



April 25th 2020 — Quantstamp Verified

KeeperDao

This smart contract audit was prepared by Quantstamp, the protocol for securing smart contracts.

Executive Summary

Type	Smart contract				
Auditors	Sung-Shine Lee, Research Engineer Leonardo Passos, Senior Research Engineer Kacper Bqk, Senior Research Engineer				
Timeline	2020-04-15 through 2020-04-21				
EVM	Muir Glacier				
Languages	Solidity, Javascript				
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review				
Specification	README.md				
Source Code	<table><tr><th>Repository</th><th>Commit</th></tr><tr><td>keeper-sol</td><td>edd235d</td></tr></table>	Repository	Commit	keeper-sol	edd235d
Repository	Commit				
keeper-sol	edd235d				
Goals	<ul style="list-style-type: none">• Business logic review• Specification and documentation review• Identify accounting errors				
Changelog	<ul style="list-style-type: none">• 2020-04-21 - Initial report				

Overall Assessment

KeeperDao is a set of smart contracts to lock funds in different investment protocols (currently, only Compound), providing flash loans on top of locked funds.

During the audit, Quantstamp identified errors in funds transfer that could result in reverting flash loans, and incorrect accounting of the internal state. Input validation is not performed on various functions and some return values from external calls are not checked, both of which could cause errors in the internal state as well.

The audited implementation does not have a local testing environment. A testnet environment exists for Kovan, but executing the deployment scripts and testing scripts for Kovan network resulted in numerous errors. Additionally, the tests that are present do not check the internal state of the smart contracts and only detect if a transaction reverted or not. Quantstamp would stress that some of the issues identified above could have been detected by having tests that check the internal state.

Altogether, Quantstamp identified 12 issues: 3 are high-severity, 3 are medium severity, and 2 are low-severity issue. One finding is marked as "undetermined". The remaining findings are informational.

Total Issues	12	(0 Resolved)
High Risk Issues	3	(0 Resolved)
Medium Risk Issues	3	(0 Resolved)
Low Risk Issues	2	(0 Resolved)
Informational Risk Issues	3	(0 Resolved)
Undetermined Risk Issues	1	(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.
ℳ 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).
ℳ Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.

Summary of Findings

ID	Description
QSP-1	Lack of unit and functional tests
QSP-2	Flash lend may revert unexpectedly
QSP-3	Incorrect math and funds transfer when user borrows
QSP-4	Race Conditions / Front-Running
QSP-5	Return values of external calls are not checked
QSP-6	Lack of input validation
QSP-7	Centralization of Power
QSP-8	'Dead' Code
QSP-9	Unlocked Pragma
QSP-10	Fee can be lost (partially or in full) due to integer division.
QSP-11	Clone-and-Own
QSP-12	Potential incorrect accounting when misusing <code>register()</code>

Severity	Status
⚠ High	Unresolved
⚠ High	Unresolved
⚠ High	Unresolved
⚠ Medium	Unresolved
⚠ Medium	Unresolved
⚠ Medium	Unresolved
✓ Low	Unresolved
✓ Low	Unresolved
ℳ Informational	Unresolved
ℳ Informational	Unresolved
ℳ Informational	Unresolved
? Undetermined	Unresolved

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:

- [Truffle](#)
- [Mythril](#)
- [Truffle-Flattener](#)
- [Securify](#)
- [Slither](#)

Steps taken to run the tools:

1. Installed Truffle: `npm install -g truffle`
2. Flattened the source code using `truffle-flattener` to accommodate the auditing tools.
3. Installed the Mythril tool from Pypi: `pip3 install mythril`
4. Ran the Mythril tool on each contract: `myth -x path/to/contract`
5. Ran the Securify tool: `java -Xmx6048m -jar securify-0.1.jar -fs contract.sol`
6. Installed the Slither tool: `pip install slither-analyzer`
7. Run Slither from the project directory `slither .`

Assessment

Findings

QSP-1 Lack of unit and functional tests

Severity: *High Risk*

Status: Unresolved

Description: Unit tests and functional tests are important to ensure the correctness of the application during development. This is particularly important for projects that manages users' funds. The project severely lacks unit testing and functional testing. Additionally, the functional tests that are present only check if a transaction goes through -- i.e. they only check if the transaction reverts or not. Internal state changes of the smart contract system are not checked. During the audit, Quantstamp team has identified issues that could be prevented by having tests.

