

# Mole Aptos Audit Report



[https://twitter.com/movebit\\_](https://twitter.com/movebit_)



[contact@movebit.xyz](mailto:contact@movebit.xyz)

# Mole Aptos Audit Report



## 1 Executive Summary

### 1.1 Project Information

Type	Yield Farming
Auditors	MoveBit
Timeline	2023-02-07 to 2023-03-09
Languages	Move
Methods	Architecture Review, Unit Testing, Formal Verification, Manual Review
Source Code	Repository: <a href="https://github.com/Mole-Fi/mole-protocol-aptos-dev">https://github.com/Mole-Fi/mole-protocol-aptos-dev</a> Received Commit: e28045f5aa3b5359d6f75ad9ffe117992a5ad9f8 Last Reviewed Commit: 53c832d7a597324ec571005b4688431fe4a894d7

### 1.2 Issue Statistic

Item	Count	Fixed	Pending	Confirmed
Total	10	7		3
Minor	8	5		3
Medium	2	2		
Major				
Critical				

## 1.3 Issue Level

- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

## 1.4 Issue Status

- **Fixed:** The issue has been resolved.
- **Pending:** The issue has been acknowledged by the code owner, but has not yet been resolved. The code owner may take action to fix it in the future.
- **Confirmed:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

## 2 Summary of Findings

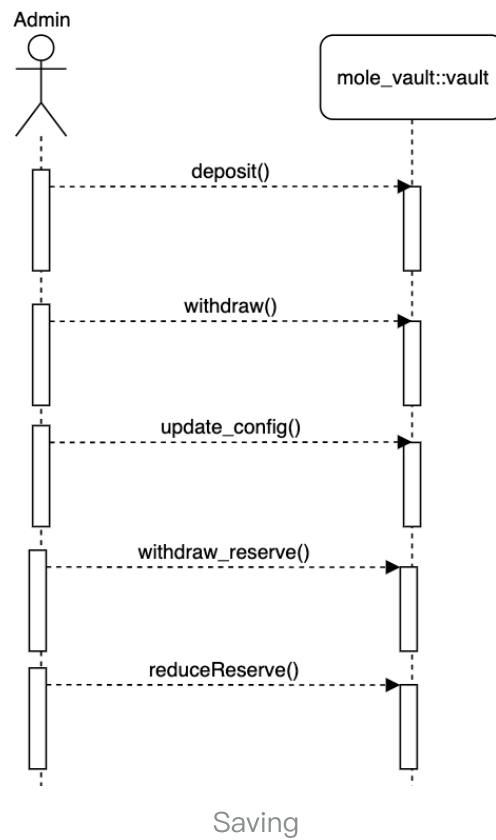
Mole is a DeFi Protocol providing savings, leveraged yield farms and funds.

The audit team read the documents on <https://doc-en.mole.fi/introduction/what-is-mole> and reviewed the code of the Mole Aptos project. The audit team primarily focused on conducting code security and normative audits. The audit team ran code execution tests and business logic security tests on the Aptos test network, and also reviewed and ran unit tests, and had taken took a deep look at the numeric arithmetic operation. The audit team has been in close contact with the developing team for the past two weeks. As a result, the audit team found a total of 10 issues. The audit team and development team have discussed these issues together, and the development team has addressed most of the issues.

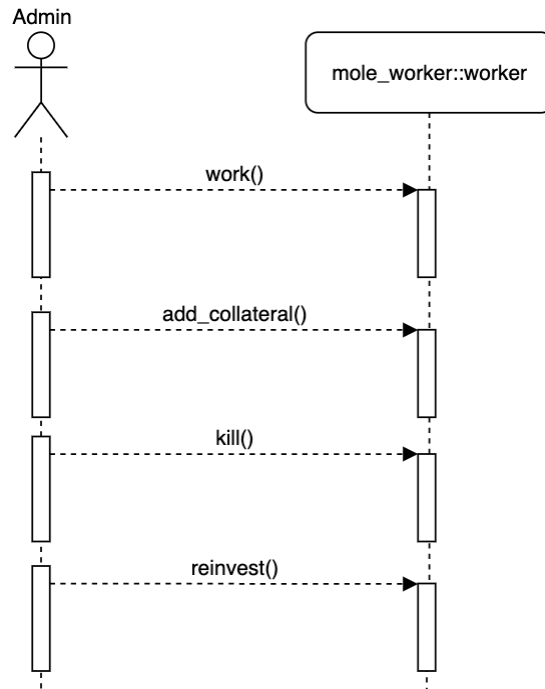
The following are the main roles in the smart contract with their respective capabilities:

### (1) Protocol Admin

- Admin can deposit/withdraw in **Vault** .
- Admin can update the config of the **Vault** .
- Admin can withdraw/reduce reserve in the **Vault** .

