Quantstamp Security Assessment Certificate

June 1st 2021 — Quantstamp Verified

Fuse Contracts

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

Executive Summary

Type	Money Market Contracts
Auditors	Ed Zulkoski, Senior Security Engineer Fayçal Lalidji, Security Auditor Jose Ignacio Orlicki, Senior Engineer
Timeline	2021-01-20 through 2021-02-04
EVM	Muir Glacier
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Online documentation
Documentation Quality	Low
Test Quality	Low

Source Code

Repository	Commit
compound-protocol	f162ce5 (initial commit)
open-oracle	0f27248 (initial commit)
fuse-contracts	8e11217 (initial commit)
compound-protocol	79229d4 (final commit)
open-oracle	8dd0c9a (final commit)
fuse-contracts	bfe0053 (final commit)

Total Issues	**13** (11 Resolved)
High Risk Issues	**1** (1 Resolved)
Medium Risk Issues	**1** (1 Resolved)
Low Risk Issues	**6** (6 Resolved)
Informational Risk Issues	**4** (3 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.
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

During the audit a number of issues were uncovered ranging in severity. Importantly, we note that the limited inline documentation and specification made it difficult to fully assess the code. Further, the test suites do not appear to be fully extended to cover all newly added code, and coverage scripts are not available. We strongly recommend improving documentation and test suites.
Update: The report has been updated based on the diff for compound-protocol, fuse-contracts, and open-oracle.
Note: The re-audit only pertained to changes that were directly related to findings in the initial report. Not all new code has been reviewed.

ID	Description	Severity	Status
QSP-1	Unset owner	High	Fixed
QSP-2	Limited tests and documentation for certain contracts	Medium	Fixed
QSP-3	`getSymbolHashIndex` may consume excessive gas	Low	Fixed
QSP-4	Missing input validation	Low	Fixed
QSP-5	Incorrect return value	Low	Fixed
QSP-6	Stale oracle price	Low	Fixed
QSP-7	Array not updated on market exit	Low	Fixed
QSP-8	`_setFuseFee`, `_withdrawFuseFees`, and `_withdrawAdminFees` are callable by any user	Low	Fixed
QSP-9	Non-view public functions design	Informational	Acknowledged
QSP-10	Fund sent by mistake can be withdrawn by any user	Informational	Fixed
QSP-11	Check of positive balances always true	Informational	Fixed
QSP-12	Unlisted price feed does not throw	Informational	Fixed
QSP-13	Unknown `fuseAdmin` address	Undetermined	Acknowledged

Quantstamp Audit Breakdown

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

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

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

Methodology

The Quantstamp auditing process follows a routine series of steps:

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

Toolset

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

Setup

Tool Setup:

- Slither v0.8.0

- Mythril v0.22.10

Steps taken to run the tools:

1. Installed the Slither tool: `pip install slither-analyzer`
2. Run Slither from the project directory: `slither .`
3. Installed the Mythril tool from Pypi: `pip3 install mythril`
4. Ran the Mythril tool on each contract: `myth -x path/to/contract`

Findings

QSP-1 Unset owner

Severity: *High Risk*

Status: Fixed

File(s) affected: `FuseFeeDistrubutor.sol`

Description: Owner is not initialized in `FuseFeeDistrubutor`; all funds withdrawn through `FuseFeeDistrubutor.withdrawAssets` will be sent to `address(0)`.

Recommendation: Use `OwnableUpgradeable.__Ownable_init` to initialize the owner address.

QSP-2 Limited tests and documentation for certain contracts

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `UniswapView.sol`, `UniswapAnchorView.sol`

Description: In the diff versus existing `open-oracle` code, the newly added `UniswapView.sol` is significantly modified from the existing `UniswapAnchorView.sol`, but does not have corresponding tests. Further, there is little inline documentation making it difficult to assess the diff.
In general, this problem is apparent across all repositories (partly due to lack of coverage scripts).

Recommendation: Provide coverage scripts for all diffs. Improve tests for new code. Ensure that testing and coverage instructions are in the documentation.
Update: Tests exist in a separate `fuse-sdk` repository. Inline documentation has been improved.

QSP-3 `getSymbolHashIndex` may consume excessive gas

Severity: *Low Risk*

Status: Fixed

File(s) affected: `UniswapAnchoredView.sol`

Description: `UniswapAnchoredView.getSymbolHashIndex` iterates over `_configs` to get the symbol hash index. Depending on the length of the `_configs` array this function can consume excessive gas when executed during a transaction.

Recommendation: A similar mapping to `_configIndexesByUnderlying` can be used to map hashes to indices instead.
Update: This has only been partially resolved. A new mapping `_configIndexesBySymbolHash` was added to resolve the issue, but `getSymbolHashIndex` was not updated to use it.
Update 2: The issue has been resolved.

QSP-4 Missing input validation

Severity: *Low Risk*

Status: Fixed

File(s) affected: `UniswapConfig.sol`, `PreferredPriceOracle.sol`, `RariFundController.sol`, `FuseFeeDistributor.sol`, `FusePoolDirectory.sol`

Description: The following function should perform additional checks:

1. `UniswapConfig.changeAdmin` should ensure that `newAdmin` is non-zero.
2. `PreferredPriceOracle.constructor` should ensure that both address arguments are non-zero.
3. In `FuseFeeDistributor.sol`, both the `constructor` and `setInterestFeeRate`, the argument `_interestFeeRate` should be validated to be less than `1e18`.
4. In `FusePoolDirectory.sol`, `deployPool` does not ensure that address arguments are non-zero.

Recommendation: Add corresponding `require` statements to above.

QSP-5 Incorrect return value

Severity: *Low Risk*

Status: Fixed

File(s) affected: `FusePoolDirectory.sol`

Description: `FusePoolDirectory.registerPool` does not return the index as expected since the call to the internal function `FusePoolDirectory._registerPool` does not contain a return statement and will always return zero.

Recommendation: Add a return statement in `FusePoolDirectory._registerPool`.

QSP-6 Stale oracle price

Severity: *Low Risk*

Status: Fixed

File(s) affected: `ChainlinkPriceOracle.sol`

Description: `ChainlinkPriceOracle.getUnderlyingPrice` calls `AggregatorV3Interface.latestRoundData` without checking `startedAt` and `updatedAt` values, meaning that the latest round returned can be obsolete since Chainlink aggregators rely on external nodes to be updated once a request is submitted by one of the sponsors.

Recommendation: The values returned by Chainlink aggregator must be validated, both `startedAt` and `updatedAt` should be verified correctly.

QSP-7 Array not updated on market exit

Severity: *Low Risk*

Status: Fixed

File(s) affected: `compound-protocol/contracts/Comptroller.sol`

Description: Users addresses added in `Comptroller.addToMarketInternal` are not removed later when `Comptroller.exitMarket` logic is executed.

