Quantstamp Security Assessment Certificate

August 16th 2021 — Quantstamp Verified

Ideamarket Arbitrum Migration

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

Executive Summary

Type	Social Tokens
Auditors	Jose Ignacio Orlicki, Senior Engineer Poming Lee, Research Engineer Kacper Bąk, Senior Research Engineer
Timeline	2021-07-05 through 2021-08-16
EVM	Berlin
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Ideamarkets Docs/Whitepaper
Documentation Quality	High
Test Quality	High

Source Code

Repository	Commit
ideamarket-contracts	396b719
ideamarket-contracts	de9e5a5

Total Issues	7 (3 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	2 (1 Resolved)
Low Risk Issues	4 (1 Resolved)
Informational Risk Issues	1 (1 Resolved)
Undetermined Risk Issues	0 (0 Resolved)

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

Summary of Findings

We have reviewed the code, documentation, and test suite and found several issues of various severities. Overall, we consider the code to be well-written and with sufficient documentation and an almost excellent test suite. Currently, the test suite is in an almost perfect shape, only 3 tests (from 428) are failing but the code coverage can be improved for the critical `evm/bridge` contracts. We have outlined suggestions to better follow best practices, and recommend addressing all the findings to tighten the contracts for future deployments or contract updates. We also provide suggestions for improvements to follow the best practices. We recommend addressing all the **7** findings to harden the contracts for future deployments or contract updates. We recommend against deploying the code as-is.

2021-08-16 update: during this reaudit, the admin team has either brought all the status of findings into fixed or acknowledged.

ID	Description	Severity	Status
QSP-1	Migration Might Lead to Funds Locked	^ Medium	Acknowledged
QSP-2	Return Value of `transfer()` Is Unchecked	^ Medium	Fixed
QSP-3	Unprotected Function `initializeStateTransfer()`	v Low	Fixed
QSP-4	`BridgeAVM` Might Be Front-run On Initialization	v Low	Acknowledged
QSP-5	Privileged Roles and Ownership	v Low	Acknowledged
QSP-6	External Dependencies	v Low	Acknowledged
QSP-7	Unnecessary `ABIEncoderV2` Pragma	○ Informational	Fixed

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 v0.7.0
- Mythril v0.22.16

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 Migration Might Lead to Funds Locked

Severity: *Medium Risk*

Status: Acknowledged

File(s) affected: `contracts/evm/bridge/IdeaTokenExchangeStateTransfer.sol`

Description: During migration, contracts are replaced with state transfer version (from L1 to L2), and contracts on L1 are disabled of their traditional functionality. As seen on migration steps *"IdeaTokenExchangeStateTransfer.setTokenTransferEnabled is called on L1 which finally allows user to migrate their IdeaTokens to L2 using IdeaTokenExchangeStateTransfer.transferIdeaTokens*". Also, migration to L2 is optional for user accounts. Then if a user does not want to (or cannot) migrate to L2, the user cannot sell it Ideamarket token on L1 because the functionality has been disabled.

Recommendation: Consider leaving functionality to sell tokens on L1 during the migration, or mitigate this behavior with documentation.

Update: 2021-08-16 update: The admin team stated that "IdeaTokens not being sellable on L1 anymore once the migration has started is per design, since during the migration all Dai managed by the Ideamarket contracts will be transferred to Arbitrum L2 by using the token bridge. Ideamarket users will be notified of the upcoming migration in due time, leaving them enough time to react and sell on L1 should they for some reason not be able to use Arbitrum. After the migration has completed users can transfer their L1 IdeaTokens to L2."

QSP-2 Return Value of `transfer()` Is Unchecked

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `BridgeAVM.sol`

Description: On L185 there is an unchecked return value for function `transfer()`. This is not safe as this function can fail sometimes.

Recommendation: Wrap in a `require()` statement to revert under this condition.

QSP-3 Unprotected Function `initializeStateTransfer()`

Severity: *Low Risk*

Status: Fixed

File(s) affected: `contracts\avm\bridge\InterestManagerStateTransferAVM.sol`

Description: There is no permission check implemented in the function `initializeStateTransfer()`. And by calling this function, an attacker can make themself the owner of the contract. The attacker can drain the contract after becoming the `owner` of the contract.

Recommendation: Add a permission check to the function `initializeStateTransfer()`.

