Quantstamp Security Assessment Certificate

December 4th 2020 — Quantstamp Verified

Compound Vesting and Grants

This security assessment was prepared by Quantstamp, the leader in blockchain security

Executive Summary

Type	Decentralized lending protocol
Auditors	Fayçal Lalidji, Security Auditor Kacper Bąk, Senior Research Engineer Jake Goh Si Yuan, Senior Security Researcher
Timeline	2020-11-09 through 2020-11-16
EVM	Muir Glacier
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	None
Documentation Quality	High
Test Quality	High

Source Code

Repository	Commit
compound-protocol	ccc7d51
compound-protocol	f9544aa

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

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
Undetermined	The impact of the issue is uncertain.
Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

Through reviewing the code, we found **3 potential issues** of various levels of severity. As of commit f9544aa all low/medium severity issues have been addressed as recommended. Code coverage could not be generated due to multiple failing tests that must be updated before merging the audited pull request.

ID	Description	Severity	Status
QSP-1	`compSpeeds` Update	Medium	Fixed
QSP-2	`_grantComp` Insufficient Balance	Low	Fixed
QSP-3	Unlocked Pragma	Informational	Acknowledged

Quantstamp Audit Breakdown

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

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

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

Methodology

The Quantstamp auditing process follows a routine series of steps:

1. Code review that includes the following
   i. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
   ii. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Toolset

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

Setup

Tool Setup:

- Slither v0.6.14

Steps taken to run the tools:

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

Findings

QSP-1 `compSpeeds` Update

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `Comptroller.sol`

Description: The implemented internal method `Comptroller.setCompSpeedInternal` does not update the related `cToken` market staking indexes. Changing the value of "Comp token distribution speed" for a specific market without updating its supply and borrow indexes will lead the users to either gain more or less Comp reward.

Recommendation: `Comptroller.updateLastVestingBlockInternal`, `Comptroller.updateCompSupplyIndex` and `Comptroller.updateCompBorrowIndex` should be called before updating `compSpeeds` value for any given market.

QSP-2 `_grantComp` Insufficient Balance

Severity: *Low Risk*

Status: Fixed

File(s) affected: `Comptroller.sol`

Description: The `Comptroller._grantComp` method only succeeds when the amount requested is less than or equal to the remaining `Comptroller` Comp balance, as implemented in `Comptroller.grantCompInternal`. However, when the amount is more than that, the method fails silently without emitting an event or throwing. As consequence, this issue could lead a governance proposal to pass without throwing.

Recommendation: Check the returned value of `Comptroller.grantCompInternal` and throw the transaction if it is different than zero.

QSP-3 Unlocked Pragma

Severity: *Informational*

Status: Acknowledged

File(s) affected: `Comptroller.sol`, `ComptrollerStorage.sol`, `Exponential.sol`, `ComptrollerStorage.sol`

Description: Every Solidity file specifies in the header a version number of the format `pragma solidity (^)0.*.*`. 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.

Automated Analyses

Slither

Slither raised multiple high and medium issues. However, all issues were classified as false positives.

Code Documentation

Outdated NatSpec:

- Documentation in `Comptroller.sol.updateCompMarketIndex` is missing `@param` description for `marketBorrowIndex`.
- Documentation in `Comptroller.sol.distributeBorrowerComp` is missing `@param` description for `marketBorrowIndex`.
- Documentation in `Comptroller.sol.distributeMarketComp` is missing `@param` description for `marketBorrowIndex`, `distribute`, `marketState`, `vestingState`, `isSupply` and `marketBorrowIndex`.

