
All files	**99.48**	**96.07**	**99.44**	**99.74**	

Appendix

File Signatures

The following are the SHA-256 hashes of the reviewed files. A file with a different SHA-256 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review.

Contracts

```
d9165f7f4502053bd20a4d6cea3008170894daf40ebb1463e04b3dc763cd6b08 ./contracts/interfaces/IJPEGLock.sol
```

```
b2d9404551b948a257acbcb6fe5d920f3b984f7922c5c69e2812d2ad8f6438e2 ./contracts/interfaces/IFloorOracle.sol
b3a4176580b6b0a3f92b7a4127b9795f06c0c5d2dbc0fc95ff947158430b0480 ./contracts/interfaces/IBooster.sol
bb22662301e43feff8a7846e2926c9fa2d9496ad2dfc83c07ab46a6df13158e0 ./contracts/interfaces/IStableCoin.sol
d2a22c131b871eef31e34b2bcba19894402c7f75de8bbaec06ede7a1febd51ed ./contracts/interfaces/IERC20Decimals.sol
c68bc30dca52adff3a1a8b66942a90610793cbef7903784757407a9cbac6ef32 ./contracts/interfaces/IUniswapV2Router.sol
e5696177afe38a2b170caeb46f0f29a23ca38ece0bbf492ce4571c4f5be0560e ./contracts/interfaces/IFungibleAssetVaultForDAO.sol
dbc7d0fc0bc779ece11ba0d3cc155eaab7ab2f9dd1f221e522206384d8813795 ./contracts/interfaces/IWETH.sol
763be192b9b52acaca11d084d7882ce70af329da92a8872f705dc8891bdedd25 ./contracts/interfaces/IStrategy.sol
ca4b005e880a674761f9ba6108c528598563f727f2b06120d650e9feebc073e5 ./contracts/interfaces/IYVault.sol
da7e5fa14107b8963d04d847015e920995cb0975d8d221becdce612d94cd45b1 ./contracts/interfaces/ISwapRouter.sol
343ba94f8b7203b9fc0e501eac7596a2d8ba7bcfe7f58194196df4d0c66f1f4c ./contracts/interfaces/IUniswapV2Factory.sol
b2ed849e166b7893f67d689f914f7b1cc78ced18baa6c4a04226f9f294462815 ./contracts/interfaces/IBaseRewardPool.sol
29624cf93e464ff66b1d13f2cba705244ce6ecfaaf850fd79628f2c145ddacee ./contracts/interfaces/ICryptoPunks.sol
c9bc8b0e46f5ff397ad2caa7ae3bba44874cccb03560cc8ba91ffc756e21069e ./contracts/interfaces/IUniswapV2Pair.sol
52e5e56ad8cf374d8b267c6831eb22ce593e7e83f684d86be605164b7ad1edd8 ./contracts/interfaces/ICurve.sol
afc8ba365941fab9659cdf48ceb5d16b7e9907b894af20feb88ce9da77c46f10 ./contracts/interfaces/IAggregatorV3Interface.sol
c5cecf95be2c76cb755fb98b931ba7a3e7fff0797755a4bfb77a24af3b8afc6a ./contracts/interfaces/IController.sol
21636dcee5517877362283ab72cd3e34d292092b2c572b205ffe2022d5cba38d ./contracts/helpers/CryptoPunksHelper.sol
af99b5e2fa39e8a81ba1ffadb7d2178b3969c115faaf7563fe3ba81d10a8f956 ./contracts/tokens/JPEG.sol
e57690b38301a3e5d7ad238f95cc2f78d2c567171e49d5b20f96655e057f89e4 ./contracts/tokens/StableCoin.sol
62ba60f100c3155e8f04d7f4aa3f3f17d4db33221ab20871da47d27eeaba6269 ./contracts/escrow/NFTEscrow.sol
a0ad1a21dd075440a0b75a9bd9a02d83250ae9f1922554e25e1f2c8131885917 ./contracts/farming/yVaultLPFarming.sol
e6e497359194c88147f989ebbdf07f92f1822576dc7011f545145716f8a47001 ./contracts/farming/LPFarming.sol
fc3849fe8a3481cc31df18145857f941fc35ef226d4f1bb668df7c5047ec6212 ./contracts/staking/JPEGStaking.sol
199f5c79062740db79beb57cf5213b90097729c20f45958cd3bb541e3c2b4f00 ./contracts/vaults/FungibleAssetVaultForDAO.sol
3417b846e0f392f4953287df91d6588a6df99f25cc083a44b1fb9656c9ee259b ./contracts/vaults/NFTVault.sol
a9e1572d3dd0b07172bc38e8f82a4aea672bf5ab447b6b7f2ba137c6c50474b8 ./contracts/vaults/yVault/Controller.sol
afce0ab800e363be630bb5c8e1a3071c731cacad00a31dcca9d5e13197cea6d9 ./contracts/vaults/yVault/yVault.sol
3cf97e6fa155c149efe43c8c5e9cc9480fee8305026d329dc13ef52303ba91fc ./contracts/vaults/yVault/strategies/StrategyPUSDConvex.sol
da560de20aacdb6fd7a9a6c66f9a70bf1edb94eb86cefa9975b6660969e82966 ./contracts/vesting/PreJPEG.sol
22fad40068bee6bec193f3d040f6bf7e393d98925c6bedc41afb38ce9038f30e ./contracts/vesting/TokenVesting.sol
556172f7eb687f9ea5c4342fa4346f70e44d7dbe96d9691b38aaf6a56e948f9e ./contracts/lock/JPEGLock.sol
9ea89ef750068ec4c19e76d83b47741a12351ea8780d7a031fe4186de835277e ./contracts/test/TestERC721.sol
febfd3edd1957e0589153bce45350f73309e32ba95e0a00ee3d79d509135dff8 ./contracts/test/MockStrategy.sol
ad4ef26ea8ccc3565cf8e28ee513bd1795a3ba04cb5352d8496a0d90d492b343 ./contracts/test/MockBooster.sol
a630d8e8b8db8185865c48a139002bf325243f68bac9f3b74703f0611267e75f ./contracts/test/MockRewardPool.sol
2baa6018e4f4c9a00154018e9328fe984e6353ac6c1392f918bf6f12e7de8c83 ./contracts/test/CryptoPunks.sol
23b3807f1f615a00c70ac8755eb6ef59cc511e3479140eaec80f67b493cad8da ./contracts/test/WETH.sol
10ab190e79a41835b4520bc5e55aadd071b9c77779b34afc301817ac3a5b8763 ./contracts/test/TestERC20.sol
3012cf13bdc586afd6a57ad4c9ff09851e5af19431306709d5533b302382c078 ./contracts/test/MockCurve.sol
50df49831c248de57ecdadec04132a2065eda94a78230b2d361e4440a1c3e3ca ./contracts/test/MockAggregator.sol
cf57574396ab1d1f392c381401fc7e2ea59d2ea17b2e98f1069f3c32cf489414 ./contracts/draft/ERC20Vault.sol
f29adb1273d5049a0c1da7c76c720ec2e753a4613c6627cd3ec06037934d7406 ./contracts/sale/TokenSale.sol
```