QSP-4 `BridgeAVM` Might Be Front-run On Initialization

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `contracts/avm/bridge/BridgeAVM.sol`

Description: On the migration process steps, `BridgeAVM` is described as first being deployed and the latter initialized on another future step. If the initialization is not done atomically on the same L2 transaction then the `initialize()` can be front-ran and executed by anyone. This is a race condition situation that can lead to temporary denial-of-service.

Recommendation: Make sure Steps 1-3 of migration are executed at the same time atomically in a single transaction, so they cannot be front-ran.

Update: 2021-08-16 update: The admin team stated that "If during migration steps 1-3 the initialization was to be frontrun, which will be checked during the process, the migration can simply be restarted from step 1 again, as up to this point no state changing methods have been executed on L1."

QSP-5 Privileged Roles and Ownership

Severity: *Low Risk*

Status: Acknowledged

Description: Smart contracts will often have `owner` variables to designate the person with special privileges to make modifications to the smart contract.

Recommendation: This centralization of power needs to be made clear to the users, especially depending on the level of privilege the contract allows to the owner.

Update: 2021-08-16 update: The admin team stated that "The contract system has been designed with upgradeability in mind. All changes made to the system, including contract code changes, need to go through the Timelock (DSPause) which assures that upcoming changes are publicly visible as queued on-chain for a certain time until they can be executed. Additionally, the access to the Timelock is protected by a 2-of-2 Gnosis Safe Multisig controlled by the Ideamarket team."

QSP-6 External Dependencies

Severity: *Low Risk*

Status: Acknowledged

Description: Contracts rely on external protocols such as DAI Token, which may be vulnerable to flash loan attacks, market manipulation, etc.

Recommendation: We recommend documenting the assumptions and relying on previously verified external code such as DAI token in order to avoid unexpected behaviors and errors. The implementation of external tokens was not subject of the audit, however, Quantstamp urges to be cautious about these external dependencies and possible integrations with external platforms as it could potentially expose the platform to flash loan attacks.

Update: 2021-08-16 update: The admin team stated that "We believe our external dependencies such as Dai, Uniswap and Compound to be well established and tested."

QSP-7 Unnecessary `ABIEncoderV2` Pragma

Severity: Informational

Status: Fixed

Description: The pragma is present in a bunch of files although it appears to be unused.

Recommendation: Remove this pragma or document why is specifically needed.

Automated Analyses

Slither

Slither has detected many results out of which the majority have been filtered out as false positives and the rest have been integrated into the findings from this report.

Mythril

Mythril has detected many results out of which the majority have been filtered out as false positives and the rest have been integrated into the findings from this report.

Code Documentation

1. [fixed] `uint gasLimit, uint maxSubmissionCost` are not described in natspec of `InterestManagerCompoundStateTransfer.executeStateTransfer()`.

Adherence to Best Practices

1. Declare function `IdeaTokenExchange.getTradingFeePayable()` as external, as is never used internally.
2. On L131 of `IdeaTokenExchange.sellTokens()` (and `buyTokens()`) use `memory` instead of `storage`, to avoid code mainteinance issues in the future that face unexpected values in persistant storage variables.