Test Results

Test Suite Results

```
Using network test Web3ProviderEngine
Setup in 358 ms
 PASS  tests/Governance/CompTest.js (16.974s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 108 ms
 PASS  tests/TimelockTest.js (28.058s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 143 ms
 PASS  tests/SpinaramaTest.js (47.41s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 154 ms
 PASS  tests/Lens/CompoundLensTest.js (95.767s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 160 ms
 PASS  tests/Governance/GovernorAlpha/CastVoteTest.js (8.809s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 119 ms
 PASS  tests/Tokens/borrowAndRepayCEtherTest.js (116.52s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 192 ms
 PASS  tests/Comptroller/comptrollerTest.js (103.418s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 191 ms
 PASS  tests/Governance/GovernorAlpha/ProposeTest.js (6.978s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 79 ms
 PASS  tests/Tokens/reservesTest.js (114.255s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 194 ms
 PASS  tests/Models/InterestRateModelTest.js (23.417s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 168 ms
 PASS  tests/Tokens/cTokenTest.js (159.463s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 166 ms
 PASS  tests/Comptroller/proxiedComptrollerV1Test.js (117.732s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 165 ms
 PASS  tests/Governance/GovernorAlpha/StateTest.js (11.599s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 180 ms
 PASS  tests/Tokens/mintAndRedeemTest.js (177.983s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 119 ms
```

```
 PASS  tests/Tokens/liquidateTest.js (184.155s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 114 ms
 PASS  tests/Models/DAIInterestRateModelTest.js (186.017s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 124 ms
 PASS  tests/Comptroller/accountLiquidityTest.js (50.382s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 125 ms
 PASS  tests/Comptroller/unitrollerTest.js (34.876s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 138 ms
 PASS  tests/Tokens/accrueInterestTest.js (43.803s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 124 ms
 PASS  tests/Comptroller/adminTest.js (8.596s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 111 ms
 PASS  tests/Comptroller/pauseGuardianTest.js (101.166s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 131 ms
 PASS  tests/Tokens/mintAndRedeemCEtherTest.js (28.829s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 208 ms
 PASS  tests/Governance/GovernorAlpha/QueueTest.js (9.75s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 110 ms
 PASS  tests/Tokens/borrowAndRepayTest.js (214.15s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 156 ms
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 105 ms
 PASS  tests/CompilerTest.js
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 112 ms
 PASS  tests/Tokens/safeTokenTest.js (14.799s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 162 ms
 PASS  tests/MaximillionTest.js (24.482s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 140 ms
 PASS  tests/Tokens/transferTest.js (26.476s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 112 ms
 PASS  tests/Tokens/compLikeTest.js (13.785s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 107 ms
 PASS  tests/Governance/CompScenarioTest.js (19.369s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 94 ms
 PASS  tests/Tokens/setInterestRateModelTest.js (62.269s)
 PASS  tests/Tokens/setComptrollerTest.js (39.479s)
Teardown in 0 ms
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 149 ms
Using network test Web3ProviderEngine
Setup in 136 ms
 PASS  tests/Tokens/adminTest.js (63.561s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 146 ms
 PASS  tests/Comptroller/liquidateCalculateAmountSeizeTest.js (99.788s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 129 ms
 PASS  tests/Scenarios/Governor/UpgradeScenTest.js (94.775s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 181 ms
 PASS  tests/Scenarios/Flywheel/ReservoirScenTest.js (118.712s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 194 ms
 PASS  tests/Scenarios/Governor/GuardianScenTest.js (114.334s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 102 ms
 PASS  tests/Scenarios/HypotheticalAccountLiquidityScenTest.js (136.866s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 181 ms
 PASS  tests/Scenarios/Governor/ExecuteScenTest.js (182.223s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 119 ms
 PASS  tests/PriceOracleProxyTest.js (278.848s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 154 ms
 PASS  tests/Scenarios/Governor/DefeatScenTest.js (122.465s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 170 ms
 PASS  tests/Comptroller/assetsListTest.js (382.911s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 158 ms
 PASS  tests/Scenarios/Governor/ProposeScenTest.js (224.643s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 146 ms
Using network test Web3ProviderEngine
Setup in 331 ms
Using network test Web3ProviderEngine
Setup in 417 ms
 PASS  tests/Scenarios/Governor/VoteScenTest.js (154.162s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 93 ms
 PASS  tests/Scenarios/Governor/QueueScenTest.js (232.085s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 185 ms