Recommendation:

1. While it is hard to set up the entire external system in a local testing environment, we recommend developing mocks to simulate some basic scenarios for unit tests.
2. Assert the expected state changes to ensure the internal calculations are correct.
3. Develop unit tests to ensure each function is working properly, have mocks to establish local functional tests and test edge cases. Have basic functional tests on Kovan that can be used to cross verify if the mocks are implemented correctly.

QSP-2 Flash lend may revert unexpectedly

Severity: *High Risk*

Status: Unresolved

File(s) affected: `CompoundKeeper.sol`

Description: The function `borrow()` may fail in line 178 upon calling `_payFee()` and before `_give()` gets executed. While in general the contract may hold some tokens, it is possible that the contract has none. Consequently, the execution would fail since the fee gets paid before the borrowed tokens are transferred back.

Exploit Scenario: This is what happens in the function `borrow()`:

1. `_take`: tokens are taken out from the Compound and **transferred** to the `_receiver`
2. `_receiver.flashLend`: `_receiver` **approves** `compoundKeeper` to transfer the amount that equals the borrowed tokens plus loan fees. Note that the amount is only approved, but not transferred back.
3. `_payFee()`: `compoundKeeper` transfers some `managementFee` to `feeCollector`. Since it performs `safeTransfer` instead of `TransferFrom`, the token is transferred from the `compoundKeeper` to the `feeCollector`. It is important to realize that since the token in step 2 is not yet transferred back, the contract will fail at this step if it doesn't hold enough funds to pay the `feeCollector`

Recommendation: Transfer all the tokens back then transfer the fee to the `feeCollector`, or directly transfer the fee from the `_receiver` to the `feeCollector`.

QSP-3 Incorrect math and funds transfer when user borrows

Severity: *High Risk*

Status: Unresolved

File(s) affected: [CompoundKeeper.sol](#)

Description: Currently, it is possible that the keeper does not make a profit when providing a flash loan; thus, the keeper can accumulate debt and with time, funds can be severely compromised. Debt occurs due to the fact that `_amount + loanFee >= managementFee(_amount) + platformFee(_amount)` does not always hold. It is important to note that `approve()` does not `transfer` the funds. It only gives the keeper the right to `transfer`, but the funds itself are still in user's account. In some fee structure settings, it is possible for the Keeper to lose money after borrowing money to others.

Exploit Scenario: Here is the breakdown: * `_take()`: The keeper transfers `amount` Tokens to `_receiver`

- `flashLend()`: `_receiver` performs some actions, then **approves** the `addFee(amount, flashLoanFeeInBips)`, as in [FlashLoanReceiver.sol, L13](#)
- `_payFee()`: The keeper calls the function `safeTransfer`, and thus the keeper transfers `managementFee(amount)` Tokens to `feeCollector`
- `_give()`: The keeper uses `transferFrom` and thus orders the `_receiver` to transfers `_amount + platformFee(_amount)` tokens to the compound protocol.

Thus, the keeper actually only receives `_amount + platformFee(_amount) - managementFee(amount)`. Looking at the math, the keeper should have received `_amount + platformFee(_amount)`. To give you a concrete example, we have identified a case where the `keeper` would lose money using Z3 prover, consider the following case:

- `borrowedAmount` = 10001
- `flashLoanFeeInBips` = 20006
- `managementFeeInBips` = 5001

Under the condition above, we would get:

- `managementFee` = 10006
- `platformFee` = 10001,

Thus, the `keeper` loses money as the `platformFee < managementFee`

Recommendation: Instead of transferring the funds to the `feeCollector` from the keeper directly, use `transferFrom` to move the funds from the [FlashLoanReceiver](#). Alternatively, consider other fixes that would make the math correct. Also, this issue could have been easily identified if there were tests that check the internal state. We strongly recommended adding tests to identify similar problems.

QSP-4 Race Conditions / Front-Running

Severity: *Medium Risk*

Status: Unresolved

File(s) affected: [CompoundKeeper.sol](#)

Description: A block is an ordered collection of transactions from all around the network. It's possible for the ordering of these transactions to manipulate the end result of a block. A miner attacker can take advantage of this by generating and moving transactions in a way that benefits themselves.

Here, the operator can front-run the borrower and cause them to pay higher fee than expected. As there are no restrictions on `flashLoanFeeInBips`, it is possible for the operator to set the fee to a significantly large number and, essentially, take all the funds from a [FlashLoanReceiver](#).

Exploit Scenario: Bob calls `borrow()` to get a flash loan. At this point, Bob assumes the flash loan fee to be x. The operator, maliciously or not, submits a transaction to update the loan fee to a value greater than x. The operator front-runs Bob by setting higher gas price. Bob's flash loan transaction is mined afterward; consequently Bob pays higher fee than expected.