Test Results

Test Suite Results

Only 2 tests failed from a total of 428 tests.

```
root@62cee0bd2f06:/tmp/ideamarket-contracts-de9e5a53e683d8cbcd30f3ad951a50ecfc4232b3# npx hardhat test
Downloading compiler 0.6.9
Compiling 89 files with 0.6.9
contracts/shared/timelock/DSPause.sol: Warning: SPDX license identifier not provided in source file. Before publishing, consider adding a comment containing "SPDX-License-Identifier:
<SPDX-License>" to each
 source file. Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code. Please see https://spdx.org for more information.

contracts/shared/timelock/DSPauseProxy.sol: Warning: SPDX license identifier not provided in source file. Before publishing, consider adding a comment containing "SPDX-License-
Identifier: <SPDX-License>" to
 each source file. Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code. Please see https://spdx.org for more information.

contracts/shared/timelock/DSPause.sol:91:5: Warning: Variable is shadowed in inline assembly by an instruction of the same name
    function add(uint x, uint y) internal pure returns (uint z) {
    ^ (Relevant source part starts here and spans across multiple lines).

Compilation finished successfully


  avm/core/BridgeAVM
     ✓ can receive static vars
     ✓ fail cannot receive static vars twice (63ms)
     ✓ fail user cannot set static vars
     ✓ can receive platform vars
     ✓ fail cannot receive platform vars twice
     ✓ fail user cannot set platform vars
     ✓ can receive token vars, set and redeem (872ms)
     ✓ fail user cannot call token function

  avm/core/IdeaTokenExchangeStateTransfer
     ✓ disabled functions revert (67ms)
     ✓ can set static vars
     ✓ fail user cannot set static vars
     ✓ can set platform vars
     ✓ fail user cannot set platform vars
     ✓ can set token vars and mint
     ✓ fail user cannot set token vars and mint

  avm/core/IdeaTokenFactoryStateTransfer
     ✓ admin is owner
     ✓ fail user cannot add market
     ✓ bridge can add token (53ms)
     ✓ fail admin cannot add token
     ✓ fail user cannot add token

  avm/core/InterestManagerStateTransfer
     ✓ admin is owner
     ✓ can invest (46ms)
     ✓ can redeem (67ms)
     ✓ owner can add to total shares
     ✓ fail user cannot add to total shares
     ✓ fail redeem not admin (68ms)

  avm/core/IdeaToken
     ✓ admin is owner
     ✓ admin can mint tokens
     ✓ admin can burn tokens
     ✓ normal user cannot mint tokens
     ✓ normal user cannot burn tokens
     ✓ user can transfer tokens (40ms)
     ✓ user can approve other user (55ms)
     ✓ user can transfer other users tokens (96ms)

  avm/core/IdeaTokenExchange
```

```
    ✓ admin is owner
    ✓ buy completely in hatch (117ms)
    ✓ buy full hatch (110ms)
    ✓ buy partially in hatch (106ms)
    ✓ buy completely outside hatch (210ms)
    ✓ sell completely in hatch (176ms)
    ✓ sell full hatch (174ms)
    ✓ sell partially in hatch (172ms)
    ✓ sell completely outside hatch (157ms)
    ✓ can fallback on buy (138ms)
    ✓ fail buy/sell - invalid token (39ms)
    ✓ fail buy/sell - max cost / minPrice (161ms)
    ✓ fail buy - not enough allowance (58ms)
    ✓ fail buy/sell - not enough tokens (417ms)
    ✓ no trading fee available (248ms)
    ✓ no platform fee available (286ms)
    ✓ no platform interest available (39ms)
    ✓ no interest available (42ms)
    ✓ fail authorize interest withdrawer not authorized
    ✓ fail authorize platform fee withdrawer not authorized
    ✓ can set factory address on init (57ms)
    ✓ fail only owner can set factory address (54ms)
    ✓ fail cannot set factory address twice (63ms)