 PASS  tests/Scenarios/Flywheel/VestingScenTest.js (352.918s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 160 ms
 PASS  tests/Scenarios/ChangeDelegateScenTest.js (46.414s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 172 ms
 PASS  tests/Scenarios/RedeemUnderlyingEthScenTest.js (394.625s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 122 ms
Using network test Web3ProviderEngine
Setup in 411 ms
 PASS  tests/Scenarios/Governor/CancelScenTest.js (209.327s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 124 ms
Using network test Web3ProviderEngine
Setup in 332 ms
 PASS  tests/Scenarios/RedeemUnderlyingWBTCScenTest.js (571.648s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 106 ms
Using network test Web3ProviderEngine
Setup in 453 ms
 PASS  tests/Scenarios/PriceOracleProxyScenTest.js (248.003s)
Teardown in 0 ms
Using network test Web3ProviderEngine
```

```
Setup in 134 ms
 PASS  tests/Scenarios/BreakLiquidateScenTest.js (138.741s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 146 ms
Using network test Web3ProviderEngine
Setup in 384 ms
Using network test Web3ProviderEngine
Setup in 361 ms
 PASS  tests/Scenarios/Flywheel/FlywheelScenTest.js (734.852s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 169 ms
 PASS  tests/Scenarios/SetComptrollerScenTest.js (116.034s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 186 ms
Using network test Web3ProviderEngine
Setup in 346 ms
 PASS  tests/Flywheel/FlywheelTest.js (1121.059s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 125 ms
 PASS  tests/Scenarios/ReduceReservesScenTest.js (367.075s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 133 ms
 PASS  tests/Scenarios/ExchangeRateScenTest.js (189.752s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 166 ms
Using network test Web3ProviderEngine
Setup in 366 ms
 PASS  tests/Scenarios/RedeemUnderlyingScenTest.js (552.228s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 204 ms
 PASS  tests/Scenarios/InKindLiquidationScenTest.js (771.705s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 234 ms
 PASS  tests/Scenarios/BorrowBalanceScenTest.js (299.112s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 148 ms
Using network test Web3ProviderEngine
Setup in 366 ms
 PASS  tests/Scenarios/RepayBorrowWBTCScenTest.js (623.278s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 206 ms
 PASS  tests/Scenarios/CTokenAdminScenTest.js (183.028s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 171 ms
Using network test Web3ProviderEngine
Setup in 337 ms
Using network test Web3ProviderEngine
Setup in 373 ms
 PASS  tests/Scenarios/TokenTransferScenTest.js (337.505s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 110 ms
Using network test Web3ProviderEngine
Setup in 568 ms
 PASS  tests/Scenarios/UnitrollerScenTest.js (188.948s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 121 ms
 PASS  tests/Scenarios/EnterExitMarketsScenTest.js (525.679s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 194 ms
Using network test Web3ProviderEngine
Setup in 352 ms
 PASS  tests/Scenarios/BorrowWBTCScenTest.js (236.179s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 164 ms
Using network test Web3ProviderEngine
Setup in 384 ms
 PASS  tests/Scenarios/ReEntryScenTest.js (52.361s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 135 ms
 PASS  tests/Scenarios/BorrowEthScenTest.js (187.645s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 141 ms
 PASS  tests/Scenarios/TetherScenTest.js (10.724s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 106 ms
 PASS  tests/Scenarios/Comp/CompScenTest.js (400.99s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 133 ms
 PASS  tests/Scenarios/RepayBorrowEthScenTest.js (771.232s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 153 ms
Using network test Web3ProviderEngine
Setup in 516 ms
 PASS  tests/Scenarios/RedeemEthScenTest.js (255.623s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 206 ms
 PASS  tests/Scenarios/MCDaiScenTest.js (10.083s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 112 ms
Using network test Web3ProviderEngine
Setup in 456 ms
 PASS  tests/Scenarios/AddReservesScenTest.js (389.071s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 131 ms
Using network test Web3ProviderEngine
Setup in 351 ms
 PASS  tests/Scenarios/MintWBTCScenTest.js (342.844s)
Teardown in 1 ms
 PASS  tests/Scenarios/MintEthScenTest.js (268.666s)
Teardown in 0 ms
 PASS  tests/Scenarios/TimelockScenTest.js (432.375s)
Teardown in 0 ms
 PASS  tests/Scenarios/BorrowCapScenTest.js (545.063s)
Teardown in 0 ms
 PASS  tests/Scenarios/SeizeScenTest.js (198.548s)
Teardown in 1 ms
 PASS  tests/Scenarios/BorrowScenTest.js (351.085s)
Teardown in 0 ms
 PASS  tests/Scenarios/FeeScenTest.js (252.994s)
Teardown in 0 ms
 PASS  tests/Scenarios/RepayBorrowScenTest.js (510.733s)
Teardown in 0 ms
 PASS  tests/Scenarios/MintScenTest.js (273.181s)
Teardown in 0 ms
 PASS  tests/Scenarios/RedeemWBTCScenTest.js (527.17s)
Teardown in 0 ms
 PASS  tests/Scenarios/RedeemScenTest.js (481.397s)

Test Suites: 2 skipped, 85 passed, 85 of 87 total
Tests:       38 skipped, 15 todo, 993 passed, 1046 total
Snapshots:   0 total
Time:        2113.138s
Ran all test suites matching /test/i.
Teardown in 0 ms
Done in 2147.65s.
```