Recommendation: 1. Consider restricting the `flashLoanFeeInBips` to a reasonable range

1. Consider letting the borrower specify the maximum fee they are willing to pay as an argument to the `borrow()` function. Then, within the `borrow()`, require that the `flashLoanFeeInBips` is smaller than the argument.

QSP-5 Return values of external calls are not checked

Severity: *Medium Risk*

Status: Unresolved

File(s) affected: [CompoundKeeper.sol](#)

Description: * For a market that is not WETH, `deregister()` does not check the return value of `exitMarket` (L124). If unchecked, data will be deleted when none should be (L125-126)

- In the `register()` function, the return value of entering a market is not verified (L109). According to <https://compound.finance/docs/comptroller#enter-markets>, “for each market, returns an error code indicating whether or not it was entered. Each is 0 on success, otherwise an Error codes”. Currently, any error will go silent and the `register()` will not revert.

Recommendation: Use a `require()` statement to check the return value and ensure that there is no internal error from Compound. In general, check all return values from external calls.

QSP-6 Lack of input validation

Severity: *Medium Risk*

Status: Unresolved

File(s) affected: [CompoundKeeper.sol](#)

Description: Input validation is important to avoid wrongly initialized resources. The contracts, in general, lack input validation. Some other findings in this report are also caused by them. Here are a few others:

- [updateFeeCollector\(\)](#) does not check if [_newFeeCollector](#) is different from 0x0. If equals to 0x0, tokens will effectively be burned when fees are paid (see [_payFee\(\)](#))
- [initialize\(\)](#) does not check if [_weth](#) is different from 0x0; if [_weth](#) is [0x0](#), a new deployment must occur.
- [deposit\(\)](#), [withdraw\(\)](#), and [borrow\(\)](#) do not check if [_token](#) has been previously registered with the platform. Not performing this check will cause callers to waste gas, as the transaction will fail along the way.
- [deposit\(\)](#) does not check if [_token](#) is different from 0x0

Recommendation: Add input validation to the functions to ensure proper data has been provided to the contract.

QSP-7 Centralization of Power

Severity: *Low Risk*

Status: Unresolved

Description: Smart contracts will often have variables to designate the person with special privileges to make modifications to the smart contract. In the scope of this audit:

- KToken is NOT deployed by CompoundKeeper and CoreKeeper. It has to be manually registered into the system by operators. However, these operators are still the owners and minters of the KTokens that are registered in the system, thus they can arbitrarily mint any amount of KToken and claim nearly all of the funds that are kept in the keepers.
- Operators can overwrite a previously stored kToken using [register\(\)](#) function. It is unclear whether this is an intended functionality.
- Operators can use [deregister\(\)](#) to delete a kToken at any point, causing the users to have funds being locked up in the keeper contract.

Recommendation: This centralization of power needs to be made clear to the users, especially depending on the level of privilege the contract allows to the owner. Consider changing the architecture to remove such possibility, or explicitly document the centralization issues and the steps taken to mitigate them.

QSP-8 'Dead' Code

Severity: *Low Risk*

Status: Unresolved

Description: "Dead" code refers to code whose execution makes no impact on the final result. Dead code raises a concern, since either the code is unnecessary or the necessary code's results were ignored.

- [gasToken](#) and [gastokenAmount](#), [updateGastoken\(\)](#), [updateGastokenAmount\(\)](#) don't seem to be used.
- [_giveEth\(\)](#) and [_giveERC20\(\)](#) try to repay some owed money. As per current implementation, the lender always pays back the loan at the end of the transaction, thus it is not possible for the keeper to owe the compound protocol funds. It is unclear why the logic is present.
- In [KeeperRoles.sol](#), functions and variable related to the role [_borrowers](#) are never used.

Recommendation: We recommend removing code which is unused. The code which you plan to use in future versions should be separated from the production code and placed in a Pull Request.

QSP-9 Unlocked Pragma

Severity: *Informational*

Status: Unresolved

Description: Every Solidity file specifies in the header a version number of the format [pragma solidity \(^\)0.4.*](#). The caret (^) before the version number implies an unlocked pragma, meaning that the compiler will use the specified version *and above*, hence the term "unlocked."

Recommendation: For consistency and to prevent unexpected behavior in the future, it is recommended to remove the caret to lock the file onto a specific Solidity version.

QSP-10 Fee can be lost (partially or in full) due to integer division.

