Quantstamp Security Assessment Certificate

July 25th 2021 — Quantstamp Verified

Rari Capital (On-chain Governance)

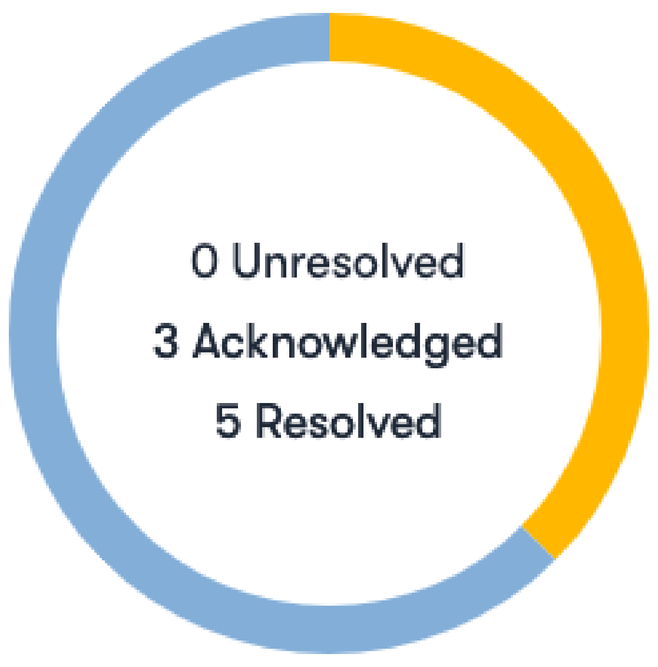
This smart contract audit was prepared by Quantstamp, the leader in blockchain security.

Executive Summary

Type	
Auditors	Fayçal Lalidji, Security Auditor Ed Zulkoski, Senior Security Engineer Kacper Bąk, Senior Research Engineer
Timeline	2021-06-22 through 2021-07-22
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review.
Specification	None
Documentation Quality	Medium
Test Quality	Medium
Source Code	

Repository	Commit
compound-protocol	79229d4...134db9c
rari-governance-contracts	None
fuse-contracts	None

Total Issues	8 (5 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	2 (2 Resolved)
Low Risk Issues	2 (2 Resolved)
Informational Risk Issues	3 (1 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

Initial Audit
Through reviewing the code, we found **8 potential issues** of various levels of severity. We recommend addressing all the findings.
Reaudit Update
All highlighted issues during the audit were fixed by Rari Capital team.

ID	Description	Severity	Status
QSP-1	`ChainlinkPriceOracleV2._price` Does Not Consult Decimal Values	^ Medium	Fixed
QSP-2	`FixedEurPriceOracle` May Return Stale Prices	^ Medium	Fixed
QSP-3	Unintended Code Removal In `Comptroller.mintAllowed`	⌄ Low	Fixed
QSP-4	Incorrect `getUnderlyingPrice` Computation	⌄ Low	Fixed
QSP-5	Unused Constant `TokenErrorReporter.UTILIZATION_ABOVE_MAX`	○ Informational	Acknowledged
QSP-6	Unchecked Function Arguments	○ Informational	Acknowledged
QSP-7	Allowance Double-Spend Exploit	○ Informational	Mitigated
QSP-8	Inconsistency Use of `minPeriod` In `_workable` and `_updateable`	? 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.

Findings

QSP-1 `ChainlinkPriceOracleV2._price` Does Not Consult Decimal Values

Severity: Medium Risk

Status: Fixed

File(s) affected: `ChainlinkPriceOracleV2.sol`

Description: The function `_price` queries various Chainlink oracles, however, the decimal value associated with each price feed is not considered. This may lead to over/undervaluing the price of the `underlying` token being considered.

Recommendation: Check the `feed.decimals` amount during price calculations.

Update: Fixed in: https://github.com/Rari-Capital/fuse-contracts/commit/ff215726d291b9285c2c941203ae551766edd1a1

QSP-2 `FixedEurPriceOracle` May Return Stale Prices

Severity: Medium Risk

Status: Fixed

File(s) affected: `FixedEurPriceOracle.sol`

Description: The function `_price` consults several oracles without ensuring that the returned data is recent. This may lead to stale pricing results and potential arbitrage.

Recommendation: Check the `updatedAt` value returned from `latestRoundData` to ensure recency.