    ✓ admin can set authorizer
    ✓ fail user cannot set authorizer
    ✓ authorizer can set interest withdrawer (251ms)
    ✓ interest withdrawer can set new interest withdrawer (260ms)
    ✓ fail authorizer cannot set interest withdrawer twice (259ms)
    ✓ admin can set interest withdrawer twice
    ✓ authorizer can set platform fee withdrawer (249ms)
    ✓ platform fee withdrawer can set new platform fee withdrawer (264ms)
    ✓ fail authorizer cannot set platform fee withdrawer twice (249ms)
    ✓ admin can set platform fee withdrawer twice
    ✓ admin can disable fees for specific token
    ✓ fail user cannot disable fees for specific token
    ✓ correct costs when buying with fee disabled (268ms)
    ✓ correct prices when selling with fee disabled (331ms)

  avm/core/IdeaTokenFactory
    ✓ admin is owner
    ✓ can add market (51ms)
    ✓ fail add market with same name (39ms)
    ✓ checks parameters when adding market
    ✓ only admin can add market
    ✓ can add token (83ms)
    ✓ fail add token with invalid name (49ms)
    ✓ fail add token with same name twice (69ms)
    ✓ fail add token invalid market (71ms)
    ✓ can set trading fee
    ✓ fail user sets trading fee
    ✓ fail set trading fee invalid market
    ✓ can set platform fee
    ✓ fail user sets platform fee
    ✓ fail set platform fee invalid market
    ✓ can set name verifier
    ✓ fail user sets name verifier
    ✓ fail set name verifier invalid market

  avm/core/IdeaTokenVault
    ✓ can lock and withdraw tokens (254ms)
    ✓ has correct locked entries (217ms)
    ✓ can lock with different durations (290ms)
    ✓ fail invalid token (104ms)
    ✓ fail invalid duration
    ✓ fail invalid amount (72ms)
    ✓ fail invalid until
    ✓ fail too early
    ✓ fail not enough allowance
    ✓ fail not enough balance

  avm/core/InterestManagerCompoundAVM
    ✓ admin is owner
    ✓ can invest (66ms)
    ✓ fail invest too few dai
    ✓ can redeem (72ms)
    ✓ fail redeem not admin (49ms)
    ✓ can withdraw COMP (63ms)

  avm/core/MultiAction
    ✓ can buy/sell tokens ETH (394ms)
    ✓ can buy/sell tokens WETH (391ms)
    ✓ can buy/sell tokens SOME (388ms)
    ✓ can buy/sell tokens 3-hop (491ms)
    ✓ can buy and fallback (174ms)
    ✓ can buy and lock ETH (194ms)
    ✓ can buy and lock DAI (151ms)
    ✓ can buy and lock DAI with fallback (150ms)
    ✓ can add and buy (153ms)
    ✓ can add and buy and lock (201ms)
    ✓ can convert add and buy (200ms)
    ✓ can convert add and buy and fallback (227ms)
    ✓ can convert add and buy and lock (233ms)
    ✓ fail buy cost too high
    ✓ fail sell price too low (225ms)
    ✓ fail directly send ETH

  avm/core/MultiActionWithoutUniswap
    ✓ can buy and lock DAI (156ms)
    ✓ can buy and lock DAI with fallback (177ms)
    ✓ can add and buy (155ms)
    ✓ can add and buy and lock (190ms)
    ✓ fail directly send ETH

  avm/nameVerifiers/DomainNoSubdomainNameVerifier
    ✓ (empty)
    ✓ test.com
    ✓ abcdefghijklmnopqrstuvwxyz_1234567-89.com
    ✓ test.com (with trailing whitespace)
    ✓ test.com (with leading whitespace)
    ✓ test.com (with leading and trailing whitespace)
    ✓ test (no dot and TLD)
    ✓ test. (no TLD)
    ✓ . (dot only)
    ✓ .com (no domain)
    ✓ test..com (double dots)
    ✓ example.test.com (subdomain)
    ✓ test!.com (invalid character)

  avm/nameVerifiers/MirrorNameVerifier
    ✓ (empty)
    ✓ vitalik
    ✓ vi-talik
    ✓ v-i-t-a-l-i-k
    ✓ Vitalik
    ✓ -vitalik
    ✓ vitalik-
    ✓ -vitalik-
    ✓ VITALIK
    ✓ 12vitalik34
    ✓ (max length)
    ✓ (too long)
    ✓ {unallowed ascii char} (682ms)