Tests

```
916af868c2225c4623f29c2c00cb7c1c1b98d805df998ae848a3d2fad2f9d136 ./tests/PreJPEG.ts
cdf0bbc9c3378a1568971bc30ee9002b930f2f3d49d832e575c17214b9d74941 ./tests/CryptoPunksHelper.ts
5abfd17c454574b7d7f744f1b24e69965fba5a3b7bff5b8bad57d3544a9e960f ./tests/LPFarming.ts
db2a71fccea13d5a259f2b95505dad892c2d026de424e6e323645966f3300f80 ./tests/NFTVault.ts
76513e470ac41ac2ea3df2f03461f1c6d352bad0c059938ba4e54714d2f9e3b8 ./tests/TokenVesting.ts
7570124fe11d57fc4de7710b528e766431964989d65238c88a5c180f74086dae ./tests/FungibleAssetVaultForDAO.ts
ede04591360eb8dba183e1e607ecffc454ea6430ee146c60e5ae0c72d24f9caa ./tests/Stablecoin.ts
0a3f234f29d76d75d966ab9451bb869ea043da1ed42584c3fece62115bac34ed ./tests/yVault.ts
7596c95d0145674bc614fcdb507a83cb79124eb7e91f52772f1013ab12f1982c ./tests/TokenSale.ts
73607f9237eacbfaa01090685df9b2a3d855a57355fb37a0ddda5ded5b0db9db ./tests/JPEGLock.ts
465efe6352d8df16d16e12a9b9874ac90cb7ecc7b0d34f969e6727a595b09e5a ./tests/utils.ts
4a53f5c2a7b6093b1c0fd22276000085a83ffa3f97a6921e6102795cf2b0632b ./tests/JPEG.ts
7d277ec9768ba79be7bcf65b0b12c0d40392015629ac235603971a572a546af5 ./tests/StrategyPUSDConvex.ts
bd0ee29d6273f8b09d4e28a43fdd8b96eacb01868357e8cce69faee16049efc1 ./tests/yVaultLPFarming.ts
2e57a065d04704a562ba2825d3ac8c890926565c0a13e2b00f4b5551dd6b536b ./tests/JPEGStaking.ts
5f2d066235667b5e9dc4a5d3e5f7516d166f37bd96d23cf5e7112709ff4f216b ./tests/Controller.ts
```

Changelog

- 2021-12-22 - Initial report
- 2022-01-21 - Reaudit report (56d7ac1)

About Quantstamp

Quantstamp is a Y Combinator-backed company that helps to secure blockchain platforms at scale using computer-aided reasoning tools, with a mission to help boost the adoption of this exponentially growing technology.

With over 1000 Google scholar citations and numerous published papers, Quantstamp's team has decades of combined experience in formal verification, static analysis, and software verification. Quantstamp has also developed a protocol to help smart contract developers and projects worldwide to perform cost-effective smart contract security scans.

To date, Quantstamp has protected $5B in digital asset risk from hackers and assisted dozens of blockchain projects globally through its white glove security assessment services. As an evangelist of the blockchain ecosystem, Quantstamp assists core infrastructure projects and leading community initiatives such as the Ethereum Community Fund to expedite the adoption of blockchain technology.

Quantstamp's collaborations with leading academic institutions such as the National University of Singapore and MIT (Massachusetts Institute of Technology) reflect our commitment to research, development, and enabling world-class blockchain security.

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp, Inc. (Quantstamp). Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on the website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.