Recommendation: `accountAssets[borrower].length` can be checked; if equal to zero remove the user address from the `allUsers` array and `users` mapping.

QSP-8 `_setFuseFee`, `_withdrawFuseFees`, and `_withdrawAdminFees` are callable by any user

Severity: *Low Risk*

Status: Fixed

File(s) affected: `CToken.sol`

Description: For `_setFuseFee`, although the function will set the fuse fee based on the `fuseAdmin` address regardless of the `msg.sender`, it is not clear if any user should be allowed to invoke the function. As one consequence, spurious `NewFuseFee` event messages could be emitted by any user.
It is not clear non-privileged users should be able to invoke the fee withdrawal functions.

Recommendation: Restrict the functions to only be callable by the `admin`.
Update: These function are intended to be called by any users. The code has been updated to not emit events in the case where no changes occur.

QSP-9 Non-view public functions design

Severity: *Informational*

Status: Acknowledged

File(s) affected: `FusePoolDirectory.sol`

Description: Multiple implemented functions in `FusePoolDirectory` consume excessive gas following the array length. Following the code documentation those functions are not intended to be called on-chain. However, some of the functions are marked as non-view since they call third party external non-view functions intended to change the called contract state.

- `FusePoolDirectory.getPublicPools`
- `FusePoolDirectory.getPublicPoolsWithData`
- `FusePoolDirectory.getPoolsByAccount`
- `FusePoolDirectory.getPoolsByAccountWithData`
- `FusePoolDirectory.getPoolStats`
- `FusePoolDirectory.getPoolAssetsWithData`
- `FusePoolDirectory.getPoolUsersWithData`
- `FusePoolDirectory.getPublicPoolUsersWithData`
- `FusePoolDirectory.getPoolUsersWithData`

Recommendation: When using such design, developers should be cautious about the risks since they are calling functions that are intended to change the contract state without changing it, which might introduce errors.
Update: We recommend adding user documentation about any potential risks with these functions. Note that several externally-called function are non-view, which could potentially introduce an off-chain calculation error.

QSP-10 Fund sent by mistake can be withdrawn by any user

Severity: *Informational*

Status: Fixed

File(s) affected: `FuseSafeLiquidator.sol`

Description: The implemented internal functions `transferSeizedFunds` and `exchangeAllEthOrTokens` transfer all the contract ether or token balances to the target address. If funds are sent by error to the contract, any user interacting with the contract will be able to take the funds.

Recommendation: Clearly document this behaviour, or track the users balances using local variables in all liquidation functions.

QSP-11 Check of positive balances always true

Severity: *Informational*

Status: Fixed

File(s) affected: `FuseFeeDistributor.sol`

Description: In `withdrawAssets()` on L54,60, checks ensure that `balance >= 0`, which always holds.

Recommendation: Change L54 and L60 replacing `>=` with `>`.

QSP-12 Unlisted price feed does not throw

Severity: Informational

Status: Fixed

File(s) affected: `ChainlinkPriceOracle.sol`

Description: In `ChainlinkPriceOracle` getting the underlying price of a `CToken` using `getUnderlyingPrice` does not verify if the underlying token is listed in `priceFeeds` arrays.

Recommendation: Add a requirement to validate if the feed is listed and throw with a correct error message.

QSP-13 Unknown `fuseAdmin` address

Severity: Undetermined

Status: Acknowledged

File(s) affected: `CTokenInterfaces.sol`

Description: The address `0x2279B7A0a67DB372996a5FaB50D91eAA73d2eBe6` currently has no transaction history.

Recommendation: It should be confirmed this is the correct address.

Automated Analyses

Slither

1. Slither reported many "linting-related" issues due to existing compound code (e.g., the use of `if(false)`, and unused function arguments).
2. Slither warns of many strict equalities throughout the code. These were classified as false positives.
3. It warns of an external transfer to a user-supplied address in `FuseSafeLiquidator.transferSeizedFunds`, however this is expected behavior.

Mythril

1. Many benign issues were reported related to control-flow dependencies on `block.number` or `block.timestamp`. We classified these as false positives.
2. Similar to Slither, it warns of an external transfer to a user-supplied address in `FuseSafeLiquidator.transferSeizedFunds`, however this is expected behavior.

Adherence to Specification

The specification and inline documentation is limited for the provided diffs. We recommend improving both sources of documentation.

Code Documentation

1. In `ChainlinkPriceOracle.sol` on L77, a comment should be added indicating that `0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2` is the address of `WETH`.
2. In `UniswapAnchoredView.constructor`, the docstring has not been updated to include `_canAdminOverwrite`.

Adherence to Best Practices

1. In `CErc20Delegator.sol`, the newly added functions are declared to return `uint`, however there is no explicit return statement. While this follows the pattern of other functions in the contract, later releases of compound resolved this issue.
2. In `CToken.sol` on L1189, the error message should instead be `SET_FUSE_FEE_ACCRUE_INTEREST_FAILED`.
3. Throughout the `fuse-contracts` repository, there are many long lines of code that should be split across multiple lines (e.g., `FuseSafeLiquidator.sol#297`).