Update: Fixed in: https://github.com/Rari-Capital/fuse-contracts/commit/d21c44c836a82a58317563db6f2828564186d445.

QSP-3 Unintended Code Removal In `Comptroller.mintAllowed`

Severity: Low Risk

Status: Fixed

File(s) affected: `Comptroller.sol`

Description: The following snippet was removed, however, it seems this check is necessary based on the function name.

```
// Make sure minter is whitelisted
if (enforceWhitelist && !whitelist[minter]) {
    return uint(Error.SUPPLIER_NOT_WHITELISTED);
}
```

Recommendation: Revert the removal.

Update: Fixed in: https://github.com/Rari-Capital/compound-protocol/commit/134db9cc99f83db418e709f8c4b59ee9eb607480.

QSP-4 Incorrect `getUnderlyingPrice` Computation

Severity: Low Risk

Status: Fixed

File(s) affected: `FixedEurPriceOracle.sol`

Description: The function `getUnderlyingPrice` appears to be copied from `FixedEthPriceOracle.sol`, and therefore relates the token price to ETH, not EUR.

Recommendation: Implement `getUnderlyingPrice` to relate to EUR instead of ETH.

QSP-5 Unused Constant `TokenErrorReporter.UTILIZATION_ABOVE_MAX`

Severity: Informational

Status: Acknowledged

File(s) affected: `ErrorReporter.sol`

Description: The constant `UTILIZATION_ABOVE_MAX` is newly defined, but it is not used anywhere.

Recommendation: Clarify if the constant is still needed.

Update: Rari team update: "the constant is leftover so we don't mess with the error order numbers on upgrade".

QSP-6 Unchecked Function Arguments

Severity: Informational

Status: Acknowledged

File(s) affected: `ChainlinkPriceOracleV2.sol`, `UniswapV3TwapPriceOracle.sol`

Description: 1. `ChainlinkPriceOracleV2.constructor` should ensure that `_admin` is non-zero.

1. `ChainlinkPriceOracleV2.changeAdmin` should ensure that `newAdmin` is non-zero, unless this is intended to revoke privileged roles.
2. `UniswapV3TwapPriceOracle.constructor` should ensure that `_uniswapV3Factory` is non-zero.
3. `RariGovernanceToken.upgrade2()` all input addresses should be validated correctly.
4. `UniswapTwapPriceOracle.constructor()` should ensure that all addresses are valid.

QSP-7 Allowance Double-Spend Exploit

Severity: Informational

Status: Mitigated

File(s) affected: `RariGovernanceToken.sol`

Description: As it presently is constructed, the contract is vulnerable to the allowance double-spend exploit, as with other ERC20 tokens.

Exploit Scenario:

1. Alice allows Bob to transfer N amount of Alice's tokens (N>0) by calling the approve() method on Token smart contract (passing Bob's address and N as method arguments)
2. After some time, Alice decides to change from N to M (M>0) the number of Alice's tokens Bob is allowed to transfer, so she calls the approve() method again, this time passing Bob's address and M as method arguments
3. Bob notices Alice's second transaction before it was mined and quickly sends another transaction that calls the transferFrom() method to transfer N Alice's tokens somewhere
4. If Bob's transaction will be executed before Alice's transaction, then Bob will successfully transfer N Alice's tokens and will gain an ability to transfer another M tokens
5. Before Alice notices any irregularities, Bob calls transferFrom() method again, this time to transfer M Alice's tokens.

Recommendation: The exploit (as described above) is mitigated through use of functions that increase/decrease the allowance relative to its current value, such as increaseAllowance() and decreaseAllowance().
Pending community agreement on an ERC standard that would protect against this exploit, we recommend that developers of applications dependent on approve() / transferFrom() should keep in mind that they have to set allowance to 0 first and verify if it was used before setting the new value. Teams who decide to wait for such a standard should make these recommendations to app developers who work with their token contract.

QSP-8 Inconsistency Use of minPeriod In _workable and _updateable

Severity: *Undetermined*

Status: Acknowledged

File(s) affected: UniswapTwapPriceOracleRoot.sol

Description: When checking the timestamp of the most recent observation, _workable uses the following expression: ... > (minPeriod >= MIN_TWAP_TIME ? minPeriod : MIN_TWAP_TIME), whereas _updateable does not consider minPeriod, only referring to MIN_TWAP_TIME.