    ✓ {allowed ascii char} (101ms)

  avm/nameVerifiers/ShowtimeNameVerifier
    ✓ (empty)
    ✓ a
    ✓ A
    ✓ aa
    ✓ 0x1a1853db0905c759b28bb1d7b84cd5cbaa31794b
    ✓ abcdefghijklmnopqrstuvwxyz_
    ✓ (too long)
    ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZ
    ✓ 123456789_
    ✓ @{unallowed ascii char} (537ms)
    ✓ @{allowed ascii char} (97ms)

  avm/nameVerifiers/SubstackNameVerifier
    ✓ (empty)
    ✓ vitalik
    ✓ vi-talik
    ✓ v-i-t-a-l-i-k
    ✓ Vitalik
    ✓ -vitalik
    ✓ vitalik-
    ✓ -vitalik-
    ✓ VITALIK
    ✓ 12vitalik34
    ✓ (max length)
    ✓ (too long)
    ✓ {unallowed ascii char} (564ms)
    ✓ {allowed ascii char} (107ms)

  avm/nameVerifiers/TwitterHandleNameVerifier
    ✓ (empty)
    ✓ @jack
```

```
    ✓ @a
    ✓ @aaaaaaaaaaaaaaa
    ✓ @abcdefghijklmno
    ✓ @pqrstuvwxyz
    ✓ @ABCDEFGHIJKLMNO
    ✓ @PQRSTUVWXYZ
    ✓ @123456789_
    ✓ (empty)
    ✓ @ (@ only)
    ✓ @aaaaaaaaaaaaaaaa (17 chars)
    ✓ @{unallowed ascii char} (535ms)
    ✓ @{allowed ascii char} (92ms)

  avm/nameVerifiers/YoutubeChannelNameVerifier
    ✓ (empty)
    ✓ a
    ✓ A
    ✓ aaaaaaaaaaaaaaa
    ✓ abcdefghijklmnopqrstuvwxyzäöü
    ✓ (too long)
    ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ
    ✓ 123456789_
    ✓ @{unallowed ascii char} (527ms)
    ✓ @{allowed ascii char} (62ms)

  avm/spells/AddMarketSpell
    ✓ can add new market (92ms)

  avm/spells/ChangeLogicSpell
    ✓ can change logic (56ms)

  avm/spells/SetPlatformFeeSpell
    ✓ can set platform fee (105ms)

  avm/spells/SetPlatformOwnerSpell
    ✓ can set new platform owner

  avm/spells/SetTimelockAdminSpell
    ✓ can set new admin (52ms)

  avm/spells/SetTimelockDelaySpell
    ✓ can set new delay (42ms)

  avm/spells/SetTokenOwnerSpell
    ✓ can set new token owner

  avm/spells/SetTradingFeeSpell
    ✓ can set trading fee (94ms)

  avm/timelock/DSPause
    ✓ admin and user cannot set owner
    ✓ admin and user cannot set delay
    ✓ admin can plot and drop
    ✓ admin can plot and exec (89ms)
    ✓ user cannot plot
    ✓ user cannot drop
    ✓ user cannot exec
    ✓ cannot exec unplotted
    ✓ cannot exec premature
    ✓ cannot disregard delay

  avm/timelock/DSPauseProxy
    ✓ fail unauthorized exec
    ✓ fail delegatecall error (41ms)

  evm/bridge/IdeaTokenExchangeStateTransfer
    ✓ admin is owner
    ✓ has correct state vars (153ms)
    ✓ fail init twice
   1) fail user calls state transfer methods
   2) fail user calls token transfer before enabled
    ✓ fail init invalid args (169ms)
    ✓ disabled functions revert (56ms)

  evm/bridge/IdeaTokenFactoryStateTransfer
    ✓ disabled functions revert (51ms)

  evm/bridge/InterestManagerCompoundStateTransfer
    ✓ disabled functions revert (40ms)

  evm/core/IdeaToken
    ✓ admin is owner
    ✓ admin can mint tokens
    ✓ admin can burn tokens
    ✓ normal user cannot mint tokens
    ✓ normal user cannot burn tokens
    ✓ user can transfer tokens
    ✓ user can approve other user (43ms)
    ✓ user can transfer other users tokens

  evm/core/IdeaTokenExchange
    ✓ admin is owner
    ✓ can buy and sell 500 tokens with correct interest (701ms)
    ✓ buy completely in hatch (116ms)
    ✓ buy full hatch (115ms)
    ✓ buy partially in hatch (113ms)
    ✓ buy completely outside hatch (210ms)
    ✓ sell completely in hatch (180ms)
    ✓ sell full hatch (196ms)
    ✓ sell partially in hatch (198ms)
    ✓ sell completely outside hatch (185ms)
    ✓ can fallback on buy (127ms)
    ✓ fail buy/sell - invalid token
    ✓ fail buy/sell - max cost / minPrice (166ms)
    ✓ fail buy - not enough allowance (46ms)