Code Coverage

Multiple code coverage tests failed to execute. Therefore, we couldn't generate the coverage statistics.

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

```
b298fa21af3425f93c8de0220417ad1827f4efe503568c2e6344792c3595c665 ./Exponential.sol
9efca9ff7861f0351ea8fbb393008792a9eb2cca55d51ee0f7a19b4e6b9e4317 ./ComptrollerStorage.sol
163a0ff8024223bbfb374d604440946e58b4aa3bf9d3b7cac0729560c9304f6d ./Comptroller.sol
70a99e54d6463f9626b2d492d26009a59d3dacd4e1e4abb69a2c0877ee1fdd64 ./ComptrollerG5.sol
```

Tests

```
19dda8605a559d42ee39f9157edf3692c7e69a3cc865c322718f5d38e78a847c ./tests/PriceOracleProxyTest.js
e854495d3f31067771e20c34a2a8c71e4838c420ce4c2f3a982c9d93a1d27f64 ./tests/gasProfiler.js
5c384dd1c5e1a1e2fb890e0bdcfa788b19149b7597b36c57d50343e255d55d9e ./tests/TimelockTest.js
851d08dc2b791e186d8edd9122acd20b3966ee85d71905e6e69df35b6cdc9178 ./tests/Scenario.js
ef6b1a22aca7c79d9bbe28e11a488d90712d8f570acddd90faaaa760c4f34b16 ./tests/Errors.js
5358fa45a77b2597d46448b7aecc96de55894ba08c6602ced648bf7a0b7c1fd5 ./tests/Jest.js
cb9ee641b3aa7df9e7f188c17b71b0b97f387c166915408bf09b4d0ff932c62a ./tests/CompilerTest.js
3469ecc216e78aec26e05a002fa2dcbcd9608853bb70de1b6724e38425259b37 ./tests/MaximillionTest.js
b0fc7e7382f6bf19bb037855883f5a4fc1606630a61adb59c2dc1ea8bb2d8574 ./tests/Matchers.js
1ce576360cbea8a1b3c09de8d196773ab156645854ac8f1796d4bc67d6e7dca2 ./tests/SpinaramaTest.js
da16cc0d260427b1be2cabc2224c0efaa6bf2a2c93abb0571974c9a56b911ee9 ./tests/Lens/CompoundLensTest.js
2f4dbcc4fe47083cff4db7c60220550b063b258346e77075a26fea1435bbd3bc ./tests/Contracts/MockMCD.sol
b2ecb6ed9cb46b1813e86b45bfda3b15a715fa4c05ae9db7df38d83a777b8126 ./tests/Contracts/FalseMarker.sol
cf43a610e04d279dfffad601eeb48b4006d545410e20f08be012654142797f00 ./tests/Contracts/TetherInterface.sol
176d795f35868f6c3df6800a6ebfa3589e03a7fa577efc11d123bdb5ca58fab7 ./tests/Contracts/FeeToken.sol
d70e8368d1ee9af48f277d9efd58e6a764c5c9f1819a5ba5f29e1099c2941f8d ./tests/Contracts/CErc20Harness.sol
b6628647f7f2da44c6ebf4f22783185a90a37ce39d18fceb35f3794494f4cb44 ./tests/Contracts/PriceOracleProxy.sol
349649b88d6e9f805a384a8d045a269a582d5cce165b67c6b6faff159cbb91a1 ./tests/Contracts/ComptrollerScenarioG1.sol
0d7fd9df64cf72889d6ac97afd3258167116518748488e997505f27cc16b4fe6 ./tests/Contracts/MathHelpers.sol
87bc237c9d1beee713e20b0b8fce333a4b52029849f555761cec6d50fe6b86bf ./tests/Contracts/TimelockHarness.sol
167d04d4dda1e53afe3120b21f732de6bb2c1d977ac46e3d0a6fe205033048e3 ./tests/Contracts/Fauceteer.sol
7e10baf5e8ab1793e452a9d28a3052534b47972c1c31a33939e36aa84301ea7d ./tests/Contracts/EvilToken.sol
34eaaa9e85252b43034072160b7cc4452a08ca3b4a9c3bd28cda689be83bff0b ./tests/Contracts/ERC20.sol