Severity: *Informational*

Status: Unresolved

File(s) affected: [CompoundKeeper.sol](#)

Description: The loss of precision due to the integer division in [L18](#), [FlashLoanReceiver.sol](#) results in partial loss of fee. While the amount should be relatively small, it is unclear whether the behaviour is known to the developers as there is no relevant documentation or in-line comment regarding this issue. Note that for small amount, it is possible for the lender to borrow small amount without paying any fee.

Exploit Scenario: * Operator sets [flashLoanFeeInBips](#) to [10](#)

- Flash loaner calls borrow passing 100 as [_amount](#)
- [flashLend](#) executes, calling [addFee](#), which returns 100
- The flash lender then approves the CompoundKeeper contract to take 100 in payment
- At this point, the flash loaner will not pay any fee

Recommendation: Please verify whether this is acceptable or not and document this behaviour.

QSP-11 Clone-and-Own

Severity: *Informational*

Status: Unresolved

File(s) affected: [Compound.sol](#)

Description: The clone-and-own approach involves copying and adjusting open source code at one's own discretion. From the development perspective, it is initially beneficial as it reduces the amount of effort. However, from the security perspective, it involves some risks as the code may not follow the best practices, may contain a security vulnerability, or may include intentionally or unintentionally modified upstream libraries.

Recommendation: Rather than the clone-and-own approach, a good industry practice is to use the Truffle framework for managing library dependencies. This eliminates the clone-and-own risks yet allows for following best practices, such as, using libraries. Use the compound as a dependency in [package.json](#). Make sure to lock the dependency version.

QSP-12 Potential incorrect accounting when misusing [register\(\)](#)

Severity: *Undetermined*

Status: Unresolved

Description: As the [register\(\)](#) does not restrict and check the input values, an operator can call the [register\(\)](#) function with arguments that could mess up the accounting and state of the smart contract system. There is no documentation specifying the assumptions regarding these inputs and, thus, it is unclear to us whether these behaviour should be allowed or not.

Exploit Scenario: Here we list out some scenarios that would be potentially problematic.

- The Operator registers two [_underlying](#) with the same [kToken](#).
- Register two different [kTokens](#) with the same underlying [cToken](#). When [deregister\(\)](#) is performed on one of the [kToken](#), then the other one would stop to be functional as the underlying [cToken](#) has exited the market.
- In [register](#), [_underlying](#) may not be equal to [CErc20\(_ctoken\).underlying\(\)](#), allowing incorrect combinations of a ctoken and underlying token to be registered.

Recommendation: On the documentation side, it is important to specify whether this should be allowed and what underlying assumptions are there between different contracts. On the smart contract side, when there are assumptions for the input, perform input validation, and enforce the assumptions using require statements if possible. For example, to enforce that the [_underlying](#) matches the [CErc20\(_ctoken\).underlying\(\)](#): in [register](#), in the [_underlying](#) is different from [weth](#) branch (else branch on L106), add a [require](#) statement prior to [cTokens\[_underlying\] = CErc20\(cToken_\)](#) checking if [_underlying == CErc20\(cToken_\).underlying\(\)](#).

Automated Analyses

Mythril

- Exception state issues were reported in various lines, however, the lines that are marked are definitions of variables and thus are deemed false positives.
- Delegatecall proxy issues were identified in various lines in the proxy contracts, we classified them as benign issues.

Securify

Securify did not report any issues.

Slither

- sends eth to arbitrary user in [CanReclaimTokens.recoverTokens](#), the [msg.sender](#) has been limited to the [owner](#). In [_giveEth](#) of [CompoundKeeper.sol](#), the eth is sent to the compound protocol. We've classified both issues as false positive.

- controlled-delegatecall on all the proxy pattern contracts, which we deemed as benign

Code Documentation

- Many functions lack complete user and/or developer documentation. Fully document functions, at the very least those marked as external or public. Specifically provide a @notice, @dev, @param (for each parameter), and @return (if any). Additionally, for each contract, provide @title.
- Variable naming seems to be inconsistent. For instance, sometimes storage variables are suffixed with _, while in other contracts they are not. Same for parameters - sometimes prefixed with _, while in other occasions no prefix is used.

Adherence to Best Practices

- It is recommended to lock all dependencies in package.json to have a stable environment for testing and execution.
- CompoundKeeper.sol, All error messages in _takeEth refer to ERC20 tokens, instead of ETH. Recommendation: fix error messages replacing ERC20 with ETH.
- CompoundKeeper.sol, L50: the function is declared to return uint256, however, it does not return anything. Fix the declaration or the implementation. In addition, make it consistent with the interface IKeeper.
- CompoundKeeper.sol, requireNoError: The function assumes that errCode is within 0~99. However, errCode is declared to be uint, which is uint256, thus the output of the function could be erroneous.
- In general, should explicitly declare uint256 instead of uint

Test Results

Test Suite Results

The test suite does not contain unit tests and only has a set of functional tests that do not check the internal state of the contracts. Additionally, these tests can only be run on Kovan testnet. Quantstamp team tried running the tests numerous times but kept hitting errors from Infura. We cannot produce a result where all tests passed successfully.