Test Results

Test Suite Results

Note that we could not run the test suite associated with `fuse-contracts`. We recommend providing a full sample `.env` file (for all repositories), and improved test scripts to automate the process.

```
 PASS  tests/TimelockTest.js (19.527s)
 PASS  tests/SpinaramaTest.js (28.082s)
Teardown in 0 ms
Teardown in 0 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Using network test Web3ProviderEngine
Setup in 64 ms
Using network test Web3ProviderEngine
```

```
Setup in 46 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Comptroller/comptrollerTest.js (67.529s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 51 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Lens/CompoundLensTest.js (50.499s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 185 ms
Teardown in 0 ms
 PASS  tests/Tokens/borrowAndRepayCEtherTest.js (90.956s)
Using network test Web3ProviderEngine
Setup in 137 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/mintAndRedeemTest.js (110.035s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 137 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/liquidateTest.js (114.584s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 72 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Governance/CompTest.js (8.922s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 35 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/borrowAndRepayTest.js (128.749s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 190 ms
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/accrueInterestTest.js (41.64s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 107 ms
 PASS  tests/Governance/GovernorAlpha/CastVoteTest.js (5.548s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 36 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Models/DAIInterestRateModelTest.js (97.604s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 192 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/cTokenTest.js (86.159s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 65 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Governance/GovernorAlpha/ProposeTest.js
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 117 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/reservesTest.js (51.366s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 154 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Models/InterestRateModelTest.js (12.738s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 142 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/fuseFeesTest.js (41.557s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 121 ms
 PASS  tests/Comptroller/proxiedComptrollerV1Test.js (58.272s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 133 ms
 PASS  tests/Tokens/adminFeesTest.js (45.427s)
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 60 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Governance/GovernorAlpha/StateTest.js (6.021s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 84 ms
 PASS  tests/Comptroller/pauseGuardianTest.js (45.236s)
Teardown in 0 ms
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Using network test Web3ProviderEngine
Setup in 154 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Comptroller/unitrollerTest.js (17.542s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 108 ms
 PASS  tests/Comptroller/accountLiquidityTest.js (22.952s)
Teardown in 0 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Using network test Web3ProviderEngine
Setup in 133 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Comptroller/adminTest.js
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 87 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Governance/GovernorAlpha/QueueTest.js
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 172 ms
 PASS  tests/Tokens/mintAndRedeemCEtherTest.js (21.18s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 123 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/setInterestRateModelTest.js (27.313s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 101 ms
 PASS  tests/MaximillionTest.js (12.546s)
 PASS  tests/Tokens/transferTest.js (11.797s)
Teardown in 0 ms
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 67 ms
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Using network test Web3ProviderEngine
Setup in 154 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/CompilerTest.js
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 112 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Tokens/adminTest.js (28.599s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 117 ms
 PASS  tests/Tokens/safeTokenTest.js (10.401s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 119 ms
 PASS  tests/Governance/CompScenarioTest.js (10.811s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 120 ms
 PASS  tests/Tokens/setComptrollerTest.js (18.307s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 92 ms
 PASS  tests/Comptroller/liquidateCalculateAmountSeizeTest.js (49.67s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 275 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
```

```
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/Governor/GuardianScenTest.js (48.588s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 45 ms
 PASS  tests/Scenarios/Governor/UpgradeScenTest.js (41.183s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 58 ms
 PASS  tests/Scenarios/HypotheticalAccountLiquidityScenTest.js (63.35s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 68 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/PriceOracleProxyTest.js (146.307s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 184 ms
 PASS  tests/Scenarios/Governor/DefeatScenTest.js (46.203s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 86 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/Governor/ExecuteScenTest.js (69.085s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 218 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/Governor/ProposeScenTest.js (79.767s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 93 ms
 PASS  tests/Comptroller/assetsListTest.js (273.074s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 130 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RedeemUnderlyingEthScenTest.js (142.433s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 117 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/Governor/CancelScenTest.js (86s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 53 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RedeemUnderlyingWBTCScenTest.js (208.157s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 202 ms
 PASS  tests/Scenarios/Governor/QueueScenTest.js (91.449s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 118 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/PriceOracleProxyScenTest.js (100.271s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 83 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/Governor/VoteScenTest.js (52.674s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 211 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/SetComptrollerScenTest.js (46.162s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 117 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/BreakLiquidateScenTest.js (68.086s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 108 ms
 PASS  tests/Scenarios/ChangeDelegateScenTest.js (19.765s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 111 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/EnterExitMarketsScenTest.js (182.501s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 121 ms
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RedeemUnderlyingScenTest.js (200.251s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 56 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/ReduceReservesScenTest.js (142.693s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 126 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Teardown in 0 ms
 PASS  tests/Scenarios/BorrowBalanceScenTest.js (101.048s)
Using network test Web3ProviderEngine
Setup in 189 ms
 PASS  tests/Scenarios/InKindLiquidationScenTest.js (311.47s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 368 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/ExchangeRateScenTest.js (76.936s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 151 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RepayBorrowWBTCScenTest.js (233.956s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 124 ms
 PASS  tests/Scenarios/TokenTransferScenTest.js (113.382s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 109 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95305) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/CTokenAdminScenTest.js (62.13s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 153 ms
 PASS  tests/Scenarios/Comp/CompScenTest.js (135.584s)
Teardown in 0 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
Using network test Web3ProviderEngine
Setup in 137 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/BorrowWBTCScenTest.js (81.47s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 140 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/AddReservesScenTest.js (150.564s)
Teardown in 1 ms
Using network test Web3ProviderEngine
Setup in 57 ms
 PASS  tests/Scenarios/RedeemEthScenTest.js (90.402s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 188 ms
(node:95311) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/UnitrollerScenTest.js (104.692s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 134 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RepayBorrowEthScenTest.js (293.02s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 139 ms
 PASS  tests/Scenarios/ReEntryScenTest.js (18.894s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 54 ms
(node:95309) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/BorrowEthScenTest.js (75.418s)
```

```
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 99 ms
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/TetherScenTest.js (6.134s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 270 ms
(node:95310) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RepayBorrowScenTest.js (220.876s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 147 ms
 PASS  tests/Scenarios/MCDaiScenTest.js (7.938s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 118 ms
(node:95306) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/MintWBTCScenTest.js (123.578s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 156 ms
 PASS  tests/Scenarios/MintEthScenTest.js (106.366s)
Teardown in 0 ms
Using network test Web3ProviderEngine
Setup in 59 ms
(node:95308) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
(node:95307) MaxListenersExceededWarning: Possible EventEmitter memory leak detected. 11 data listeners added to [Provider]. Use emitter.setMaxListeners() to increase limit
 PASS  tests/Scenarios/RedeemWBTCScenTest.js (272.973s)
Teardown in 0 ms
 PASS  tests/Scenarios/TimelockScenTest.js (172.673s)
Teardown in 0 ms
 PASS  tests/Scenarios/SeizeScenTest.js (83.5s)
Teardown in 0 ms
 PASS  tests/Scenarios/BorrowScenTest.js (154.06s)
Teardown in 0 ms
 PASS  tests/Scenarios/MintScenTest.js (91.312s)
Teardown in 0 ms
 PASS  tests/Scenarios/FeeScenTest.js (84.129s)
Teardown in 0 ms
 PASS  tests/Scenarios/RedeemScenTest.js (204.329s)

Test Suites: 81 passed, 81 total
Tests:       17 skipped, 15 todo, 943 passed, 975 total
Snapshots:   0 total
Time:        1036.79s
Ran all test suites matching /test/i.
Teardown in 0 ms
 ✓  Done in 1120.98s.

 PASS  tests/OpenOracleViewTest.js
Teardown in 0 ms
 PASS  tests/NonReporterPricesTest.js (6.093s)
Teardown in 0 ms
 PASS  tests/OpenOracleDataTest.js (12.197s)
Teardown in 0 ms
 PASS  tests/UniswapConfigTest.js (12.9s)
Teardown in 0 ms
 PASS  tests/UniswapViewTest.js (16.125s)
Teardown in 0 ms
 PASS  tests/PostRealWorldPricesTest.js (17.575s)
Teardown in 0 ms
 PASS  tests/UniswapAnchoredViewTest.js (37.141s)

Test Suites: 7 passed, 7 total
Tests:       63 passed, 63 total
Snapshots:   0 total
Time:        41.353s
Ran all test suites matching /test/i.
Teardown in 0 ms
 ✓  Done in 66.33s.
```

Code Coverage

No coverage scripts were available, making it difficult to assess the quality of the test suite.