dfe52a0a041631f00e3851a90307683cf50a93e6a97e9e9d8eef1ef0dd741264 ./tests/Contracts/FixedPriceOracle.sol
9e86b10a2659f302d1643e1cd2c492c698b33e97e166e0ce647da492da5b614d ./tests/Contracts/Counter.sol
fffc8aa485138515368781e1053719c0117a06058fef08ba5e0874c5aa1482f3 ./tests/Contracts/ComptrollerScenarioG4.sol
3cf7df3c6a30319867cb011ec3373f54232ffc3b42a74f791d098f164df0d2ce ./tests/Contracts/ComptrollerScenarioG2.sol
836d838a1db13333de3438063d25a47507f4680cfa104acb1b18daddc4886630 ./tests/Contracts/ComptrollerHarness.sol
3cc11b832ed5b3e5c18e01b21fb86fa0f37badd626364933b62640c3aff7a685 ./tests/Contracts/WBTC.sol
c782e7940244f7e106fb29543158703c2f544856602769f16da24a2da12320d6 ./tests/Contracts/ComptrollerScenarioG3.sol
5dabf4413d579426e299886b7124e6bf5c415a1fd8fc6d3322c8af0c3d49a532 ./tests/Contracts/CompHarness.sol
4e85b16aaa42a85cfeff0894ed7b00ead01cfdc5d42dde1a9251f638208e9234 ./tests/Contracts/GovernorAlphaHarness.sol
297d6be038dccf0d50dc4883c9c330c27380fdc02efc0155e684bf798bbec30c ./tests/Contracts/CEtherHarness.sol
5288acf7cb76e1b86658fa7b7812b118fb405700543fd43d31d0431029b7e688 ./tests/Contracts/FaucetToken.sol
a3c8ad4dbbb5bd58806b0e1285fe8c9319d9c8fb4dfaed3d862a35647b1cc159 ./tests/Contracts/InterestRateModelHarness.sol
bf84c0e16a80947ad63f6dfa9e973f9b47437c1758450d45570a14af4c2b085c ./tests/Contracts/Const.sol
10144c7d50d2679e2f4ea63df2ed58ec14f22e8e09d77d15473a55f8e3f58d5e ./tests/Contracts/Structs.sol
1478422bbeb039fb7b82f12b3724c30d98bc6c270fcfc8b29ce11f80dce4cfe4 ./tests/Contracts/ComptrollerScenario.sol
eeda18f052fb5cf750b817b8e613a90a2802db6eeda2745d288cfea0fd603ffd ./tests/Contracts/ComptrollerScenarioG5.sol
09d569c78402ac3747023f0b8b726e75afa4cf2fa0598f0baaf4966991882da2 ./tests/Utils/Compound.js
760666fd6801178144a7e2e5ee4fcdf761e63ab1d4dad5d3f483f3eea004ba94 ./tests/Utils/InfuraProxy.js
f8926c5c008667fd0cb74a229c7ae10ec9400da914a12c9a1fd4fffa68fa09e0 ./tests/Utils/Ethereum.js
17f1dae75f61ebf222ffab3ff97df7a0a42740dd7513e75dd8cb41cdb561c001 ./tests/Utils/JS.js
27fe3919f7c3bc28e1822aa1f0ccdf750285abf813d1dee490c35137047ffdaa ./tests/Utils/EIP712.js
c0ef9125ef417a1216d648e9ae546f412c980ac1ef1de7d2c164b5a2aaa40eb9 ./tests/Governance/CompTest.js
2a481672769902fc25ebc4d58c9d58917155f4e92ff56543280f8114884fb7b9 ./tests/Governance/CompScenarioTest.js
1afc663d267e18b7ce28acde1dffc6ef0e28b7c37bd001db36b295640d050779 ./tests/Governance/GovernorAlpha/StateTest.js
```

```
5f5972390f0f1666982ff55ff56799b52748e0e1132805a2f37a904396b27fe3 ./tests/Governance/GovernorAlpha/QueueTest.js
45f10e9446c8d68eead1fc509a220fa0dc854f0d4d24d2fef972bbebe74a64f2 ./tests/Governance/GovernorAlpha/ProposeTest.js
10bd124f58ad69ba89f228fa77306e2df3f9435717d0d112ff120e10bb9b38a7 ./tests/Governance/GovernorAlpha/CastVoteTest.js