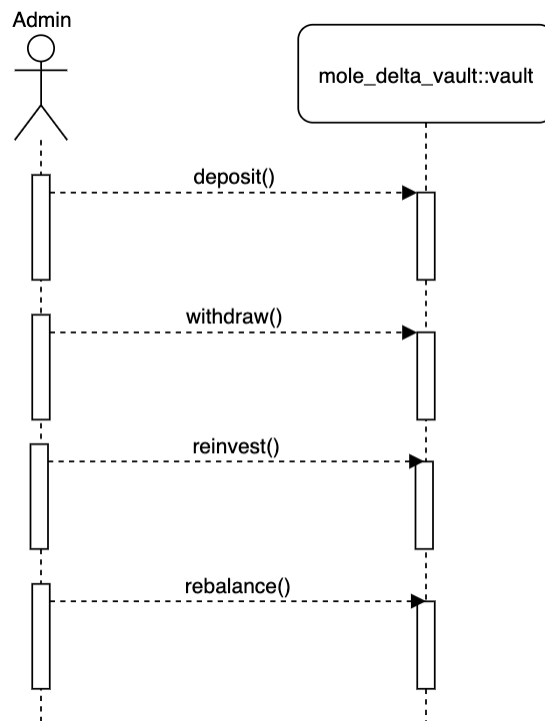


- Admin can create a position in **Farming** .
- Admin can reinvest for yield **Farming** .



Leveraged Yield Farming

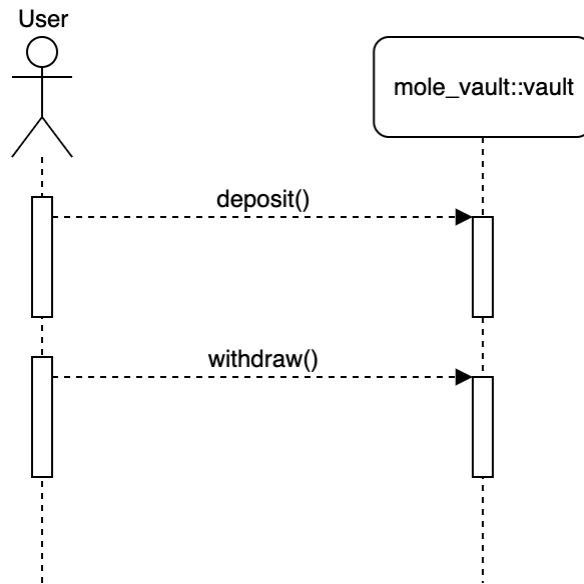
- Admin can deposit/withdraw token to **Fund** .
- Admin can rebalance and reinvest for a **Fund** .



Fund

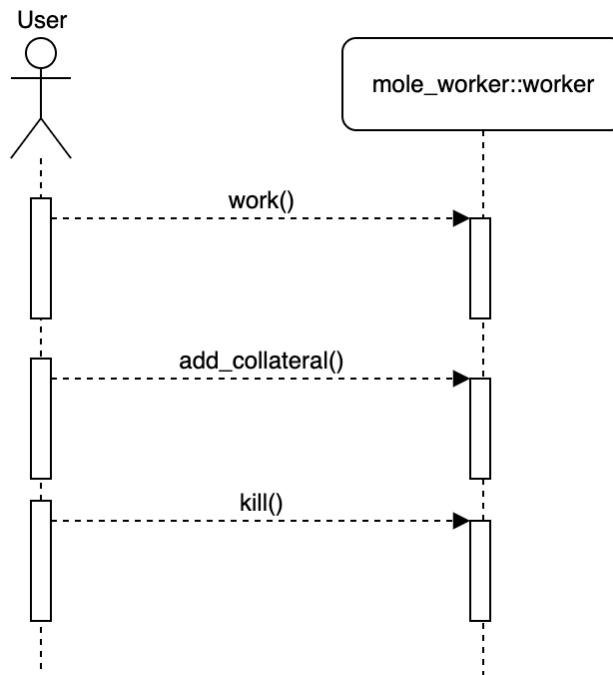
## (2) User

- User can deposit/withdraw in **Vault** .



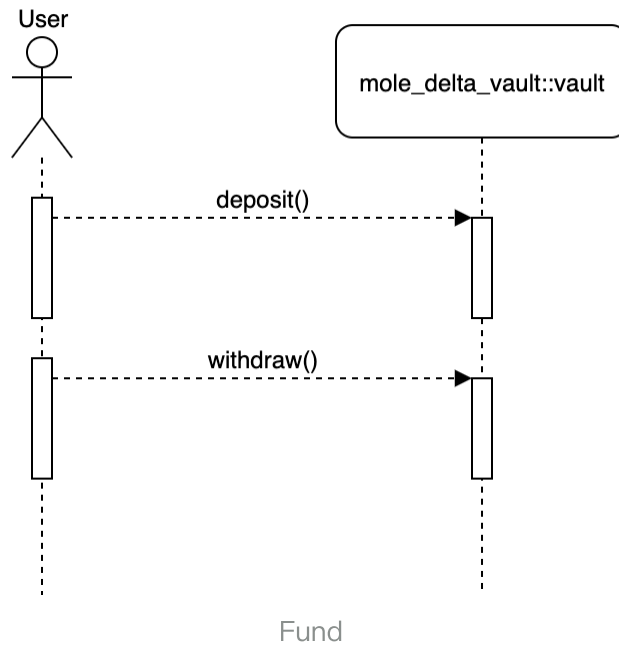
Saving

- User can create a position in **Farming** .
- User can add collateral to a position of user.
- User can kill a position of user.



Leveraged Yield Farming

- User can deposit/withdraw token to **Fund** .



### 3 MoveBit Audit BreakDown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values
- The flow of capability
- Witness Type

## 4 Methodology

The security team adopted the "Testing and Automated Analysis", "Code Review" and "Formal Verification" strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are in the conventions in the "Audit Objective", and that can expand to the context beyond the scope according to the actual testing needs. The main types of this security audit include:

### (1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

### (2) Code Review

Code scope sees **Appendix 1**.