    ✓ fail buy/sell - not enough tokens (169ms)
    ✓ can withdraw platform interest (262ms)
    ✓ no trading fee available
    ✓ no platform fee available
    ✓ no platform interest available (39ms)
    ✓ no interest available (41ms)
    ✓ fail authorize interest withdrawer not authorized
    ✓ fail withdraw interest not authorized
    ✓ fail withdraw platform fee not authorized
    ✓ fail withdraw platform interest not authorized
    ✓ fail authorize platform fee withdrawer not authorized
    ✓ can set factory address on init (50ms)
    ✓ fail only owner can set factory address (46ms)
    ✓ fail cannot set factory address twice (59ms)
    ✓ admin can set authorizer
    ✓ fail user cannot set authorizer
    ✓ authorizer can set interest withdrawer
    ✓ interest withdrawer can set new interest withdrawer
    ✓ fail authorizer cannot set interest withdrawer twice
    ✓ admin can set interest withdrawer twice
    ✓ authorizer can set platform fee withdrawer
    ✓ platform fee withdrawer can set new platform fee withdrawer
    ✓ fail authorizer cannot set platform fee withdrawer twice
    ✓ admin can set platform fee withdrawer twice
    ✓ admin can disable fees for specific token
    ✓ fail user cannot disable fees for specific token
    ✓ correct costs when buying with fee disabled
    ✓ correct prices when selling with fee disabled (180ms)

  evm/core/IdeaTokenFactory
    ✓ admin is owner
    ✓ can add market (56ms)
    ✓ fail add market with same name (41ms)
    ✓ checks parameters when adding market
    ✓ only admin can add market
    ✓ can add token (71ms)
    ✓ fail add token with invalid name (46ms)
    ✓ fail add token with same name twice (71ms)
    ✓ fail add token invalid market (65ms)
    ✓ can set trading fee
    ✓ fail user sets trading fee
    ✓ fail set trading fee invalid market
    ✓ can set platform fee
    ✓ fail user sets platform fee
    ✓ fail set platform fee invalid market
    ✓ can set name verifier
    ✓ fail user sets name verifier
    ✓ fail set name verifier invalid market

  evm/core/IdeaTokenVault
    ✓ can lock and withdraw tokens (261ms)
    ✓ has correct locked entries (230ms)
    ✓ can lock with different durations (222ms)
    ✓ fail invalid token (139ms)
    ✓ fail invalid duration
    ✓ fail invalid amount
    ✓ fail invalid until
    ✓ fail too early
    ✓ fail not enough allowance
    ✓ fail not enough balance
```

```
evm/core/InterestManagerCompound
   ✓ admin is owner
   ✓ can invest (56ms)
   ✓ fail invest too few dai
   ✓ can redeem (76ms)
   ✓ fail redeem not admin (82ms)
   ✓ can withdraw COMP (67ms)

evm/core/MultiAction
   ✓ can buy/sell tokens ETH (375ms)
   ✓ can buy/sell tokens WETH (398ms)
   ✓ can buy/sell tokens SOME (397ms)
   ✓ can buy/sell tokens 3-hop (498ms)
   ✓ can buy and fallback (216ms)
   ✓ can buy and lock ETH (212ms)
   ✓ can buy and lock DAI (169ms)
   ✓ can buy and lock DAI with fallback (251ms)
   ✓ can add and buy (201ms)
   ✓ can add and buy and lock (203ms)
   ✓ can convert add and buy (272ms)
   ✓ can convert add and buy and fallback (251ms)
   ✓ can convert add and buy and lock (248ms)
   ✓ fail buy cost too high
   ✓ fail sell price too low (240ms)
   ✓ fail directly send ETH

evm/nameVerifiers/DomainNoSubdomainNameVerifier
   ✓ (empty)
   ✓ test.com
   ✓ abcdefghijklmnopqrstuvwxyz_1234567-89.com
   ✓ test.com (with trailing whitespace)
   ✓ test.com (with leading whitespace)
   ✓ test.com (with leading and trailing whitespace)
   ✓ test (no dot and TLD)
   ✓ test. (no TLD)
   ✓ . (dot only)
   ✓ .com (no domain)
   ✓ test..com (double dots)