All in all, we suggest developing mocks, unit tests, and functional tests that check the internal state of the contracts. More importantly, we recommend setting up a local environment to simulate protocol operations in Ganache and enable measurement of the code coverage via solidity-coverage.

```
(base) sungshil@MPC-UW:~/Projects/QuantStamp/Audit/keeper-sol$ yarn test
yarn run v1.21.1
$ yarn run generate && truffle test --network kovan
$ truffle compile && typechain --target truffle './build/**/*.json'
```

```
Compiling your contracts...
=====
> Everything is up to date, there is nothing to compile.
```

```
ts-gen: Running TypeChain
ts-gen: ./build/**/*.json matched 118 files.
ts-gen: Processing build/development/Address.json
ts-gen: Processing build/development/BaseAdminUpgradeabilityProxy.json
ts-gen: Processing build/development/BaseUpgradeabilityProxy.json
ts-gen: Processing build/development/CanReclaimTokens.json
ts-gen: Processing build/development/CErc20.json
ts-gen: Processing build/development/CEther.json
ts-gen: Processing build/development/Claimable.json
ts-gen: Processing build/development/CompoundKeeperV1.json
ts-gen: Processing build/development/Comptroller.json
ts-gen: Processing build/development/Context.json
ts-gen: Processing build/development/CoreKeeperV1.json
ts-gen: Processing build/development/CToken.json
ts-gen: Processing build/development/ERC20.json
ts-gen: Processing build/development/ERC20Burnable.json
ts-gen: Processing build/development/ERC20Detailed.json
ts-gen: Processing build/development/ERC20Mintable.json
ts-gen: Processing build/development/ERC20Pausable.json
ts-gen: Processing build/development/FlashLoanReceiver.json
ts-gen: Processing build/development/Gastoken.json
ts-gen: Processing build/development/IERC20.json
ts-gen: Processing build/development/IKeeper.json
ts-gen: Processing build/development/Initializable.json
ts-gen: Processing build/development/InitializableAdminUpgradeabilityProxy.json
ts-gen: Processing build/development/InitializableUpgradeabilityProxy.json
ts-gen: Processing build/development/KeeperBAT.json
ts-gen: Processing build/development/KeeperCBAT.json
ts-gen: Processing build/development/KeeperCDAI.json
ts-gen: Processing build/development/KeeperCETH.json
ts-gen: Processing build/development/KeeperCREP.json
ts-gen: Processing build/development/KeeperCSAI.json
ts-gen: Processing build/development/KeeperCUSDC.json
ts-gen: Processing build/development/KeeperCWBTC.json
ts-gen: Processing build/development/KeeperCZRX.json
ts-gen: Processing build/development/KeeperDAI.json
ts-gen: Processing build/development/KeeperETH.json
ts-gen: Processing build/development/KeeperREP.json
ts-gen: Processing build/development/KeeperRoles.json
ts-gen: Processing build/development/KeeperSAI.json
```