### (3) Formal Verification

Perform formal verification for key functions with the Move Prover.

### (4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time, and they should actively cooperate (which may include the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in time.

## 5 Findings

### 5.1 Assertions can be optimized

**Severity:** Minor

**Status:** Fixed

**Descriptions:** In the `coin::destroy_zero` function, it will be judged whether the balance of the coin is 0, and it will only be destroyed when it is 0, so there is no need to judge whether the value is 0 in the source code.



**Code Location:**

move/snapshot/mole\_pancake/workers/mole\_pancake\_worker/sources/pancake\_worker.move,  
line: 141

```
▼ pancake_worker.move

assert!(
    coin::value(&coin_base_back) == 0,
    error::invalid_argument(ENO_ZERO_BACK)
);

coin::destroy_zero(coin_base_back);
```

**Suggestion:** Delete the assert in the source code.

## 5.2 Lack of the check for coin amount

**Severity:** Minor

**Status:** Fixed

**Descriptions:** According to the parameters of the `deposit` function, the result of the `share` mint to the user in the calculation may be 0. When minting tokens, tokens with a value of 0 should not be minted.

**Code Location:** move/snapshot/mole\_vault/sources/vault.move, line: 312

```
▼ vault.move

if (total == 0) {
    share = amount;
} else {
    let total_supply = option::get_with_default(&coin::supply<MagicCoin<CoinType>>(), 0);
    let share_u128 = (amount as u128) * total_supply / (total as u128);
    share = (share_u128 as u64);
};
mint_magic_coin<CoinType>(account, share);
```

**Suggestion:** Add assert to ensure `share` is always greater than 0 when mint coin.

▼ vault.move

```
1  ...
2  assert(share > 0, err_code)
3  mint_magic_coin<CoinType>(account, share);
```

## 5.3 `strategy_type` missing check

**Severity:** Medium

**Status:** Fixed

**Descriptions:** The functions in `add_collateral` and `work` correspond to different strategies, and the same `wokr_inner` function is called internally. They are controlled by the `strategy_type` parameter to execute different logic. `add_collateral` and `work` correspond to different scenarios. For example, the former corresponds to increasing positions, while the latter corresponds to opening leverage and reducing positions. However, the `add_collateral` function lacks the check of `strategy_type`, which leads to the illogical problem that the reduction strategy can be called.

**Code Location:**

move/snapshot/mole\_pancake/workers/mole\_pancake\_worker/sources/pancake\_worker.move,  
line: 195

▼ pancake\_worker.move

```
1 public entry fun add_collateral<BaseCoin, FarmingCoin, LP>(
2     account: &signer,
3     id: u64,
4     amount: u64,
5     go_rogue: bool,
6     strategy_type: u8,
7     data: vector<u8>
8 ) acquires WorkerInfo {
9     emergency::assert_no_emergency();
10    ...
11    let coin_base_back = work_inner<BaseCoin, FarmingCoin, LP>(
12        account,
13        id,
14        coin_base,
15        debt,
16        strategy_type,
17        data
18    );
19    ...
20 }
```

**Suggestion:** Add corresponding restrictions in the `add_collateral` function.

## 5.4 Wrong error code throw function

**Severity:** Minor

**Status:** Fixed

**Descriptions:** The code uses `permission_denied` to throw error codes. Different errors are thrown in different ways in the source code. Therefore, it is recommended to use `invalid_argument` for parameter errors.

**Code Location:**

move/snapshot/mole\_pancake/workers/mole\_pancake\_worker/sources/pancake\_worker.move,  
line: 320,334

▼ pancake\_worker.move

```
1 assert!(
2     reinvest_bounty_bps <= worker_info.max_reinvest_bounty_bps,
3     error::permission_denied(EEXCEEDED_MAX_REINVEST_BOUNTY_BPS)
4 );
```

**Suggestion:** Use `invalid_argument` to throw an error code.

## 5.5 TinyCoin has no check value upper limit

**Severity:** Minor

**Status:** Confirmed

**Descriptions:** After the swap, there may be a situation where the value of `TinyCoin` is relatively large, which is not tiny enough, so causing some losses to users.

**Code Location:**

snapshot/workers/mole\_pancake\_worker/sources/strategies/pancake\_strategy\_add\_base\_coin\_only.move, line: 107,108

```
▼ pancake_strategy_add_base_coin_only.move

1  public(friend) fun execute<BaseCoin, FarmingCoin, LP>(
2      _user: &signer,
3      coin_base: Coin<BaseCoin>,
4      coin_lp: Coin<LP>,
5      _debt: u64,
6      data: vector<u8>
7  ): (Coin<BaseCoin>, Coin<LP>) acquires TinyCoin {
8      ...
9      merge_to_tiny_coin(coin_base_left);
10     merge_to_tiny_coin(coin_farming_left);
11     ...
12 }
```

**Suggestion:** Determine whether the value of the coin exceeds an upper limit, and if so, transfer it back to the user.

**Confirmed:** Communicated with the developer team, and they designed it in this way. After swap, the value of `Tinycoin` is small enough relative to the input token, and will not cause losses to users. Compared with other solutions, it is more appropriate to keep the current code.