Recommendation: Clarify if this is the intended semantics for _workable and _updateable.

Update: Rari team update: "This is deliberate, we want bots to be able to specify their own minPeriod in _workable, but it is not necessary to force this condition in the update function".

Code Documentation

1. In UniswapTwapPriceOracleRoot.price the check underlying < WETH should have documentation that describes the sorting in price pairs.
2. On L23 of Comptroller.sol, the comment "Emitted when an admin supports a market" does not seem to match the related event MarketUnlisted.

Adherence to Best Practices

1. State variables should be defined before their usage in each contract.
2. Comptroller._setWhitelistStatuses should first check that suppliers.length == statuses.length.

Test Results

Test Suite Results

```
Test Suites: 59 failed, 22 passed, 81 total
Tests:       593 failed, 17 skipped, 15 todo, 350 passed, 975 total
Snapshots:   0 total
Time:        520.946s
Ran all test suites matching /test/i.
Teardown in 0 ms
error Command failed with exit code 1.
```

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

ad9723274e0b36d73246940ff79564ad437b30451318209dc498be78242cef27 ./RariGovernanceToken.sol

a7dbf3def46c1194f1960e39abea203e19d6fff5919a7e93ae33b719618ee6fa ./CurveLpTokenPriceOracle.sol

c01487f667eeda37785e5030a1e65cb4c6d913207fce6c4d06196be6139595d0 ./MasterPriceOracle.sol

1b5a96e915c634964ced45f4c213312d8006c51a6087c3b29608112165ba019e ./UniswapTwapPriceOracleRoot.sol

239c5462e6ead40fc942df6e46c8125a7e75b41eea8dbc82a5d395b2d49eb1df ./FixedEurPriceOracle.sol

c3a71b3bf7eeb941f27fb98faa5bc686847b0d0da231f8b707ea674f3e4fb034 ./UniswapV3TwapPriceOracle.sol

c39deeb9f75de5c0864db48025ff1b8acb874713727c229cbd43913f3776d8b6 ./FixedEthPriceOracle.sol

b9240f57fe03cd518467fb262c2182e77054dfe546160971e7d5c3a8870358d5 ./UniswapTwapPriceOracle.sol

892b37cd66703e7c7065e02660dd986b3ab94e928f8ccb8cdd94e8f37ea84021 ./ChainlinkPriceOracleV2.sol

40935179c6d3cc817a957008046f30a1ed09c9168d80ccdef5f7760d212bcdee ./CurveLiquidityGaugeV2PriceOracle.sol