ts-gen: Processing build/development/KeeperUSDC.json
ts-gen: Processing build/development/KeeperWBTC.json
ts-gen: Processing build/development/KeeperZRX.json
ts-gen: Processing build/development/KToken.json
ts-gen: Processing build/development/Migrations.json
ts-gen: Processing build/development/MinterRole.json
ts-gen: Processing build/development/MockHonestLoanReceiver.json
ts-gen: Processing build/development/MockMaliciousLoanReceiver.json
ts-gen: Processing build/development/MockTokenA.json
ts-gen: Processing build/development/MockTokenB.json
ts-gen: Processing build/development/OpenZeppelinUpgradesAddress.json
ts-gen: Processing build/development/Ownable.json
ts-gen: Processing build/development/Pausable.json
ts-gen: Processing build/development/PauserRole.json
ts-gen: Processing build/development/Proxy.json
ts-gen: Processing build/development/ReentrancyGuard.json
ts-gen: Processing build/development/Roles.json
ts-gen: Processing build/development/SafeERC20.json
ts-gen: Processing build/development/SafeMath.json
ts-gen: Processing build/development/UpgradeabilityProxy.json
ts-gen: Processing build/development/Weth.json
ts-gen: Processing build/kovan/Address.json
ts-gen: Processing build/kovan/BaseAdminUpgradeabilityProxy.json
ts-gen: Processing build/kovan/BaseUpgradeabilityProxy.json
ts-gen: Processing build/kovan/CanReclaimTokens.json
ts-gen: Processing build/kovan/CErc20.json
ts-gen: Processing build/kovan/CEther.json
ts-gen: Processing build/kovan/Claimable.json
ts-gen: Processing build/kovan/CompoundKeeperV1.json
ts-gen: Processing build/kovan/Comptroller.json
ts-gen: Processing build/kovan/Context.json
ts-gen: Processing build/kovan/CoreKeeperV1.json
ts-gen: Processing build/kovan/CToken.json
ts-gen: Processing build/kovan/ERC20.json
ts-gen: Processing build/kovan/ERC20Burnable.json
ts-gen: Processing build/kovan/ERC20Detailed.json
ts-gen: Processing build/kovan/ERC20Mintable.json
ts-gen: Processing build/kovan/ERC20Pausable.json
ts-gen: Processing build/kovan/FlashLoanReceiver.json
ts-gen: Processing build/kovan/Gastoken.json
ts-gen: Processing build/kovan/IERC20.json
ts-gen: Processing build/kovan/IKeeper.json
ts-gen: Processing build/kovan/Initializable.json
ts-gen: Processing build/kovan/InitializableAdminUpgradeabilityProxy.json
ts-gen: Processing build/kovan/InitializableUpgradeabilityProxy.json
ts-gen: Processing build/kovan/KeeperBAT.json
ts-gen: Processing build/kovan/KeeperCBAT.json
ts-gen: Processing build/kovan/KeeperCDAI.json
ts-gen: Processing build/kovan/KeeperCETH.json
ts-gen: Processing build/kovan/KeeperCREP.json
ts-gen: Processing build/kovan/KeeperCSAI.json
ts-gen: Processing build/kovan/KeeperCUSDC.json
ts-gen: Processing build/kovan/KeeperCWBTC.json
ts-gen: Processing build/kovan/KeeperCZRX.json
ts-gen: Processing build/kovan/KeeperDAI.json
ts-gen: Processing build/kovan/KeeperETH.json
ts-gen: Processing build/kovan/KeeperREP.json
ts-gen: Processing build/kovan/KeeperRoles.json
ts-gen: Processing build/kovan/KeeperSAI.json
ts-gen: Processing build/kovan/KeeperUSDC.json
ts-gen: Processing build/kovan/KeeperWBTC.json
ts-gen: Processing build/kovan/KeeperZRX.json
ts-gen: Processing build/kovan/KToken.json
ts-gen: Processing build/kovan/Migrations.json
ts-gen: Processing build/kovan/MinterRole.json
ts-gen: Processing build/kovan/MockHonestLoanReceiver.json
ts-gen: Processing build/kovan/MockMaliciousLoanReceiver.json
ts-gen: Processing build/kovan/MockTokenA.json
ts-gen: Processing build/kovan/MockTokenB.json
ts-gen: Processing build/kovan/OpenZeppelinUpgradesAddress.json
ts-gen: Processing build/kovan/Ownable.json
ts-gen: Processing build/kovan/Pausable.json
ts-gen: Processing build/kovan/PauserRole.json
ts-gen: Processing build/kovan/Proxy.json
ts-gen: Processing build/kovan/ReentrancyGuard.json
ts-gen: Processing build/kovan/Roles.json
ts-gen: Processing build/kovan/SafeERC20.json
ts-gen: Processing build/kovan/SafeMath.json
ts-gen: Processing build/kovan/UpgradeabilityProxy.json
ts-gen: Processing build/kovan/Weth.json
ts-gen: Writing file: types/truffle-contracts/index.d.ts
ts-gen: Writing file: types/truffle-contracts/merge.d.ts
ts-gen: ✓ All done! Generated files: 2
Using network 'kovan'.

Compiling your contracts...
=====
> Everything is up to date, there is nothing to compile.