8e8b23d890c2c95bbc6adec14363a19f9d82dd3fa989a8ce3641e90b5fcb4b62 ./tests/Scenarios/RepayBorrowScenTest.js
9ba1859b1e2341272c60a134855b585b9044d3b98d60e4cbbad571fe7423effc ./tests/Scenarios/CTokenAdminScenTest.js
506be5485394cb2c9bbc6f6bb6cc45b234a6c352172577706b27d1a7de4f4c9f ./tests/Scenarios/RedeemUnderlyingScenTest.js
ecfbedea3ca6e97266b4e76555ec6f7705628055998a3bc7f7051039292a067a ./tests/Scenarios/RedeemUnderlyingWBTCScenTest.js
7e6e76b14ed1fcf84ea6ac065be86fe0392cd2ac56851b5dc13ba9d7e6a37334 ./tests/Scenarios/BorrowScenTest.js
e3523f04ddfd19a14a44f74f32dd77305e06414af2e0ba1749b00c258b00ea87 ./tests/Scenarios/ExchangeRateScenTest.js
4c716c17c8d6d607621dd117900898731e9380df408ec22a1c141bcd7ec4965e ./tests/Scenarios/FeeScenTest.js
48966575141a703b0b5ffae7883627768eb63fbf15deedff9446fb3be607b0ee ./tests/Scenarios/RepayBorrowWBTCScenTest.js
16b28c43b7e03d0940111656945db3b1053c2753a623333ebfd85e81dfba4b1c ./tests/Scenarios/HypotheticalAccountLiquidityScenTest.js
2de2738aa61707ba2d2191babe2f55d1351fa140fdeb6af82074569df30d6f2e ./tests/Scenarios/SetComptrollerScenTest.js
b37e241c41fe97f45361a7d135afb2c699fccb565ecd2abf9d32ef57b50c0562 ./tests/Scenarios/BreakLiquidateScenTest.js
be689993bebc216c4cac9781ae286bf810aa34c793d8d743c53945c787d3ebd9 ./tests/Scenarios/EnterExitMarketsScenTest.js
e08db9fbdfd99a4b7704073b2cc64dcc7a18371ff0ec37723decdc7df5cefd90 ./tests/Scenarios/RedeemUnderlyingEthScenTest.js
a05ea0319b7966741c6a4944680ff5b7586132c5bca1b649685a9d1f0a97dcf9 ./tests/Scenarios/RepayBorrowEthScenTest.js
fbebcc9776712f53927fda86b2f86093e6b749f4602e31630dfb04462d30cd3c ./tests/Scenarios/BorrowEthScenTest.js
b3e59040b0087633e9f66dc4259d1d4fd5a04e4cfb76bb877713f8c830e9c690 ./tests/Scenarios/MintEthScenTest.js
9462f13e5d02224092386a00d92d261bb805079c1131fe2d1ca159d87a03d30a ./tests/Scenarios/BorrowBalanceScenTest.js
e37a817659914f87330a3347a534a4b42aa98ee8307f8f4e4ead02f3f4c0c639 ./tests/Scenarios/RedeemScenTest.js
3f8068cd66e6d3dd9e483cabc896690dacc3050446d97c85bcba37ad4524d9a5 ./tests/Scenarios/AddReservesScenTest.js
76bdb38fdec13324d65e2e22d5a51cc11971e92d29f26f3671143151e6788955 ./tests/Scenarios/TetherScenTest.js
c7889c9279fe003850a17fcb8a14f16357af221b522d8163decd38908e70ef68 ./tests/Scenarios/MintScenTest.js
13f66b96a6e1ef1f0150a609c9a841fd01ce62493f6dfda92a6af821a218b6d8 ./tests/Scenarios/MCDaiScenTest.js
4bab260de71fdf7f22d7419ee041e68ecfe68c245e0bfe17af9b5df9394f8dbc ./tests/Scenarios/UnitrollerScenTest.js
5e1c8ebd93d8065bd53b7ff1867dcb2a8dc430b6faa9d5dad949a0b7d7831aad ./tests/Scenarios/InKindLiquidationScenTest.js
93a699f3cb8cf2978e5ad148d25443f355a3f119bdf84d4f7a4fcbefa0629c4a ./tests/Scenarios/ReduceReservesScenTest.js
b27517399783a102932891ffd3e632421e809cac2245bbcc2b4f7b2c23cfbf89 ./tests/Scenarios/ChangeDelegateScenTest.js