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

```
741df53fe70bc914a98ce7da3f9aec0adf7f0fc3cb6fe57eda8d437a6f9efdf0 ./OpenOraclePriceData.sol
39b22bd60f6b51a9aea9b9d1da116fae2143511a06323de10c6cc7202d6ff819 ./OpenOracleData.sol
9b88169a14a8bf8e8147be58c03d3ec81c8aa50a724db120dc43d73db6843955 ./OpenOracleView.sol
3f924a8d3797af05e9355d9cf62963dc0617cf75e0355a5113c27e23bab39ee9 ./UniswapLib.sol
d472369436d43750fbdbda850283642851b98db8b88f50cbf8b13857bdd842b3 ./UniswapConfig.sol
828a36f2d86347147a31a758044022448b62cde79928ec931043922d56ca3ba3 ./UniswapView.sol
c7807e42f8246d3a0073004539a9b5e78671de796944ce8cab26f3aa72c87f84 ./UniswapAnchoredView.sol
a96563a07fe5be0317f7d46a0d1d4d897aa7e7e5405220e3f707d4c9fe8a29f0 ./Migrations.sol
f0b97b5c65dd5b7335163b2c63ff622074f880ba1a1fa0b99a6bd734e096fde8 ./FuseSafeLiquidator.sol
d1ed44e24cbfb01b64ed9c051731e709ef01dee55c4ee56d3a6b3ac37b7109ff ./FusePoolDirectory.sol
4bbf485c84d596270387cf6ec2309551a108fb9131f1fa36fa2ab7c56af90398 ./FusePoolLens.sol
95b3e82b3682e24f61487a6ebcf2a2b2dffd84871edb881cdf3433cc2b180d92 ./FuseFeeDistributor.sol
537ae354d4a424fd72183b251525d706bea8a0254b21219cd04d5e0330516fe1 ./Keep3rV1Oracle.sol
37402727f4def63e350704cb3ef8227eaaf6560a9995e11c307e0b0b599163cc ./Bank.sol
dae686b43a74143561fcc31d730bd234460869bec87cda36fc4d14ae19fbbfbb ./Comptroller.sol
6a32c0b851fecbcab78509fdc60e9575e2df12bad69ffae0f61c3ab6f01a7a70 ./CErc20.sol
07923a895fd5a2e7661335a15acb8634864c9872919c6401e361ed8ca158c0cb ./PriceOracle.sol
55c73c8fa1100a6e967e0f007dd99d8b83dcd66168fb9b427d42879a2fb07062 ./CToken.sol
113e2b0fea78167c4024ccc62b6de0e68ad5bcb999da9049672a21a09baf4d1a ./Unitroller.sol
cf322e1daa56bc1bf4b2ed2ae2fee5a82640915d1b140d895d4a0539311d5c0b ./CEther.sol
7bf2969dba6691d8d4e2edf1bc1ef358873e518eff7b405782b827b3821c69c6 ./ExchangeRates.sol
```

da119706448522490c855074d49b6e6720e9d55800d8e2b28a788c8668fecb67 ./MixinResolver.sol

3c349aab778ec93e07e34d338128b1d4659acbbe3989a40c46c74c9c0b2dd93c ./ISynth.sol

1089686256d5fb2e78f553eb60d3661ffb9e9eed45d80717c207f86738c9ca4b ./AddressResolver.sol

c80ba390d254aacdd6be39f4b237ceb3a97290048b2626a94a3e908e449beab0 ./Proxy.sol

46c97c949bce910325e27eda12e21f85b1c8f96a2c9168454c8d58d1ecff799f ./IWETH.sol

1e12cdf8c3ea39617957f16f5cafdc8d68612762d8840c667b16cfdcf279b631 ./AggregatorV3Interface.sol

86d06ff65ff89640f565f246820b66a8d1dd2f79fd3019e1c28c3bb2d075db4a ./IUniswapV2Router01.sol

fece8987fe2b33ef1b883730a23bb241427308781f6653add6aaa76648cdb038 ./IUniswapV2Router02.sol

fa37130ac7235fe7ec4923457337494edcce39f78e62d34ed16525997d73ea87 ./UniswapV2Library.sol

f83b8f66ba979f52edbe5cdf9da867108a711e74e4d39d6f9f84f962a0623504 ./IUniswapV2Pair.sol

a0aaf326cdaea894b36bb520fd400cc3ff50b9601509365a390744366c548dd5 ./IUniswapV2Callee.sol

c99f124bc1337e66ef1784023ad60fc37c4b37cf960b8906a1a4cdd6d3f8d2aa ./IVault.sol

08e701ccd7b58bcb21a4ea1fe569189bdca0e75a39cd0ebeb6d80c7849559d9b ./IVaultV2.sol

fefd1775323083b63a41ca8a2b3debabd0451a1e86a44f43572b89711ad1507a ./BasePriceOracle.sol

dfded2bedf4e6305cd010b7006816dd7da5971230fa8357d1f4ef370cddb292c ./AlphaHomoraV1PriceOracle.sol

eefc430a99b2142257785c1ee4e7d56949b4953ed6ad45d192399810f1afee9e ./MasterPriceOracle.sol

df492520d28b93fa057213e4f7c9b8a1af246006257a4865dae4579770d82d42 ./PreferredPriceOracle.sol

2dd29006e14fc7695f41a766773de5dfd9215c2945f674288f10b2b546c24ca9 ./SynthetixPriceOracle.sol

6adf8f28e3953e907cea904b460033be554b90a8ca68ed587bf8fb847cfe6713 ./YVaultV2PriceOracle.sol

fe9eb97d84ffccf99ff9de294c946ec817511fb39f77ae42a6f79c984a36f8ea ./ChainlinkPriceOracle.sol

443c0ffeac67e7421c77106154e7dc41173d1758906ba506c2b5cb39c57c8283 ./UniswapLpTokenPriceOracle.sol

03536db132ac3ca945cb18e6dc02807e0ce71dc8db4d19d7f9099381839c47b5 ./Keep3rPriceOracle.sol

15c9693ee751ffadd0df511fd01a1f005349cf17d86c78b44c821d9f3312ae3e ./RecursivePriceOracle.sol

740d8f3948cc60798ed8e5ebcd83690c75cdef2ac3ec746923e15cb0d21d7cbc ./YVaultV1PriceOracle.sol

918d5790253d16e1b5221918d040399ad3598aec848b6a9007428965fe57e058 ./contracts/EIP20NonStandardInterface.sol

740241b3304332bd2329f10d691b165acea3170ff333245c0fae3727da0bd134 ./contracts/ComptrollerInterface.sol

fb6745aa44143601ca42c5e43a0ad490e548f213635003c6e4b55bee6ca06a17 ./contracts/ComptrollerG1.sol