Compound Keeper 0x7bA12601a8eE5ac626915137B5693Ee7eeDC550B
Core Keeper 0x996C6Fee67Ec48B668a83a02BfD21c0CB1359D29
Error: Invalid JSON RPC response: ""
at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-cookies/dist/xml-http-request-event-target.js:27:61)
at t. setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-

[illegible]

[illegible]

[illegible]


```
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
```



```

    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
    at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
    at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
    at ClientRequest.emit (events.js:193:13)
    at TLSSocket.socketErrorListener (_http_client.js:397:9)
    at TLSSocket.emit (events.js:193:13)
    at emitErrorNT (internal/streams/destroy.js:91:8)
    at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""

```



```
Contract: CompoundKeeper
Error: Invalid JSON RPC response: ""
```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


```
engine/subproviders/provider.js:18:1)
  at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
  at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
  at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
  at t._onHttpResponseBodyEnd (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:318:1)
  at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
  at IncomingMessage.emit (events.js:198:15)
  at endReadableNT (_stream_readable.js:1139:12)
  at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: project ID request rate exceeded
  at callback (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3-provider-
engine/subproviders/provider.js:18:1)
  at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
  at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
  at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
  at t._onHttpResponseBodyEnd (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:318:1)
  at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
  at IncomingMessage.emit (events.js:198:15)
  at endReadableNT (_stream_readable.js:1139:12)
  at processTicksAndRejections (internal/process/task_queues.js:81:17)
  ✓ Can revert on an invalid flash loan (7985ms)
  ✓ Can withdraw from CompoundKeeper (7145ms)
```

```
Contract: CoreKeeper
Error: Invalid JSON RPC response: ""
  at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
  at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
  at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
  at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
  at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
  at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
  at ClientRequest.emit (events.js:193:13)
  at TLSSocket.socketErrorListener (_http_client.js:397:9)
  at TLSSocket.emit (events.js:193:13)
  at emitErrorNT (internal/streams/destroy.js:91:8)
  at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
  at processTicksAndRejections (internal/process/task_queues.js:81:17)
Compound Keeper 0x154D29EadD8c16cc9f0a48c8882c6bbD5935fDC0
Error: Invalid JSON RPC response: ""
  at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
  at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
  at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
  at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
  at t._onHttpRequestError (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:349:1)
  at ClientRequest.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:252:47)
  at ClientRequest.emit (events.js:193:13)
  at TLSSocket.socketErrorListener (_http_client.js:397:9)
  at TLSSocket.emit (events.js:193:13)
  at emitErrorNT (internal/streams/destroy.js:91:8)
  at emitErrorAndCloseNT (internal/streams/destroy.js:59:3)
  at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: Invalid JSON RPC response: ""
  at Object.InvalidResponse (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-core-helpers/src/errors.js:42:1)
  at t._a[as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:92:1)
```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


```
cookies/dist/xml-http-request.js:318:1)
  at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
    at IncomingMessage.emit (events.js:198:15)
    at endReadableNT (_stream_readable.js:1139:12)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: project ID request rate exceeded
  at callback (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3-provider-
engine/subproviders/provider.js:18:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpResponseEnd (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:318:1)
    at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
    at IncomingMessage.emit (events.js:198:15)
    at endReadableNT (_stream_readable.js:1139:12)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: project ID request rate exceeded
  at callback (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3-provider-
engine/subproviders/provider.js:18:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpResponseEnd (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:318:1)
    at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
    at IncomingMessage.emit (events.js:198:15)
    at endReadableNT (_stream_readable.js:1139:12)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
Error: project ID request rate exceeded
  at callback (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/web3-provider-
engine/subproviders/provider.js:18:1)
    at t._a [as onreadystatechange] (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
    at t.dispatchEvent (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request-event-target.js:27:61)
    at t._setReadyState (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:208:1)
    at t._onHttpResponseEnd (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-hdwallet-
provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:318:1)
    at IncomingMessage.<anonymous> (/Users/sungshil/Projects/QuantStamp/Audit/keeper-sol/node_modules/truffle-
hdwallet-provider/dist/webpack:/truffle-hdwallet-provider/Users/gnidan/src/work/truffle/node_modules/xhr2-
cookies/dist/xml-http-request.js:289:47)
    at IncomingMessage.emit (events.js:198:15)
    at endReadableNT (_stream_readable.js:1139:12)
    at processTicksAndRejections (internal/process/task_queues.js:81:17)
```

6 passing (2m)
1 failing

```
1) Contract: CoreKeeper
  "before all" hook: prepare suite:
    Error: project ID request rate exceeded
      at callback (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3-provider-engine/subproviders/provider.js:18:1)
        at t._a [as onreadystatechange] (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/web3/node_modules/web3-providers-http/src/index.js:96:1)
        at t.dispatchEvent (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/xhr2-cookies/dist/xml-http-request-event-target.js:27:61)
        at t._setReadyState (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/xhr2-cookies/dist/xml-http-request.js:208:1)
        at t._onHttpResponseEnd (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/xhr2-cookies/dist/xml-http-request.js:318:1)
        at IncomingMessage.<anonymous> (node_modules/truffle-hdwallet-provider/dist/webpack:/truffle-hdwallet-
provider/Users/gnidan/src/work/truffle/node_modules/xhr2-cookies/dist/xml-http-request.js:289:47)
        at endReadableNT (_stream_readable.js:1139:12)
        at processTicksAndRejections (internal/process/task_queues.js:81:17)
```


Code Coverage

There is no local testing environment set up, thus it is not possible to measure code coverage. However, from inspecting the code, it is clear that the code coverage is very low. Additionally, since the tests don't assert the internal state of the smart contract, the lines of code that are reported to be covered are also not really tested.