2f903f59c90057cfe955b933ae3fb7b17f097e8ca28d2efb3e8e7cc56e1403eb ./tests/Scenarios/RedeemWBTCScenTest.js
01ca493f015cc003b578b60a7df83a8c7c576dbff3b0efbb91bf1ea67ad153ec ./tests/Scenarios/TimelockScenTest.js
c3261939c88aa2a210d91c18118f6f06d38212ca3e8cb0125c79538bc601989d ./tests/Scenarios/BorrowWBTCScenTest.js
18bd40435c9385aae3b5018bdb65da6265eff8b26d16d8e9a03ffa26049efff9 ./tests/Scenarios/ReEntryScenTest.js
d505cbc2d5d96010232526ce9f8c44f32e8c0f8cd732ef8a8da11b4c1c5a676e ./tests/Scenarios/MintWBTCScenTest.js
c294549c150c8f3fe0ce7f9708d4e12860c5725fe20948e712d8e8651f540e6b ./tests/Scenarios/RedeemEthScenTest.js
4a3529fcea2305838a08275b4ceeb4861fea396e9a5cb4acb651d96c0c3de729 ./tests/Scenarios/TokenTransferScenTest.js
2eb4bcabc0cbd1af93d91ff1157b2183cfb9bd881e8e977bccf1575b5443e799 ./tests/Scenarios/SeizeScenTest.js
cfce4030a370f632f1d9df7d2d44e4dc0af05ec641bd223ec906b24b0c09bb07 ./tests/Scenarios/PriceOracleProxyScenTest.js
ad7f7b28e17a9d715b0ef8d811c7bc7fca4aa9e23aa0d2f706abc1cbab70f8f4 ./tests/Scenarios/BorrowCapScenTest.js
a8d77f870a989264aaa2c6361d0cd46ea93497dc886d851d7c068a087674aee2 ./tests/Scenarios/Governor/VoteScenTest.js
dcff6540ca7ad2d404d6f0820f1f699c5e2a721883a2115a094067768d327068 ./tests/Scenarios/Governor/QueueScenTest.js
3ed48d345ed89b6f02c81990f3ba912ea71500d177d7920ef95d11363e868869 ./tests/Scenarios/Governor/DefeatScenTest.js
00b7d5ad7266361d1de01459f809b178c1f683a2714fed986fdbbdda9675d185 ./tests/Scenarios/Governor/CancelScenTest.js
aa4f9419cfa64c2781b88e3a8a86f15243e7d1ffd3d10ceba24f09a158856ffa ./tests/Scenarios/Governor/ProposeScenTest.js
d258fb116bb44586f517e6703f1be7e244d5f566eb76882c2cebdecfc9608b7c ./tests/Scenarios/Governor/ExecuteScenTest.js
98e20441a2e53f58fdcdf95d3bd60f708ad96597dec7e140d0fbceebd0d3e03c ./tests/Scenarios/Governor/GuardianScenTest.js
4eeafe9f7d5b95fe0737438464ec96a1ee1337408e44457f57307ea973f64a77 ./tests/Scenarios/Governor/UpgradeScenTest.js
05e757f24b262122dea8145a7eb786f100af9f423817a1b5c15992d6cc9f8a78 ./tests/Scenarios/Flywheel/VestingScenTest.js
0dd36bafff7cf8d9400c7917bb87dcc2839c172bf49faad41a1746ca6286bbf0 ./tests/Scenarios/Flywheel/FlywheelScenTest.js
734e67402eafdb096dc1a32e670a2e9306fc22a47ccea4d1cbd7669f5d7b28ca ./tests/Scenarios/Flywheel/ReservoirScenTest.js
dff0484a99ddab064e86b685919f8a182edcf622dd8c3aae6d125ae11c31f312 ./tests/Scenarios/Comp/CompScenTest.js
d4e78130d226d6c287a41336b360e33d1acfbe42c7778d0acd54699105b2ded1 ./tests/Flywheel/FlywheelTest.js
94e833dfcbf96436966fddd608764060e47db8969edcb4e0baa04f12d13aba9a ./tests/Flywheel/GasTest.js
c66cacf00aeacedd7dc44ab7e3487dda54220cf2b013cf9401770e3fcaf24d66 ./tests/Fuzz/CompWheelFuzzTest.js
10a0f7464875a618ef12acde3fdfd23d4dc50f0e719725d11dc0931f80808ae8 ./tests/Tokens/adminTest.js