6c891b015e1b95b4080622f0f2d25ba26654c7659fc0ec49107bdc017f0bc260 ./contracts/Comptroller.sol

4cf422072ebb8bfde8b806190589befc6b88bc2ebe2fa9e663414f648e0a7868 ./contracts/CErc20.sol

cbe3decf83d6d3649271438102e64ca68ff1c708294d2077a7ea58915ebfc667 ./contracts/Exponential.sol

7640a53ea1a186b2fb7748175d9d78a6db16c365c25a5a2019bfbe3107f8702e ./contracts/IFuseFeeDistributor.sol

8a5a574ee7b71ab417d5065cff4759ea32ce5c15f65e6e70fcbdd9a41d19c153 ./contracts/PriceOracle.sol

84062a9c79c49540412ca1937901e846b39d654577abef2abf8a484f28f61373 ./contracts/CToken.sol

2d2c169c80256b3554744d77b715a5793dc320cee9ed97640d0733951a59af9c ./contracts/CErc20Delegator.sol

8bf61c84b872ead30d77a98c511ee1e71790772d13df75109d118a8c8f49a54f ./contracts/CEtherImmutable.sol

6fad549a6e8e5b7a48f686da454ddd90900e6fd2275dbb9d9614b51015075812 ./contracts/CErc20Delegate.sol

f8d86756385ad250677ffac757ce31a34622af2c96e36401c8c3f48d06e95002 ./contracts/CDaiDelegate.sol

204a19fb7a661c5bafcd5f7916254a457ca1fd9104e5708a73dd5010b11353dc ./contracts/SafeMath.sol

c223d53c6acca3307512f8fc36727e99a37e58ae4d75a9aa0e9450fa9da10ce7 ./contracts/ErrorReporter.sol

050b50b9544b56ab35f26ea3ea139ca6c58544fa435e4107b8c241948e23902b ./contracts/Unitroller.sol

dcb5b6857f6455d1daf77feb84a4cd11d3fb191fbc8097315479e88308f89083 ./contracts/CarefulMath.sol

36a81d9c51869682d7428c80357b0bd5ce9c41abb5ca51015f115fe33ae3a0e1 ./contracts/JumpRateModel.sol

ea4204fc8c5c72a5f4984177c209a16be5d538f1a3ee826744c901c21d27e382 ./contracts/Timelock.sol

bc2ecd2927c202aab91222af287c07503cb348d8a96da3d368f195648356c4b7 ./contracts/EIP20Interface.sol

7d992de9a0711d9cc0a0c3d4b301377b339f1146ac6f37ea1609b34c7d0882c5 ./contracts/InterestRateModel.sol

67b79f97c413e388b7e9ae451f4d27c280218ee5449c76f884e0074cf761dab0 ./contracts/ComptrollerStorage.sol

b5d06e0d725b01ecb8d0b88aa89300ddc0399904d84915a311f42f96970ba997 ./contracts/WhitePaperInterestRateModel.sol

6d5ab5c24cc133aadd45e4106b954347145f6f68ed67c8031709009ffe7c2083 ./contracts/CEtherDelegator.sol

d001ad3fbacbffa399a177b024ddcfd323fdffbf90712eda346946752072d278 ./contracts/CEtherDelegate.sol

ad8716c2277b1ef11b7ba767686816b8eb64d395aaed817faf7bc576467cae66 ./contracts/DAIInterestRateModelV2.sol

afaa6b004044d9c0f18104ec84bb4bd30af36f4045ad95816d61f517abf2c428 ./contracts/CErc20Immutable.sol

98d77b0d0aae78a7fde8910828649991679369 6f7ece848357ed1e4fb8d2d957 ./contracts/CEther.sol

32f9252032165bfe274fe16f0d74b3f7add6a037b7183dc964bcf01d0a5e687c ./contracts/Maximillion.sol

d2246fc240b4810a14915b760546531935135ce61927d1eed82e1e91a5557bb3 ./contracts/SimplePriceOracle.sol

5a8b3eae6bcf5b258696b1eb3b7286d8ae645d6541bb38697ba2a20b4d03062b ./contracts/CTokenInterfaces.sol

8a0553ad8bd250fc18710315dee64e3425550589c6466c01c3227fd8c7b3f1d4 ./contracts/Governance/GovernorAlpha.sol

874013f6c87f2b0bf0a5d81a57fdd298ec191686cb6eed4c8498f402ef3597e6 ./contracts/Governance/Comp.sol

ec42e688c7e46c4b20c0a4cb3774ad1a1ace29d12cffb777e2e5972a6afabea5 ./contracts/Lens/CompoundLens.sol