## 5.6 Tokens might not be registered

**Severity:** Minor

**Status:** Fixed

**Descriptions:** In the `kill` function of the `liquidswap_worker` module, there is no check in advance on whether to register the `BaseCoin` token.

**Code Location:**

move/snapshot/mole\_liquidswap\_v2\_workers/mole\_liquidswap\_v2\_worker\_without\_master\_chef/sources/liquidswap\_worker.move, line: 263

▼ liquidswap\_worker.move

```
1 public entry fun kill<BaseCoin, FarmingCoin, LP>(account: &signer, id: u6
  4) acquires WorkerInfo {
2     emergency::assert_no_emergency();
3
4
5     let cap = get_position_operator_cap<BaseCoin, FarmingCoin, LP>();
6     // before kill
7     let kill_context = vault::before_kill<BaseCoin>(
8         account,
9         id,
10        health<BaseCoin, FarmingCoin, LP>(id),
11        is_stable<BaseCoin, FarmingCoin, LP>(),
12        cap
13    );
```

**Suggestion:** Add the `check_and_register_for_liquidator` function at the beginning of the function.

▼ liquidswap\_worker.move

```
1 check_and_register_for_liquidator<BaseCoin>(account);
2
3 fun check_and_register_for_liquidator<BaseCoin>(account: &signer) {
4     let account_addr = signer::address_of(account);
5     if (!coin::is_account_registered<BaseCoin>(account_addr)) {
6         coin::register<BaseCoin>(account);
7     };
8 }
```

## 5.7 Computational Precision Loss

**Severity:** Minor

**Status:** Confirmed

**Descriptions:** The formula in the code is square extraction first and then multiplication, which can be changed to multiplication first and then square extraction if there is no overflow, or the high-precision sqrt function can improve the accuracy.

**Code Location:** move/snapshot/mole\_delta\_neutral/sources/delta\_neutral\_oracle.move, line: 83

▼ delta\_neutral\_oracle.move

```
let total_value = sqrt_k * math::mul_to_u128(2, math::sqrt(px0)) / (NUM_2_31 as u128) * (math::sqrt(px1) as u128) / (NUM_2_31 as u128);
```

**Suggestion:** According to the formula  $\frac{2 \times \sqrt{p_{x0} \times p_{x1}}}{2^{62}}$ , the code can be changed to `2 * math::sqrt(px0 * px1)`.

**Confirmed:** Communicated with the developer team, px0 and px1 is a large number which is bigger than u64, multiplication will cause overflow, and the error is a small number relative to the result, which will not cause user loss.

## 5.8 Dependency Management

**Severity:** Medium

**Status:** Fixed

**Descriptions:** In the `Move.toml` file, the dependent third-party code version is the corresponding branch, and this branch may have continuous development updates. Every time the current project is compiled and deployed, the actual third-party codes it depends on may be different, so it is recommended to modify it to the corresponding git commit version number.

**Code Location:** mole-protocol-aptos-dev/move/snapshot/mole/Move.toml, line: 23,29,34

▼ Move.toml

```
[dependencies]
Pyth = { git = "https://github.com/pyth-network/pyth-crosschain.git", subdir =
  "target_chains/aptos/contracts", rev = "main" }
MoleCoin = { local = "../mole_coins/mole_coin" }
MoleFairLaunch = { local = "../mole_coins/mole_fair_launch" }

[dependencies.AptosFramework]
git = "https://github.com/aptos-labs/aptos-core.git"
rev = "main"
subdir = "aptos-move/framework/aptos-framework"

[dependencies.Switchboard]
git = "https://github.com/switchboard-xyz/sbv2-aptos.git"
subdir = "move/switchboard/"
rev = "main"
```

**Suggestion:** The rev of the third-party dependent code is recommended to be changed to the git version number.

▼ Move.toml

```
[dependencies]
Pyth = { git = "https://github.com/pyth-network/pyth-crosschain.git", subdir =
  "target_chains/aptos/contracts", rev = "0xABCD" }
MoleCoin = { local = "../mole_coins/mole_coin" }
MoleFairLaunch = { local = "../mole_coins/mole_fair_launch" }

[dependencies.AptosFramework]
git = "https://github.com/aptos-labs/aptos-core.git"
rev = "1a87ed5d9ebff44a317bdd0db5c88ab4d1753c45"
subdir = "aptos-move/framework/aptos-framework"

[dependencies.Switchboard]
git = "https://github.com/switchboard-xyz/sbv2-aptos.git"
subdir = "move/switchboard/"
rev = "bdd48565bb5f261417f6b876b39df74b9d039669"
```