a1d9deec6baf200cb9eeb0aeb4762c0c56eee6866a66a4095695eea5ce1230b5 ./YVaultV2PriceOracle.sol

```
fa1a7531fbf57e1b8f371335bbe1122e07b28378a8c59d82c50ae04f6d48e44b ./BasePriceOracle.sol
4fd31e5530a539993018600d1315ce0366a6200be2ff8d1cfe72f29cc109fbf5 ./ChainlinkPriceOracle.sol
c4ff8bb255b4d04d585754a0a62ac3c6c6975ddaba0c1034911688f91ca4191f ./CErc20.sol
0dd81e22b735a74b47703f978ed4feb784d8522d8d4e7a9d574a999f53c2c261 ./Unitroller.sol
1e3a4b4f70dfe09d3ea6851bc8e95f3cffff89aa70f8446f5434ac5e560d8ab8 ./CEther.sol
ede989368a74111d391b0e9b3e8053167ca8f06917015d17d5f8fa2b6f6fce5e ./CToken.sol
bda31b1dc2fe2f3fb2612a68eeef49e1e00a2d715a7c92fd0fe1846f67e2cfa3 ./PriceOracle.sol
b94fea41e17e1fe4dc9a38e5524cd3fd0b9a5eccc59dc0773ee8bc842cc2d742 ./Comptroller.sol
1d082dfdb3a82eb4f329197c624201b1e161d98afcdb7976728ee0238fbadde9 ./IVault.sol
5a42940277a465415dd1d1fab96006fbb21ed7a11f2d45b7468015ad2fa007a6 ./IVaultV2.sol
4b490bb75ecb852c59f6594624867a58aecb46e151cf0aa41bc53e6a065b70e9 ./IWETH.sol
316511b3e97fb070127ba1134eb74dbe102f0b2f38bfa6780fcb8137ebac775a ./IUniswapV2Router01.sol
56aaf53db3510abe90b2ae23a9700fff4aa6dc0ea25fc955dc2a9e4f06df6419 ./IUniswapV2Callee.sol
05f6d191eddeb41ec270fc67b9843c30f2b0c2523245505b88124d538ea95e51 ./IUniswapV2Pair.sol
bceb67eab18ab598f0b28a73b19ad2b06707e68d4aa54fc154e053230de5077e ./IUniswapV2Factory.sol
ff62055e54da18676eb1348d7bbf12a374132297d015655c1ad105312ef89372 ./IUniswapV2Router02.sol
4f1738b4c778c91164030330831271e01447413ad0a49b50fe7bcd931b20be46 ./UniswapV2Library.sol
e561bf8403fcae964b5d58b105c7a604ab5ceea9eccef009c33114704b4736d7 ./AggregatorV3Interface.sol
8bc794c78ed1dc4da37307a8ea83069c65620737c374797497dffdd597ad2af6 ./ICurveLiquidityGaugeV2.sol
968a364928ecfcaa8f6d9f373779d5f019b7975c47815db1c2a791edcb0abbb6 ./ICurvePool.sol
419c0c645fe23a1c5d72548ce93e8d246498aa96dab6bfca287a32b5e58caf13 ./ICurveRegistry.sol
8bf61c84b872ead30d77a98c511ee1e71790772d13df75109d118a8c8f49a54f ./contracts/CEtherImmutable.sol
daebe63435b50a636f65496d286461820909a3bc895166c70c49f775554c465b ./contracts/SimplePriceOracle.sol
32f9252032165bfe274fe16f0d74b3f7add6a037b7183dc964bcf01d0a5e687c ./contracts/Maximillion.sol
204a19fb7a661c5bafcd5f7916254a457ca1fd9104e5708a73dd5010b11353dc ./contracts/SafeMath.sol
46c234fd4db0e0df6357e1496ddb133339e9c299d65a01efd5369bf58bb10456 ./contracts/CErc20.sol
a1a9e8b78d5aacdab7b53e3a5f9ea6050d87f224a5538212abb5c941d9bcc0f0 ./contracts/Unitroller.sol
8be0794fae3f3b1b50dcccb0ec7ade434d172725f50d494b272b179fe2990ee8 ./contracts/CEther.sol
7640a53ea1a186b2fb7748175d9d78a6db16c365c25a5a2019bfbe3107f8702e ./contracts/IFuseFeeDistributor.sol