Tests

85d9a0357febb013212dd97b93e827cee5401c77684e244fd3abb0c1cd6d2022 ./fee-distributor.js

```
1cff79de87ed5a05804526ce12e4de2317dc18bd2c42b8ac3cbc3d529d90aa5f ./PostRealWorldPricesTest.js
dead39896123e5c72a245d0b18a608e6f5f44e9a7f647961b0bd00b07fad5f23 ./UniswapViewTest.js
80b81fbb0418b92491e4ef40e29eadf4c542f007dabfda04cf66a741edec7546 ./UniswapAnchoredViewTest.js
e6f3d23865c5facd77ead1b93f66124a4be9079bca9a420a567196c5fe5b3a0d ./UniswapConfigTest.js
8edba59c2c02408fa0fe7d591380e0fd7d6cae1440654e284f9b0f446fccc9a7 ./DockerProvider.js
8f9b9584f9192a88bec344a229f4d14f844e788f37737c52c0af14c9fc6e5dd3 ./Matchers.js
e4ca2566b2b6343d439a0749081f8230bd3eccc1134e938fbc0bde13e6fe45c9 ./Helpers.js
ebddad1577fcccb914974eab82acd37d24acdea1a83e9fbc710968c3028694e9 ./OpenOracleViewTest.js
56030fc263870aeb23b4b39558330c5848d02378ea669a34ada99fe86156c0d6 ./NonReporterPricesTest.js
1e3ed9b146af3b28ec3ef2ff0f274b875ea88f3285aebfc671f6068e98955275 ./OpenOracleDataTest.js
7dede022d948181c58908c360f7deabad8ad821543b298c7663e43ea93045e84 ./MockUniswapAnchoredView.sol
42088d9b821114a78453c92473fe2f5bd6319a20850745a2cc2229a6a7453eb7 ./Test.sol
9d9b03c8ff013f1c9a14075d55e852f5e12e6667652731615b646f858e52898c ./ProxyPriceOracle.sol
1eaf946ae2bff0484a9422444958668b7d4a10211860ff299511f0749732e9a0 ./MockUniswapTokenPair.sol
8967104cc6adef5132b04d737242621ae19fd546cf3a62b4df948b85df1f3723 ./MockUniswapView.sol
1cff79de87ed5a05804526ce12e4de2317dc18bd2c42b8ac3cbc3d529d90aa5f ./PostRealWorldPricesTest.js
dead39896123e5c72a245d0b18a608e6f5f44e9a7f647961b0bd00b07fad5f23 ./UniswapViewTest.js
80b81fbb0418b92491e4ef40e29eadf4c542f007dabfda04cf66a741edec7546 ./UniswapAnchoredViewTest.js
e6f3d23865c5facd77ead1b93f66124a4be9079bca9a420a567196c5fe5b3a0d ./UniswapConfigTest.js
8edba59c2c02408fa0fe7d591380e0fd7d6cae1440654e284f9b0f446fccc9a7 ./DockerProvider.js
8f9b9584f9192a88bec344a229f4d14f844e788f37737c52c0af14c9fc6e5dd3 ./Matchers.js
e4ca2566b2b6343d439a0749081f8230bd3eccc1134e938fbc0bde13e6fe45c9 ./Helpers.js
ebddad1577fcccb914974eab82acd37d24acdea1a83e9fbc710968c3028694e9 ./OpenOracleViewTest.js
56030fc263870aeb23b4b39558330c5848d02378ea669a34ada99fe86156c0d6 ./NonReporterPricesTest.js
1e3ed9b146af3b28ec3ef2ff0f274b875ea88f3285aebfc671f6068e98955275 ./OpenOracleDataTest.js
f5353e5a9b425db9fcbd586f98bce641a04d5d4a3ebbaaf9c8f34e9d9114159b ./MockUniswapAnchoredView.sol
42088d9b821114a78453c92473fe2f5bd6319a20850745a2cc2229a6a7453eb7 ./Test.sol
9d9b03c8ff013f1c9a14075d55e852f5e12e6667652731615b646f858e52898c ./ProxyPriceOracle.sol
1eaf946ae2bff0484a9422444958668b7d4a10211860ff299511f0749732e9a0 ./MockUniswapTokenPair.sol
79162b8b981468c9b24b648c574688065a1a7b202c708f8638fe101b28c8edc3 ./MockUniswapView.sol
a7376686eb77c45f312433c8f9cd35a0a91f61b5fff71c915f018c41b3eb8a39 ./tests/TimelockTest.js
5358fa45a77b2597d46448b7aecc96de55894ba08c6602ced648bf7a0b7c1fd5 ./tests/Jest.js
cb9ee641b3aa7df9e7f188c17b71b0b97f387c166915408bf09b4d0ff932c62a ./tests/CompilerTest.js
0a0a31d16c3b086e44cdbc6293fe647f72ab6d04513b3ff3eeea610f30426676 ./tests/SpinaramaTest.js
e743152d69acebc103976cbcc5308e2c4b04dc88b0aa9758042f622e6b04895c ./tests/Matchers.js
ef6b1a22aca7c79d9bbe28e11a488d90712d8f570acddd90faaaa760c4f34b16 ./tests/Errors.js
195e04575a62b67b0122ea8936b54dec20353e003737acf931cd1db3dfb6ee14 ./tests/MaximillionTest.js
4881988d8aecdd723aec711d7a0c491108cac041438827118d2df9d9406054f9 ./tests/gasProfiler.js
4afc7ad52ed18baf2f66194ed483717f4401b076f3da64662726cd19abb6a92b ./tests/Scenario.js
19dda8605a559d42ee39f9157edf3692c7e69a3cc865c322718f5d38e78a847c ./tests/PriceOracleProxyTest.js
41e42b91f2676480badf3bcafdbb0a8ed5f24a7f22c3f30fe0982d0d5f038377 ./tests/Tokens/setComptrollerTest.js
1e557f4e0f005d3c22d057114a4b137d293ea773a2883e8e1cf14e5c6194ea7f ./tests/Tokens/mintAndRedeemCEtherTest.js
10a0f7464875a618ef12acde3fdfd23d4dc50f0e719725d11dc0931f80808ae8 ./tests/Tokens/adminTest.js
4ae356b56c2cd9d0c734ddfd3b60bc4f7c009359141c736fef084828873293df ./tests/Tokens/accrueInterestTest.js
3c6dc5c2e501fa2d89e098e5a895362dfdb2623f338121216cbca8b43ebc9e76 ./tests/Tokens/setInterestRateModelTest.js
db2ea3dde6edca6e0a271809c597cc8b92053cf04a5dab620a2e573e894484e0 ./tests/Tokens/borrowAndRepayTest.js
64b86160333767ebaa9511c88d07f35408728331be81e1ed8d5ec653cb2ee9c2 ./tests/Tokens/borrowAndRepayCEtherTest.js
fbf1f252d25f3de7999bc383d1f675fbebf99d53ee87e81f68d23eb1ec85c2ee ./tests/Tokens/liquidateTest.js
eea8a7385a58f55599669f4df859457547ea6aebafeca0bd697cd16c2e77adbb ./tests/Tokens/safeTokenTest.js
9561e78bcc5609a7cd09a7469f239cec2a87331028ad2f4bb96f17f28d77a439 ./tests/Tokens/fuseFeesTest.js
4f4326a42de75cb73f0b3c38f1717d2824f032070ffaff4a34b8458cdd7da5a8 ./tests/Tokens/mintAndRedeemTest.js
f06a70fb618081fdac17c57602d3b123e5c4947611104f5b854be243e3a22882 ./tests/Tokens/adminFeesTest.js
337c0b27103f616b43b9bff42f0f92de07e12124670c664e760fdbdd6f1b1f30 ./tests/Tokens/transferTest.js
4e4f84f9360267f5382270f21a5966bb54c2c06508db5fdcb94bd955cde6f7e9 ./tests/Tokens/reservesTest.js
3b0ff7932b35128ecf2c004bf7c7e702289f79d23f35c66fa534362b93b41b34 ./tests/Tokens/cTokenTest.js
4dd916fd1ede7837ec238cb592fb4ae905a95c103c39168e7e5bce1ed8eb3923 ./tests/Comptroller/adminTest.js
4b9712da45967d30094d62edc395b96324172b63d623e6d4649ef34679e4663f ./tests/Comptroller/liquidateCalculateAmountSeizeTest.js
b04db2d2aea981533e510fbafd634d764ad6a9fbe7909da21849a1d33af6355f ./tests/Comptroller/accountLiquidityTest.js
35cbb19deef587b6baa79954d0d76a297493061310f79cc6f72f9431224a3ec5 ./tests/Comptroller/comptrollerTest.js
ff2f54a1aced42cee680115711e86a2649af95c7484c4ee38a50298cb827b5c4 ./tests/Comptroller/proxiedComptrollerV1Test.js
4b93e830dee7d9034e6b4e6204081b932a542a06431e4d26abf44f07b8de1e95 ./tests/Comptroller/unitrollerTest.js
```