## 5.9 Too many repetitive codes

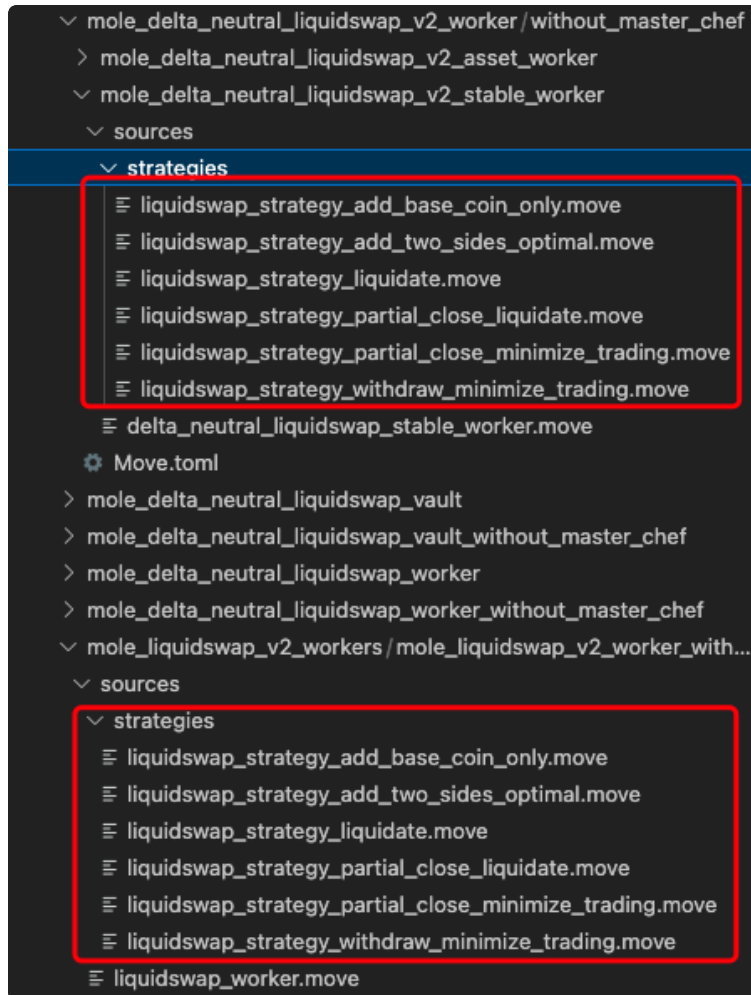
**Severity:** Minor

**Status:** Confirmed

**Descriptions:** The two directories in the screenshot below have more than 90% of the same codes, the code maintenance is more troublesome.

**Code Location:**

move/snapshot/mole\_pancake/workers/mole\_pancake\_worker/sources/strategies,  
move/snapshot/mole\_pancake/delta\_neutral\_workers/mole\_delta\_neutral\_pancake\_stable\_worker  
/sources/strategies.



**Suggestion:** It is recommended to encapsulate it into a common code, and then provide different entrances for the fund and farm business, or use the same entry to distinguish services by parameters.

**Confirmed:** Communicated with the developer team, the project structure is relatively complicated, now this is just a suggestion for the follow-up maintenance of the project party and does not affect the project function, so there is no need to modify it for the time being.



## 5.10 Many **TODOs** in code

**Severity:** Minor

**Status:** Fixed

**Descriptions:** There are still many **TODOs** in code, such as spec files, work, and unit tests which should be completed.

**Suggestion:** Delete the finished **TODOs** comments and completed the remaining todos.

## Appendix 1 – Files in Scope

The following are the SHA1 hashes of the last reviewed files.

./snapshot/mock_coins/sources/coins.move	9998dc2e4e299071b34610084d9f9f711bca7bfff
./snapshot/mole_delta_neutral_liquidswap_vault_without_master_chef/sources/delta_neutral_liquidswap_vault.move	457892935155b2c6c3675b9196437aab50313efd
./snapshot/mole_delta_neutral_liquidswap_vault_without_master_chef/sources/delta_neutral_liquidswap_vault_gateway.move	886dc87db9204a364d0d3489b9267f83fb518762
./snapshot/mole_delta_neutral_liquidswap_vault/sources/delta_neutral_liquidswap_vault.move	07e72eb81095e3780253d0db6ac6693fa8908371
./snapshot/mole_delta_neutral_liquidswap_vault/sources/delta_neutral_liquidswap_vault_gateway.move	886dc87db9204a364d0d3489b9267f83fb518762
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/liquidswap_worker.move	2c3a5bcf46caf2d784f1be73954e5ea0a9777b99
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	c3ecf683928370a7882b29b232fb0a818b8917c5

./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_add_base_coin_only.move	1ef4de39f0d52a82ebb1a8a859777ab5ac914520
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	52d5536dc6b828d1c693a656fc4a74a4d966e16c
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_liquidate.move	148d73440a77b79e4efa91a6efee1cad34049cda
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	8ffd04fc72fb98b6af2fa89859e6b9e498399feb
./snapshot/mole_liquidswap_v2_workers/mole_liquidswap_v2_worker_without_master_chef/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	796eab70e8c81b3d3d5654338dc15cd99ebade15
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/delta_neutral_liquidswap_asset_worker.move	265d7976f0db154df30fd2daa7c71db0a26da5c6
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	751a63962100dc0e442448f95a9b213ba2255eac
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	d5b9dc2cd0091ba30a4d155fcbaa3c02b9daa3ab

./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	4d1b28bf6006de28ccf833a065f14470adfb603f
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_liquidate.move	dd0c8efa5be4884e20af86ee2100acd76935e4e1
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	c79b2c23f6b5ca9551c7d09bd475f8919465f6a4
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	3656db3a46fe88933a058e6a23f1d54d425b8193
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	a06de20a138fb5a14893c62952129f0ffc4b1634
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	91242549859215d97919a3a8cf787e78634e61f2
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	9424b5b709cd73be02359b8074e9b2f2b4a80003
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_liquidate.move	8a924383df56f29ad544300f9475f4beba15ca9b