cbe3decf83d6d3649271438102e64ca68ff1c708294d2077a7ea58915ebfc667 ./contracts/Exponential.sol
7d992de9a0711d9cc0a0c3d4b301377b339f1146ac6f37ea1609b34c7d0882c5 ./contracts/InterestRateModel.sol
43ba81257dcec3fe866e6cb57bb4bf9f0417e5e927c8c6356ba951eb9eda5546 ./contracts/CErc20Delegator.sol
57a63dcf508e5ba6d1c18abd7961028e9e676283404806288d42dd98d4987f2c ./contracts/CToken.sol
f8d86756385ad250677ffac757ce31a34622af2c96e36401c8c3f48d06e95002 ./contracts/CDaiDelegate.sol
7bbb9d332700f7d8196d791533dfe49f60af455cf461d326188ca34de20d2e12 ./contracts/CEtherDelegate.sol
36a81d9c51869682d7428c80357b0bd5ce9c41abb5ca51015f115fe33ae3a0e1 ./contracts/JumpRateModel.sol
918d5790253d16e1b5221918d040399ad3598aec848b6a9007428965fe57e058 ./contracts/EIP20NonStandardInterface.sol
00ef8af0928c0c886a231a4880d2d9cec71fdf7cd2c471a500a445b50cbb5579 ./contracts/ComptrollerStorage.sol
fb6745aa44143601ca42c5e43a0ad490e548f213635003c6e4b55bee6ca06a17 ./contracts/ComptrollerG1.sol
38f35ebb398e0c7d822068135f9b57898d1b5186cf9dac9b20adcaaaca7def57 ./contracts/CTokenInterfaces.sol
ad45f080f43bbff44472707cb981b6c2a95efd7424238ea733614221d8ca5790 ./contracts/CErc20Delegate.sol
8a5a574ee7b71ab417d5065cff4759ea32ce5c15f65e6e70fcbdd9a41d19c153 ./contracts/PriceOracle.sol
ad8716c2277b1ef11b7ba767686816b8eb64d395aaed817faf7bc576467cae66 ./contracts/DAIInterestRateModelV2.sol
dcb5b6857f6455d1daf77feb84a4cd11d3fb191fbc8097315479e88308f89083 ./contracts/CarefulMath.sol
ea4204fc8c5c72a5f4984177c209a16be5d538f1a3ee826744c901c21d27e382 ./contracts/Timelock.sol
b5d06e0d725b01ecb8d0b88aa89300ddc0399904d84915a311f42f96970ba997 ./contracts/WhitePaperInterestRateModel.sol
6c10018dc43041506036e90515603f81835b37be2d437e9d836219475c90da9c ./contracts/CEtherDelegator.sol
ea53516a5c69882b8c74361c12c3ead2b467cb9604642a3d370858a0ff564516 ./contracts/ErrorReporter.sol
1ee06ec83b881d3027aeb35c81da75c577964f41fb963ec9cf3fac25afc4004e ./contracts/Comptroller.sol
bc2ecd2927c202aab91222af287c07503cb348d8a96da3d368f195648356c4b7 ./contracts/EIP20Interface.sol
afaa6b004044d9c0f18104ec84bb4bd30af36f4045ad95816d61f517abf2c428 ./contracts/CErc20Immutable.sol
740241b3304332bd2329f10d691b165acea3170ff333245c0fae3727da0bd134 ./contracts/ComptrollerInterface.sol
ec42e688c7e46c4b20c0a4cb3774ad1a1ace29d12cffb777e2e5972a6afabea5 ./contracts/Lens/CompoundLens.sol
874013f6c87f2b0bf0a5d81a57fdd298ec191686cb6eed4c8498f402ef3597e6 ./contracts/Governance/Comp.sol
8a0553ad8bd250fc18710315dee64e3425550589c6466c01c3227fd8c7b3f1d4 ./contracts/Governance/GovernorAlpha.sol
```