3de85d96d59ef5cdcae84efc2ff5c78b6e90160ec57615273fcd0e8a852753a1 ./tests/Tokens/mintAndRedeemTest.js
3c6dc5c2e501fa2d89e098e5a895362dfdb2623f338121216cbca8b43ebc9e76 ./tests/Tokens/setInterestRateModelTest.js
8f474b7f960c02a1ecacab961d9a0d505111fd5e429d674644e7ab26dcefe150 ./tests/Tokens/borrowAndRepayTest.js
7064e91c262319d840cd8aa324e72ea2dd5e28848900b1478e34a74d2e81e6e5 ./tests/Tokens/accrueInterestTest.js
5e388ec9c56207f99ac6c87f5eb62a7149626a5226ad1afbca2ecdb56025a17f ./tests/Tokens/mintAndRedeemCEtherTest.js
84a2142d55b673ca0656fa1d6d4ba2dde554e03766c429ac6ebcc050fc6ea7f0 ./tests/Tokens/borrowAndRepayCEtherTest.js
eea8a7385a58f55599669f4df859457547ea6aebafeca0bd697cd16c2e77adbb ./tests/Tokens/safeTokenTest.js
2dd78101e9c4bf0e522e8e36ce0bcac9ee80076b97089991fb5c1d370aa2864e ./tests/Tokens/compLikeTest.js
337c0b27103f616b43b9bff42f0f92de07e12124670c664e760fdbdd6f1b1f30 ./tests/Tokens/transferTest.js
b402644e5a52e90a057b5525de33427efaf05cf7827d3f03f4b720dbfa23f96d ./tests/Tokens/reservesTest.js
a55b5b71cfd631bf1887b90469d4fddc021e378460b9ebf685b70f2b09175797 ./tests/Tokens/cTokenTest.js
```

```
6b9058eb944bb10b365da9bbdc4eddba1c2c1bbeacc4cd2673dd73468808bf06 ./tests/Tokens/liquidateTest.js
41e42b91f2676480badf3bcafdbb0a8ed5f24a7f22c3f30fe0982d0d5f038377 ./tests/Tokens/setComptrollerTest.js
0eaab99a5436654137479e7115d75984bb7a0d1cdeb5c129386808690a0d737b ./tests/Models/InterestRateModelTest.js
fb7110f3d39ec431b226cd6e6677796d4f0ee32c2c99a73a178b158182b8d637 ./tests/Models/DAIInterestRateModelTest.js
4dd916fd1ede7837ec238cb592fb4ae905a95c103c39168e7e5bce1ed8eb3923 ./tests/Comptroller/adminTest.js
2242a84ccdec4477aa9e62ba9c65e4761968c0723974f2852889a3647cbc4050 ./tests/Comptroller/accountLiquidityTest.js
2b93650ce41e8dff3214769000ef96cc244d448506effac79eac45cde3ee9648 ./tests/Comptroller/comptrollerTest.js
ff2f54a1aced42cee680115711e86a2649af95c7484c4ee38a50298cb827b5c4 ./tests/Comptroller/proxiedComptrollerV1Test.js
4b93e830dee7d9034e6b4e6204081b932a542a06431e4d26abf44f07b8de1e95 ./tests/Comptroller/unitrollerTest.js
bfae5171df6c8d9108bd34792649b00aaa3266f62e5327c63590b65393f55f0f ./tests/Comptroller/liquidateCalculateAmountSeizeTest.js
28539878d46c8be3ef13576097eb0d21a8d5bdfa183c05c2b319f1e9835c0096 ./tests/Comptroller/assetsListTest.js
e4960aae37d36d52fd26a67f6f553e8f825da3a4e9e29fb7a9ae8429cc463a60 ./tests/Comptroller/pauseGuardianTest.js
```

Changelog

- 2020-11-18 - Initial report
- 2020-11-27 - Fixes reaudit
- 2020-12-03 - Issue 2 description fix.

About Quantstamp

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

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

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

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