./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	452c58792795e8c0c0141af47b5605bbf0a60412
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	405f6e53f68711c4463391a207b471f4980f9714
./snapshot/mole_delta_neutral_liquidswap_worker/mole_delta_neutral_liquidswap_stable_worker/sources/delta_neutral_liquidswap_stable_worker.move	5f2be4227a85767e53ce259bf1d29070b4841731
./snapshot/mole_coins/mole_coin/sources/mole_coin.move	ec0b1e7f6be48f3861f3aec83131fb75290a46b7
./snapshot/mole_coins/mole_fair_launch/sources/fair_launch.move	e587886e6da452267e4ad5d067d00f3cb1af7bda
./snapshot/mole_coins/mole_fair_launch/sources/fair_launch_emergency.move	52e85ef6bfdd5a1b5f8294f3f0a49499326b7a26
./snapshot/mole_worker/sources/worker_config.move	74c27c9e89201c689616cac1d70b7eca822a12c2
./snapshot/mock_coin/tests/mock_coin_test.move	0a32f85ee75e24138b12d087c83ad6ca9bbd0b54
./snapshot/mock_coin/sources/mock_coin.move	853ee1a4a9c32fd777d0e562314b9b981c067d68
./snapshot/mole_delta_neutral/tests/managed_directional_vault_config_test.move	0105d898f99c96859151c99200131413717a78b5
./snapshot/mole_delta_neutral/tests/delta_neutral_oracle_test.move	8064912a706eb6808c8ffa027d9ae6131c3ac52b
./snapshot/mole_delta_neutral/tests/managed_delta_neutral_vault_config_test.move	fb43fe6a94cc1ddd78195f0f7f8892124f1736b8

./snapshot/mole_delta_neutral/tests/manage_d_delta_anchor_vault_config_test.move	06a7de68b355b5b47b2c208172b49b6aa9a491cb
./snapshot/mole_delta_neutral/tests/delta_neutral_vault_config_test.move	99e6f6396ab72443bbc658c19c258cf3164aecf0
./snapshot/mole_delta_neutral/sources/delta_anchor_vault_config.move	ea8bc9ecea4d72c1bfc73666ed9b64c1240264ca
./snapshot/mole_delta_neutral/sources/delta_neutral_vault_config.move	8258bbbedeb9ec92dbf9b9103d20fbc538272d155
./snapshot/mole_delta_neutral/sources/managed_delta_neutral_vault_config.move	8f94eb0d4967e2947f4f5e8b70a6e70ad05d989e
./snapshot/mole_delta_neutral/sources/delta_neutral_oracle.move	08eca6d17a04adccb80677f8c55b203b35be75cd
./snapshot/mole_delta_neutral/sources/managed_directional_vault_config.move	624815c6dec48aed980520856b9d6c1f6c822f91
./snapshot/mole_delta_neutral/sources/managed_delta_anchor_vault_config.move	e3c7ecc6a87c17914ab227544d13152f1e9a103d
./snapshot/mole_delta_neutral/sources/directional_vault_config.move	7fd90859c942b5940d04e592bebcd65c04cd7315
./snapshot/mole_simple_oracle/tests/simple_price_oracle_test.move	eda364ad280837d81878c3df778ec33475d04a37
./snapshot/mole_simple_oracle/sources/simple_price_oracle.move	e5d3bf67bb9a3dd821ffe24656c8405ddd6aaf42
./snapshot/miscellaneous/tests/miscellaneous_test.move	ee022c3269422f070274a8466b39381aaf8ed498
./snapshot/miscellaneous/sources/miscellaneous.spec.move	3d1b453b1516e4704cf77d049c6e537618251d06
./snapshot/miscellaneous/sources/gas_measure.move	ae477f80ede2f300a842959231b154d667ee73ba
./snapshot/miscellaneous/sources/miscellaneous.move	0cdab6cf1d351065d1e04eab4fc7c37b2f19c596

./snapshot/mole_delta_neutral_liquidswap_v2_vault/without_master_chef/mole_delta_neutral_liquidswap_vault/sources/delta_neutral_liquidswap_vault.move	c141e1cd6c5ffe18651708646e859050910d584c
./snapshot/mole_delta_neutral_liquidswap_v2_vault/without_master_chef/mole_delta_neutral_liquidswap_vault/sources/delta_neutral_liquidswap_vault_gateway.move	818769ecbba50bda2cfb8471d029dd9ddb6c057d
./snapshot/mole_liquidswap_worker_without_master_chef/tests/liquidswap_worker_without_master_chef_test.move	b03585a6a3df39a0b7e91b6b28a192f67ce4cfbe
./snapshot/mole_liquidswap_worker_without_master_chef/sources/liquidswap_worker.move	86e83b0849020eb5e7bd69ad61c8f1319a6901d8
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	d5a853a8780fe4135adbd213e2016c92ac54e689
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_add_base_coin_only.move	01123864a0a254afb41810b54222862ae49637e1
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	41a6bc64dc49c18570c512c97359b9d6964ae1e4
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_liquidate.move	dc995084e81414f294b0589ce4a46a824b546f4d
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	b3d0302ea7f15180b4fada9b33bedd7be7439cec
./snapshot/mole_liquidswap_worker_without_master_chef/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	7aaf2187e6a9c084c897c760b9d57360aa7c5580