7fedc5fe287daf65eedaf2b9fe4cd90c29441a12b5e3032a5bfc709972de4757 ./tests/Comptroller/assetsListTest.js

e4960aae37d36d52fd26a67f6f553e8f825da3a4e9e29fb7a9ae8429cc463a60 ./tests/Comptroller/pauseGuardianTest.js

c0ef9125ef417a1216d648e9ae546f412c980ac1ef1de7d2c164b5a2aaa40eb9 ./tests/Governance/CompTest.js

2a481672769902fc25ebc4d58c9d58917155f4e92ff56543280f8114884fb7b9 ./tests/Governance/CompScenarioTest.js

5f5972390f0f1666982ff55ff56799b52748e0e1132805a2f37a904396b27fe3 ./tests/Governance/GovernorAlpha/QueueTest.js

45f10e9446c8d68eead1fc509a220fa0dc854f0d4d24d2fef972bbebe74a64f2 ./tests/Governance/GovernorAlpha/ProposeTest.js

10bd124f58ad69ba89f228fa77306e2df3f9435717d0d112ff120e10bb9b38a7 ./tests/Governance/GovernorAlpha/CastVoteTest.js

b220d6f0047d78cd420176a98763fed8160cf7a0e877a50b14e08a5da4adc84c ./tests/Governance/GovernorAlpha/StateTest.js

e37a817659914f87330a3347a534a4b42aa98ee8307f8f4e4ead02f3f4c0c639 ./tests/Scenarios/RedeemScenTest.js

4c716c17c8d6d607621dd117900898731e9380df408ec22a1c141bcd7ec4965e ./tests/Scenarios/FeeScenTest.js

8e8b23d890c2c95bbc6adec14363a19f9d82dd3fa989a8ce3641e90b5fcb4b62 ./tests/Scenarios/RepayBorrowScenTest.js

a05ea0319b7966741c6a4944680ff5b7586132c5bca1b649685a9d1f0a97dcf9 ./tests/Scenarios/RepayBorrowEthScenTest.js

fbebcc9776712f53927fda86b2f86093e6b749f4602e31630dfb04462d30cd3c ./tests/Scenarios/BorrowEthScenTest.js

b3e59040b0087633e9f66dc4259d1d4fd5a04e4cfb76bb877713f8c830e9c690 ./tests/Scenarios/MintEthScenTest.js

b27517399783a102932891ffd3e632421e809cac2245bbcc2b4f7b2c23cfbf89 ./tests/Scenarios/ChangeDelegateScenTest.js

16b28c43b7e03d0940111656945db3b1053c2753a623333ebfd85e81dfba4b1c ./tests/Scenarios/HypotheticalAccountLiquidityScenTest.js

2eb4bcabc0cbd1af93d91ff1157b2183cfb9bd881e8e977bccf1575b5443e799 ./tests/Scenarios/SeizeScenTest.js

e3523f04ddfd19a14a44f74f32dd77305e06414af2e0ba1749b00c258b00ea87 ./tests/Scenarios/ExchangeRateScenTest.js

2f903f59c90057cfe955b933ae3fb7b17f097e8ca28d2efb3e8e7cc56e1403eb ./tests/Scenarios/RedeemWBTCScenTest.js

13f66b96a6e1ef1f0150a609c9a841fd01ce62493f6dfda92a6af821a218b6d8 ./tests/Scenarios/MCDaiScenTest.js

4a3529fcea2305838a08275b4ceeb4861fea396e9a5cb4acb651d96c0c3de729 ./tests/Scenarios/TokenTransferScenTest.js

d505cbc2d5d96010232526ce9f8c44f32e8c0f8cd732ef8a8da11b4c1c5a676e ./tests/Scenarios/MintWBTCScenTest.js

3f8068cd66e6d3dd9e483cabc896690dacc3050446d97c85bcba37ad4524d9a5 ./tests/Scenarios/AddReservesScenTest.js

76bdb38fdec13324d65e2e22d5a51cc11971e92d29f26f3671143151e6788955 ./tests/Scenarios/TetherScenTest.js

4bab260de71fdf7f22d7419ee041e68ecfe68c245e0bfe17af9b5df9394f8dbc ./tests/Scenarios/UnitrollerScenTest.js

9462f13e5d02224092386a00d92d261bb805079c1131fe2d1ca159d87a03d30a ./tests/Scenarios/BorrowBalanceScenTest.js

48966575141a703b0b5ffae7883627768eb63fbf15deedff9446fb3be607b0ee ./tests/Scenarios/RepayBorrowWBTCScenTest.js

be689993bebc216c4cac9781ae286bf810aa34c793d8d743c53945c787d3ebd9 ./tests/Scenarios/EnterExitMarketsScenTest.js

01ca493f015cc003b578b60a7df83a8c7c576dbff3b0efbb91bf1ea67ad153ec ./tests/Scenarios/TimelockScenTest.js

2de2738aa61707ba2d2191babe2f55d1351fa140fdeb6af82074569df30d6f2e ./tests/Scenarios/SetComptrollerScenTest.js

18bd40435c9385aae3b5018bdb65da6265eff8b26d16d8e9a03ffa26049efff9 ./tests/Scenarios/ReEntryScenTest.js

c294549c150c8f3fe0ce7f9708d4e12860c5725fe20948e712d8e8651f540e6b ./tests/Scenarios/RedeemEthScenTest.js

506be5485394cb2c9bbc6f6bb6cc45b234a6c352172577706b27d1a7de4f4c9f ./tests/Scenarios/RedeemUnderlyingScenTest.js

9ba1859b1e2341272c60a134855b585b9044d3b98d60e4cbbad571fe7423effc ./tests/Scenarios/CTokenAdminScenTest.js

5e1c8ebd93d8065bd53b7ff1867dcb2a8dc430b6faa9d5dad949a0b7d7831aad ./tests/Scenarios/InKindLiquidationScenTest.js

e08db9fbdfd99a4b7704073b2cc64dcc7a18371ff0ec37723decdc7df5cefd90 ./tests/Scenarios/RedeemUnderlyingEthScenTest.js

ecfbedea3ca6e97266b4e76555ec6f7705628055998a3bc7f7051039292a067a ./tests/Scenarios/RedeemUnderlyingWBTCScenTest.js