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

28e71c3629159664885c8c3eb7c6cfa0cf33f231793c8a219e2aca5ac8e21b7e	./contracts/Migrations.sol
5ac19927d4e9255f7998dc68502a5d95bbabc499460b416605637a4f02f20b1c	./contracts/compound/CompoundKeeper.sol
7095aacca8099fece7248268a4169976e9a180baad77533e94f8642111dbd3a8	./contracts/compound/KTokens.sol
9da890e8b42d53efe255650b84d87501be4d5b5a089df07115e1cec6a1c77059	./contracts/compound/Compound.sol
37357ddac754eee0fd61219fbe81bd6ddac2f7b1fbdde10e4534416c91e29e9f	./contracts/common/Claimable.sol
82037df701679791b89f59241a62abee64a910ba594c33acb119a5bfa581caf4	./contracts/common/CanReclaimTokens.sol
cd0dc6d01269118bc7dc30d7c94ea5a3b1c3022fc9b247efa9d653c80a57b561	./contracts/common/Gastoken.sol
236964834a41830a8ed816ff14abc890ec2770133061d528fb94bc6483f5be39	./contracts/protocol/KeeperRoles.sol
84f279dddab4dc37e1ae734d0babe16644a68660dc1411b119db061d8097dbf6	./contracts/protocol/KeeperDAOProxyAdmin.sol
50d2e6d5c6a05a669cd73e5ba1210256b78f0e5b711c9cfce66f0bc039137f42	./contracts/protocol/FlashLoanReceiver.sol
83b2bd4832751387809ed10c9ce68bf3f9e1619dc6c888ad345e2c076c3dec50	./contracts/protocol/KToken.sol
399ced04989e761d13786da3c0fa53780368980b422fbd3310a791be853b107f	./contracts/protocol/IKeeper.sol
a428cb5446b72d9be4c3cb4c0ae2379c32e74c9daa504fe06e9099ad81e95d59	./contracts/mock/MockTokenB.sol
57077ac60db5ce84bd4e588c59482c724249b2724f2358a9014cc24c09de2b6e	./contracts/mock/MockTokenA.sol
6850a556c5a056fecf4d6e0a9185a80d159ac43b864fca9b6132154ed258b9ae	./contracts/mock/MockHonestLoanReceiver.sol
e0b84761e8ed28f07b860272c05285edc329b3388f4c25f15dfe8630c3509c06	./contracts/mock/MockMaliciousLoanReceiver.sol
0cb47ff1acee7575b68e2f7440524e241e133a78fd77239c7bf5b683440a532a	./contracts/core/CoreKeeper.sol
5f880faf90ddf0c6bd499ffc14c497c086234651bff5bc74e62f16a9f3e96370	./contracts/core/KTokens.sol

About Quantstamp

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

Quantstamp’s team boasts decades of combined experience in formal verification, static analysis, and software verification. Collectively, our individuals have over 500 Google scholar citations and numerous published papers. In its mission to proliferate development and adoption of blockchain applications, Quantstamp is also developing a new protocol for smart contract verification to help smart contract developers and projects worldwide to perform cost-effective smart contract security audits.

To date, Quantstamp has helped to secure hundreds of millions of dollars of transaction value in smart contracts and has assisted dozens of blockchain projects globally with its white glove security auditing 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.

Finally, Quantstamp’s dedication to research and development in the form of collaborations with leading academic institutions such as National University of Singapore and MIT (Massachusetts Institute of Technology) reflects Quantstamp’s commitment to enable world-class smart contract innovation.

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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The Solidity language itself and other smart contract languages remain under development and are subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond Solidity or the smart contract programming language, or other programming aspects that could present security risks. You may risk loss of tokens, Ether, and/or other loss. A report is not an endorsement (or other opinion) of any particular project or team, and the report does not guarantee the security of any particular project. A report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. To the fullest extent permitted by law, we disclaim all warranties, express 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 website, or any website or mobile application featured in any banner or other 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. You may risk loss of QSP tokens or other loss. 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.