./snapshot/mole_liquidswap_worker/tests/liquidswap_worker_test.move	cd916f07f3460e39256ab55a50af62a0f817b270
./snapshot/mole_liquidswap_worker/sources/liquidswap_worker.move	e9236f07f64b4df2d16429f0d39816df00b81d97
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	a87609bdbbe36e844f01e25432d19ab20dcd0f563
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	4402ccc2a6364e9a82953dc55fd9e803ce29bf4e
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	ed7f46c44714b535cd2cae2a5d3bfacf415e64ba
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_liquidate.move	7f2d918e81573b50ac3b0d4664710f3f65471631
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	aaac1017efcd9cfc7db5fe028f814362617c18b0
./snapshot/mole_liquidswap_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	51a5abd9fff922114a4aaabe840c767d8c99fbf5
./snapshot/mole_liquidswap_worker/sources/liquidswap_worker_without_master_chef.move	3797134232f7a682071294719560b6a629daf52f
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	03c0ef3a9b1ae783e9683a2b5ede577ec70d2847

./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	52aa92b7415cf0913a64196003387f1e4764fb14
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	07ee406c0cfa4ae70232f46d0bd9c36b0b91c1f5
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_liquidate.move	7f592ba13a1b48168dacb19c66355234395490e0
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	84c122c86cf3cf46d87c8c2c669a01163692b90b
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	7fbdbff83a7cc990323fde10e27ddc808f658852
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_stable_worker/sources/delta_neutral_liquidswap_stable_worker.move	68999db52245b5b94b9c57b0d9e21e3da4df5086
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/delta_neutral_liquidswap_asset_worker.move	0786bb4befda833d308c4b4e6d6d0c503bf2422b



./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	ac7cc36844fe1e8c20f0f852487bfa649a51d381
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	55fbefac806599fe4fbad6295b23e4ed667978e0
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	9705bb5a84cfd9f1c6df23b45ac1767438196909
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_liquidate.move	8d7e755272fa34080cb83f3e77a08123bb6a0fe8
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	ade4fd48dd31490dbd213020bbd190699c40b79b
./snapshot/mole_delta_neutral_liquidswap_v2_worker/without_master_chef/mole_delta_neutral_liquidswap_v2_asset_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	6875e7bb89d326a374c9716a2e733367a30e7ec6
./snapshot/mole_pancake/delta_anchor_vaults/mole_delta_anchor_pancake_vault/sources/delta_anchor_pancake_vault.move	147d5e174043175269e2f91814c7e31d196200fc

./snapshot/mole_pancake/delta_anchor_vaults/mole_delta_anchor_pancake_vault/sources/delta_anchor_pancake_vault_gateway.move	c607a3feab144651683d12579ce068004a10df57
./snapshot/mole_pancake/common/sources/pancake_utils.move	28aeebfcb5da604a520f3b85c031b05f3748c26a
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_add_base_coin_only.move	4822974c9ed6b126cf648d585ef3094965e4d8a4
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_with_draw_minimize_trading.move	583e67ebe29bbeb9284228aa5699011ecda9bdf6
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_liquidate.move	ff56a295ef8fdc75591aafa698759926f9481b0a
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_add_two_sides_optimal.move	d3b6ebe93c3156d03bc8f637775802df9dcbc963
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_partial_close_minimize_trading.move	037850fc85ac501887fed764fb980e3959e443c6
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/strategies/pancake_strategy_partial_close_liquidate.move	27f5eb4943628895f36b642dea973bfe4758d421
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_stable_worker/sources/delta_neutral_pancake_stable_worker.move	cfc2029d4237ba0b9d8ad091f47c4d5de1f043d2

./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_add_base_coin_only.move	d9e1a775868de68c4f1d003602b1cb71ccdc9c51
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_withdraw_minimize_trading.move	3b70c056a95f7b65161a64ba45c463a6fabcad4a
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_liquidate.move	40aa1cbeaeff0a16cc309f1dfbbb564eb6f89a4c
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_add_two_sides_optimal.move	a6c73fd2b126c55f6da7038a6ef6e308422a487d
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_partial_close_minimize_trading.move	a7e84363453ae2c8377676e762272fc3700ce9d6
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/strategies/pancake_strategy_partial_close_liquidate.move	0c9805cd46696d49983c74eb2d0c1e198e3d0efa
./snapshot/mole_pancake/delta_neutral_workers/mole_delta_neutral_pancake_asset_worker/sources/delta_neutral_pancake_asset_worker.move	8a3505569ef76027a5ca2b4a1173aaf0826aa7fe
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/pancake_worker.move	07445065d67d869be610f7b2433976f8dd5b3648
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_add_base_coin_only.move	82f9d180fc8de2039a773d7fb1cb23488ea8f291