7e6e76b14ed1fcf84ea6ac065be86fe0392cd2ac56851b5dc13ba9d7e6a37334 ./tests/Scenarios/BorrowScenTest.js

cfce4030a370f632f1d9df7d2d44e4dc0af05ec641bd223ec906b24b0c09bb07 ./tests/Scenarios/PriceOracleProxyScenTest.js

c7889c9279fe003850a17fcb8a14f16357af221b522d8163decd38908e70ef68 ./tests/Scenarios/MintScenTest.js

b37e241c41fe97f45361a7d135afb2c699fccb565ecd2abf9d32ef57b50c0562 ./tests/Scenarios/BreakLiquidateScenTest.js

c3261939c88aa2a210d91c18118f6f06d38212ca3e8cb0125c79538bc601989d ./tests/Scenarios/BorrowWBTCScenTest.js

93a699f3cb8cf2978e5ad148d25443f355a3f119bdf84d4f7a4fcbefa0629c4a ./tests/Scenarios/ReduceReservesScenTest.js

dff0484a99ddab064e86b685919f8a182edcf622dd8c3aae6d125ae11c31f312 ./tests/Scenarios/Comp/CompScenTest.js

d258fb116bb44586f517e6703f1be7e244d5f566eb76882c2cebdecfc9608b7c ./tests/Scenarios/Governor/ExecuteScenTest.js

aa4f9419cfa64c2781b88e3a8a86f15243e7d1ffd3d10ceba24f09a158856ffa ./tests/Scenarios/Governor/ProposeScenTest.js

00b7d5ad7266361d1de01459f809b178c1f683a2714fed986fdbbdda9675d185 ./tests/Scenarios/Governor/CancelScenTest.js

4eeafe9f7d5b95fe0737438464ec96a1ee1337408e44457f57307ea973f64a77 ./tests/Scenarios/Governor/UpgradeScenTest.js

3ed48d345ed89b6f02c81990f3ba912ea71500d177d7920ef95d11363e868869 ./tests/Scenarios/Governor/DefeatScenTest.js

dcff6540ca7ad2d404d6f0820f1f699c5e2a721883a2115a094067768d327068 ./tests/Scenarios/Governor/QueueScenTest.js

98e20441a2e53f58fdcdf95d3bd60f708ad96597dec7e140d0fbceebd0d3e03c ./tests/Scenarios/Governor/GuardianScenTest.js

a8d77f870a989264aaa2c6361d0cd46ea93497dc886d851d7c068a087674aee2 ./tests/Scenarios/Governor/VoteScenTest.js

e9ea8a272199c7aae90a501f2ab5a644d9d28f93964c50b9120f20dce3fcea18 ./tests/Lens/CompoundLensTest.js

8df8bc4353c4eefe0951f932488ff8fd685b08768ae5632b8ab044c1ceea1f52 ./tests/Models/InterestRateModelTest.js

39be23e87a13f8358879af1b0bb9e943c35ab8af939382e1b09e4c2567ca35f5 ./tests/Models/DAIInterestRateModelTest.js

17f1dae75f61ebf222ffab3ff97df7a0a42740dd7513e75dd8cb41cdb561c001 ./tests/Utils/JS.js

27fe3919f7c3bc28e1822aa1f0ccdf750285abf813d1dee490c35137047ffdaa ./tests/Utils/EIP712.js

a3421ed1eb4b1cd2613ee3c02d7953b84425f8760d6f4423ff0e7776cf3bbb64 ./tests/Utils/Ethereum.js

9bb1d5dfe230ca568c52765c874282264bce5df9222a25529f37112b7c118f90 ./tests/Utils/Compound.js

760666fd6801178144a7e2e5ee4fcdf761e63ab1d4dad5d3f483f3eea004ba94 ./tests/Utils/InfuraProxy.js

bf84c0e16a80947ad63f6dfa9e973f9b47437c1758450d45570a14af4c2b085c ./tests/Contracts/Const.sol

```
0d7fd9df64cf72889d6ac97afd3258167116518748488e997505f27cc16b4fe6 ./tests/Contracts/MathHelpers.sol
3cc11b832ed5b3e5c18e01b21fb86fa0f37badd626364933b62640c3aff7a685 ./tests/Contracts/WBTC.sol
176d795f35868f6c3df6800a6ebfa3589e03a7fa577efc11d123bdb5ca58fab7 ./tests/Contracts/FeeToken.sol
b2ecb6ed9cb46b1813e86b45bfda3b15a715fa4c05ae9db7df38d83a777b8126 ./tests/Contracts/FalseMarker.sol
10144c7d50d2679e2f4ea63df2ed58ec14f22e8e09d77d15473a55f8e3f58d5e ./tests/Contracts/Structs.sol
34eaaa9e85252b43034072160b7cc4452a08ca3b4a9c3bd28cda689be83bff0b ./tests/Contracts/ERC20.sol
349649b88d6e9f805a384a8d045a269a582d5cce165b67c6b6faff159cbb91a1 ./tests/Contracts/ComptrollerScenarioG1.sol
4e85b16aaa42a85cfeff0894ed7b00ead01cfdc5d42dde1a9251f638208e9234 ./tests/Contracts/GovernorAlphaHarness.sol
cf43a610e04d279dfffad601eeb48b4006d545410e20f08be012654142797f00 ./tests/Contracts/TetherInterface.sol
d2056385754d16486ed601ee4f1af940349a88bb7dfd660859786fcbf919571c ./tests/Contracts/ComptrollerHarness.sol
2f4dbcc4fe47083cff4db7c60220550b063b258346e77075a26fea1435bbd3bc ./tests/Contracts/MockMCD.sol
fdf2f2ea8ae514125babb2484d04fcbd4773127698bcf254eaa58bde65ac2ace ./tests/Contracts/CEtherHarness.sol
dfe52a0a041631f00e3851a90307683cf50a93e6a97e9e9d8eef1ef0dd741264 ./tests/Contracts/FixedPriceOracle.sol
d4fe8238e018dc1299366e0a5b8f1499e01ce10f0d39dffe2d000a8729433b60 ./tests/Contracts/TimelockHarness.sol
9e86b10a2659f302d1643e1cd2c492c698b33e97e166e0ce647da492da5b614d ./tests/Contracts/Counter.sol
a3c8ad4dbbb5bd58806b0e1285fe8c9319d9c8fb4dfaed3d862a35647b1cc159 ./tests/Contracts/InterestRateModelHarness.sol
5dabf4413d579426e299886b7124e6bf5c415a1fd8fc6d3322c8af0c3d49a532 ./tests/Contracts/CompHarness.sol
7e10baf5e8ab1793e452a9d28a3052534b47972c1c31a33939e36aa84301ea7d ./tests/Contracts/EvilToken.sol
bf2001547e1910070ef8799e0f245988daebd05e17026904b2bd6ed7f953b22e ./tests/Contracts/CErc20Harness.sol
5288acf7cb76e1b86658fa7b7812b118fb405700543fd43d31d0431029b7e688 ./tests/Contracts/FaucetToken.sol
```

Changelog

- 2021-02-04 - Initial report
- 2021-03-04 - Revised report

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.