Tests

```
19dda8605a559d42ee39f9157edf3692c7e69a3cc865c322718f5d38e78a847c ./tests/PriceOracleProxyTest.js
4881988d8aecdd723aec711d7a0c491108cac041438827118d2df9d9406054f9 ./tests/gasProfiler.js
a7376686eb77c45f312433c8f9cd35a0a91f61b5fff71c915f018c41b3eb8a39 ./tests/TimelockTest.js
4afc7ad52ed18baf2f66194ed483717f4401b076f3da64662726cd19abb6a92b ./tests/Scenario.js
```

```
ef6b1a22aca7c79d9bbe28e11a488d90712d8f570acddd90faaaa760c4f34b16 ./tests/Errors.js
5358fa45a77b2597d46448b7aecc96de55894ba08c6602ced648bf7a0b7c1fd5 ./tests/Jest.js
cb9ee641b3aa7df9e7f188c17b71b0b97f387c166915408bf09b4d0ff932c62a ./tests/CompilerTest.js
195e04575a62b67b0122ea8936b54dec20353e003737acf931cd1db3dfb6ee14 ./tests/MaximillionTest.js
e743152d69acebc103976cbcc5308e2c4b04dc88b0aa9758042f622e6b04895c ./tests/Matchers.js
0a0a31d16c3b086e44cdbc6293fe647f72ab6d04513b3ff3eeea610f30426676 ./tests/SpinaramaTest.js
e9ea8a272199c7aae90a501f2ab5a644d9d28f93964c50b9120f20dce3fcea18 ./tests/Lens/CompoundLensTest.js
2f4dbcc4fe47083cff4db7c60220550b063b258346e77075a26fea1435bbd3bc ./tests/Contracts/MockMCD.sol
b2ecb6ed9cb46b1813e86b45bfda3b15a715fa4c05ae9db7df38d83a777b8126 ./tests/Contracts/FalseMarker.sol
cf43a610e04d279dfffad601eeb48b4006d545410e20f08be012654142797f00 ./tests/Contracts/TetherInterface.sol
176d795f35868f6c3df6800a6ebfa3589e03a7fa577efc11d123bdb5ca58fab7 ./tests/Contracts/FeeToken.sol
ad06e924f41f58b111ab344170a8b16be0438f09af12c7722f8304e15d103ab2 ./tests/Contracts/CErc20Harness.sol
349649b88d6e9f805a384a8d045a269a582d5cce165b67c6b6faff159cbb91a1 ./tests/Contracts/ComptrollerScenarioG1.sol
0d7fd9df64cf72889d6ac97afd3258167116518748488e997505f27cc16b4fe6 ./tests/Contracts/MathHelpers.sol
d4fe8238e018dc1299366e0a5b8f1499e01ce10f0d39dffe2d000a8729433b60 ./tests/Contracts/TimelockHarness.sol
7e10baf5e8ab1793e452a9d28a3052534b47972c1c31a33939e36aa84301ea7d ./tests/Contracts/EvilToken.sol
34eaaa9e85252b43034072160b7cc4452a08ca3b4a9c3bd28cda689be83bff0b ./tests/Contracts/ERC20.sol
dfe52a0a041631f00e3851a90307683cf50a93e6a97e9e9d8eef1ef0dd741264 ./tests/Contracts/FixedPriceOracle.sol
9e86b10a2659f302d1643e1cd2c492c698b33e97e166e0ce647da492da5b614d ./tests/Contracts/Counter.sol
d2056385754d16486ed601ee4f1af940349a88bb7dfd660859786fcbf919571c ./tests/Contracts/ComptrollerHarness.sol
3cc11b832ed5b3e5c18e01b21fb86fa0f37badd626364933b62640c3aff7a685 ./tests/Contracts/WBTC.sol
5dabf4413d579426e299886b7124e6bf5c415a1fd8fc6d3322c8af0c3d49a532 ./tests/Contracts/CompHarness.sol
4e85b16aaa42a85cfeff0894ed7b00ead01cfdc5d42dde1a9251f638208e9234 ./tests/Contracts/GovernorAlphaHarness.sol
fdf2f2ea8ae514125babb2484d04fcbd4773127698bcf254eaa58bde65ac2ace ./tests/Contracts/CEtherHarness.sol
5288acf7cb76e1b86658fa7b7812b118fb405700543fd43d31d0431029b7e688 ./tests/Contracts/FaucetToken.sol
a3c8ad4dbbb5bd58806b0e1285fe8c9319d9c8fb4dfaed3d862a35647b1cc159 ./tests/Contracts/InterestRateModelHarness.sol
bf84c0e16a80947ad63f6dfa9e973f9b47437c1758450d45570a14af4c2b085c ./tests/Contracts/Const.sol
10144c7d50d2679e2f4ea63df2ed58ec14f22e8e09d77d15473a55f8e3f58d5e ./tests/Contracts/Structs.sol
0265281eba9108e02e7263c4d5514884696aea51688f51d5f2e4e2a819edc7f3 ./tests/Utils/Compound.js
760666fd6801178144a7e2e5ee4fcdf761e63ab1d4dad5d3f483f3eea004ba94 ./tests/Utils/InfuraProxy.js
a3421ed1eb4b1cd2613ee3c02d7953b84425f8760d6f4423ff0e7776cf3bbb64 ./tests/Utils/Ethereum.js
17f1dae75f61ebf222ffab3ff97df7a0a42740dd7513e75dd8cb41cdb561c001 ./tests/Utils/JS.js
27fe3919f7c3bc28e1822aa1f0ccdf750285abf813d1dee490c35137047ffdaa ./tests/Utils/EIP712.js
c0ef9125ef417a1216d648e9ae546f412c980ac1ef1de7d2c164b5a2aaa40eb9 ./tests/Governance/CompTest.js
2a481672769902fc25ebc4d58c9d58917155f4e92ff56543280f8114884fb7b9 ./tests/Governance/CompScenarioTest.js