./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_withdraw_minimize_trading.move	2d5a3f5f912b99227212cce91779b2b70f80356f
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_liquidate.move	d470a05d726f78381ee88a9bda98b3d2fec6b441
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_add_two_sides_optimal.move	6dd513d7231bb87a8382492adc3585bd29a06126
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_partial_close_minimize_trading.move	c1fa6c593c508a2103c3c563bd74a3f4f44401ac
./snapshot/mole_pancake/workers/mole_pancake_worker/sources/strategies/pancake_strategy_partial_close_liquidate.move	611ac7d7fa03511558e99c652b32ebc17addfd62
./snapshot/mole_pancake/delta_neutral_vaults/mole_delta_neutral_pancake_vault/sources/delta_neutral_pancake_vault_gateway.move	bcbdd2c29ab29616aaefcb06e4b70ed719c45f3c
./snapshot/mole_pancake/delta_neutral_vaults/mole_delta_neutral_pancake_vault/sources/delta_neutral_pancake_vault.move	811679bfed78b796e81ee85776246d0b4e41266f
./snapshot/mole_pancake/directional_vaults/mole_directional_pancake_vault/sources/directional_pancake_vault.move	62cca90ffbe4148dd85417ba4adf68b4a1f3f552
./snapshot/mole_pancake/directional_vaults/mole_directional_pancake_vault/sources/directional_pancake_vault_gateway.move	5177f181b115debe0853d8b5135506f6c25cdf3d
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/delta_neutral_liquidswap_asset_worker.move	9ad607d9c6f1ceed25d61dbe7c77025c9b61e5d0

./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	751a63962100dc0e442448f95a9b213ba2255eac
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	d5b9dc2cd0091ba30a4d155fcbaa3c02b9daa3ab
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	4d1b28bf6006de28ccf833a065f14470adfb603f
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_liquidate.move	dd0c8efa5be4884e20af86ee2100acd76935e4e1
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	c79b2c23f6b5ca9551c7d09bd475f8919465f6a4
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_asset_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	3656db3a46fe88933a058e6a23f1d54d425b8193

./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_withdraw_minimize_trading.move	a06de20a138fb5a14893c62952129f0ffc4b1634
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_add_base_coin_only.move	91242549859215d97919a3a8cf787e78634e61f2
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_add_two_sides_optimal.move	9424b5b709cd73be02359b8074e9b2f2b4a80003
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_liquidate.move	8a924383df56f29ad544300f9475f4beba15ca9b
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_partial_close_minimize_trading.move	452c58792795e8c0c0141af47b5605bbf0a60412
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/strategies/liquidswap_strategy_partial_close_liquidate.move	405f6e53f68711c4463391a207b471f4980f9714
./snapshot/mole_delta_neutral_liquidswap_worker_without_master_chef/mole_delta_neutral_liquidswap_stable_worker/sources/delta_neutral_liquidswap_stable_worker.move	ad1129f8ebe69f0abe47d1df0b886291ed2649f9

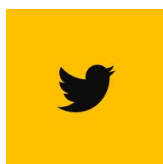
./snapshot/mole_vault/tests/vault_config_test.move	10abb26e0ac63be823fd5acd84c2e5dc65afb3ba
./snapshot/mole_vault/tests/vault_test.move	ea360b1246e7f0681d74bd2e0ba19fd9ee92b839
./snapshot/mole_vault/tests/managed_vault_config_test.move	497f50dc6fa80a9fcf98e2e7b6bfb070846f4b63
./snapshot/mole_vault/sources/managed_vault_config.move	0942811349aad20f69c16830a04b17cebad2a28e
./snapshot/mole_vault/sources/vault_config.move	264b594d564604a3ec9dcfe8c96f0a01e919a1bc
./snapshot/mole_vault/sources/vault.move	28e2a4d5f5344ff46f4ea51298a6425dc11fb518
./snapshot/mole/sources/utils/coder.move	a22ebe4f472bd7474d673fe0e6843e62a9421351
./snapshot/mole/sources/utils/coder.spec.move	e8c629e9eb340e42335589dc37b9410bd9fe6306
./snapshot/mole/sources/utils/math.move	102ed5ec61ff8be2a5280c07fbe1915c2e2930a8
./snapshot/mole/sources/utils/deployer.move	ef05d98c2b9c7fa6028f0edd0fc15c4177e8858b
./snapshot/mole/sources/utils/coin_converter.move	171682e36b78037ee92f4c6f2c57b10c60e2593c
./snapshot/mole/sources/switchboard_oracle.move	a18dbfbc9d0302601ebfff0b3ddba13da11a8831
./snapshot/mole/sources/emergency.move	0d60fba0c3cf1cb68727cfa22633fc672f5264e9
./snapshot/mole/sources/price_oracle.move	c97f594c97450fcdf2477c33f32a8d42a8231844
./snapshot/mole/sources/pyth_oracle.move	ab5912b77fab78cc9d0b771b5b3cc4cefa3f1371

./snapshot/mole/sources/interest_model.move	5c3ffb55de4bc1f1574f6a486478ff5e2a213c71
./snapshot/mole/sources/triple_slope_model.move	f87d3a01c082b7dcebb05607d389bf0252adca0e
./snapshot/mole/sources/mole_addresses.move	a1dcb7055d9d5adc593b791c4604983e6f701267
./snapshot/mole/sources/oracle_medianizer.move	46e65072560e929d9def66b707436f4f4b61b212
./snapshot/dex_master_chef/tests/master_chef_test.move	844fe2e1161482416ed5631e325356e360db4469
./snapshot/dex_master_chef/sources/dex_coin.move	f55404135e0005e46df4a438c7fc89718db4880d
./snapshot/dex_master_chef/sources/master_chef.move	049110605baeda3afcebc7b708d73abf9a6700b93
./snapshot/deps_list/tests/index_test.move	c383bed58adf09de78d77da808242f75a3abb586

## Appendix 2 – Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include 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 own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.





[https://twitter.com/movebit\\_](https://twitter.com/movebit_)



[contact@movebit.xyz](mailto:contact@movebit.xyz)

---