b220d6f0047d78cd420176a98763fed8160cf7a0e877a50b14e08a5da4adc84c ./tests/Governance/GovernorAlpha/StateTest.js
5f5972390f0f1666982ff55ff56799b52748e0e1132805a2f37a904396b27fe3 ./tests/Governance/GovernorAlpha/QueueTest.js
45f10e9446c8d68eead1fc509a220fa0dc854f0d4d24d2fef972bbebe74a64f2 ./tests/Governance/GovernorAlpha/ProposeTest.js
10bd124f58ad69ba89f228fa77306e2df3f9435717d0d112ff120e10bb9b38a7 ./tests/Governance/GovernorAlpha/CastVoteTest.js
10a0f7464875a618ef12acde3fdfd23d4dc50f0e719725d11dc0931f80808ae8 ./tests/Tokens/adminTest.js
f06a70fb618081fdac17c57602d3b123e5c4947611104f5b854be243e3a22882 ./tests/Tokens/adminFeesTest.js
4f4326a42de75cb73f0b3c38f1717d2824f032070ffaff4a34b8458cdd7da5a8 ./tests/Tokens/mintAndRedeemTest.js
3c6dc5c2e501fa2d89e098e5a895362dfdb2623f338121216cbca8b43ebc9e76 ./tests/Tokens/setInterestRateModelTest.js
db2ea3dde6edca6e0a271809c597cc8b92053cf04a5dab620a2e573e894484e0 ./tests/Tokens/borrowAndRepayTest.js
4ae356b56c2cd9d0c734ddfd3b60bc4f7c009359141c736fef084828873293df ./tests/Tokens/accrueInterestTest.js
1e557f4e0f005d3c22d057114a4b137d293ea773a2883e8e1cf14e5c6194ea7f ./tests/Tokens/mintAndRedeemCEtherTest.js
64b86160333767ebaa9511c88d07f35408728331be81e1ed8d5ec653cb2ee9c2 ./tests/Tokens/borrowAndRepayCEtherTest.js
742d4bb068a84c956bc1c4e5c602062dcd4bbb9871669f656b844c01acfa2c5e ./tests/Tokens/fuseFeesTest.js
eea8a7385a58f55599669f4df859457547ea6aebafeca0bd697cd16c2e77adbb ./tests/Tokens/safeTokenTest.js
337c0b27103f616b43b9bff42f0f92de07e12124670c664e760fdbdd6f1b1f30 ./tests/Tokens/transferTest.js
4e4f84f9360267f5382270f21a5966bb54c2c06508db5fdcb94bd955cde6f7e9 ./tests/Tokens/reservesTest.js
3b0ff7932b35128ecf2c004bf7c7e702289f79d23f35c66fa534362b93b41b34 ./tests/Tokens/cTokenTest.js
fbf1f252d25f3de7999bc383d1f675fbebf99d53ee87e81f68d23eb1ec85c2ee ./tests/Tokens/liquidateTest.js
41e42b91f2676480badf3bcafdbb0a8ed5f24a7f22c3f30fe0982d0d5f038377 ./tests/Tokens/setComptrollerTest.js
8df8bc4353c4eefe0951f932488ff8fd685b08768ae5632b8ab044c1ceea1f52 ./tests/Models/InterestRateModelTest.js
39be23e87a13f8358879af1b0bb9e943c35ab8af939382e1b09e4c2567ca35f5 ./tests/Models/DAIInterestRateModelTest.js
4dd916fd1ede7837ec238cb592fb4ae905a95c103c39168e7e5bce1ed8eb3923 ./tests/Comptroller/adminTest.js
b04db2d2aea981533e510fbafd634d764ad6a9fbe7909da21849a1d33af6355f ./tests/Comptroller/accountLiquidityTest.js
35cbb19deef587b6baa79954d0d76a297493061310f79cc6f72f9431224a3ec5 ./tests/Comptroller/comptrollerTest.js
ff2f54a1aced42cee680115711e86a2649af95c7484c4ee38a50298cb827b5c4 ./tests/Comptroller/proxiedComptrollerV1Test.js
4b93e830dee7d9034e6b4e6204081b932a542a06431e4d26abf44f07b8de1e95 ./tests/Comptroller/unitrollerTest.js
```

```
4b9712da45967d30094d62edc395b96324172b63d623e6d4649ef34679e4663f ./tests/Comptroller/liquidateCalculateAmountSeizeTest.js
7fedc5fe287daf65eedaf2b9fe4cd90c29441a12b5e3032a5bfc709972de4757 ./tests/Comptroller/assetsListTest.js
e4960aae37d36d52fd26a67f6f553e8f825da3a4e9e29fb7a9ae8429cc463a60 ./tests/Comptroller/pauseGuardianTest.js
```

Changelog

- 2021-07-02 - Initial report
- 2021-07-22 - reaudit update

About Quantstamp

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

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

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

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

Timeliness of content

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

Notice of confidentiality

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

Links to other websites

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

Disclaimer

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