   ✓ example.test.com (subdomain)
   ✓ test!.com (invalid character)

evm/nameVerifiers/MirrorNameVerifier
   ✓ (empty)
   ✓ vitalik
   ✓ vi-talik
   ✓ v-i-t-a-l-i-k
   ✓ Vitalik
   ✓ -vitalik
   ✓ vitalik-
   ✓ -vitalik-
   ✓ VITALIK
   ✓ 12vitalik34
   ✓ (max length)
   ✓ (too long)
   ✓ {unallowed ascii char} (606ms)
   ✓ {allowed ascii char} (96ms)

evm/nameVerifiers/ShowtimeNameVerifier
   ✓ (empty)
   ✓ a
   ✓ A
   ✓ aa
   ✓ 0x1a1853db0905c759b28bb1d7b84cd5cbaa31794b
   ✓ abcdefghijklmnopqrstuvwxyz_
   ✓ (too long)
   ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZ
   ✓ 123456789_
   ✓ @{unallowed ascii char} (591ms)
   ✓ @{allowed ascii char} (93ms)

evm/nameVerifiers/SubstackNameVerifier
   ✓ (empty)
   ✓ vitalik
   ✓ vi-talik
   ✓ v-i-t-a-l-i-k
   ✓ Vitalik
   ✓ -vitalik
   ✓ vitalik-
   ✓ -vitalik-
   ✓ VITALIK
   ✓ 12vitalik34
   ✓ (max length)
   ✓ (too long)
   ✓ {unallowed ascii char} (581ms)
   ✓ {allowed ascii char} (93ms)

evm/nameVerifiers/TwitterHandleNameVerifier
   ✓ (empty)
   ✓ @jack
   ✓ @a
   ✓ @aaaaaaaaaaaaaaa
   ✓ @abcdefghijklmno
   ✓ @pqrstuvwxyz
   ✓ @ABCDEFGHIJKLMNO
   ✓ @PQRSTUVWXYZ
   ✓ @123456789_
   ✓ (empty)
   ✓ @ (@ only)
   ✓ @aaaaaaaaaaaaaaaaa (17 chars)
   ✓ @{unallowed ascii char} (536ms)
   ✓ @{allowed ascii char} (95ms)

evm/nameVerifiers/YoutubeChannelNameVerifier
   ✓ (empty)
   ✓ a
   ✓ A
   ✓ aaaaaaaaaaaaaaa
   ✓ abcdefghijklmnopqrstuvwxyzäöü
   ✓ (too long)
   ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ
   ✓ 123456789_
   ✓ @{unallowed ascii char} (513ms)
   ✓ @{allowed ascii char} (63ms)

evm/spells/AddMarketSpell
   ✓ can add new market (87ms)

evm/spells/ChangeLogicAndCallSpell
   ✓ can change logic and call (59ms)

evm/spells/ChangeLogicSpell
   ✓ can change logic (53ms)

evm/spells/SetPlatformFeeSpell
   ✓ can set platform fee (109ms)

evm/spells/SetPlatformOwnerSpell
   ✓ can set new platform owner

evm/spells/SetPlatformOwnerSpell
   ✓ can set new platform owner

evm/spells/SetTimelockAdminSpell
   ✓ can set new admin

evm/spells/SetTimelockDelaySpell
   ✓ can set new delay

evm/spells/SetTokenOwnerSpell
   ✓ can set new token owner

evm/spells/SetTradingFeeSpell
   ✓ can set trading fee (94ms)

evm/timelock/DSPause
   ✓ admin and user cannot set owner
   ✓ admin and user cannot set delay
   ✓ admin can plot and drop
   ✓ admin can plot and exec (77ms)
   ✓ user cannot plot
   ✓ user cannot drop
   ✓ user cannot exec
   ✓ cannot exec unplotted
   ✓ cannot exec premature
   ✓ cannot disregard delay

evm/timelock/DSPauseProxy
   ✓ fail unauthorized exec
   ✓ fail delegatecall error


  426 passing (2m)
  2 failing

  1) evm/bridge/IdeaTokenExchangeStateTransfer
       fail user calls state transfer methods:
     AssertionError: Expected transaction to be reverted with only-transfer-manager, but other exception was thrown: Error: missing argument: passed to contract (count=1,
expectedCount=3, code=MISSING_ARGUM
ENT, version=contracts/5.2.0)
```

```
  2) evm/bridge/IdeaTokenExchangeStateTransfer
       fail user calls token transfer before enabled:
     AssertionError: Expected transaction to be reverted with not-enabled, but other exception was thrown: Error: missing argument: passed to contract (count=4, expectedCount=6,
code=MISSING_ARGUMENT, versi
on=contracts/5.2.0)
```

Code Coverage

Code coverage reports were generated using Hardhat Coverage Plugin. We recommend improving all coverage to >80%.

426 passing (2m) 2 failing

1) evm/bridge/IdeaTokenExchangeStateTransfer fail user calls state transfer methods: AssertionError: Expected transaction to be reverted with only-transfer-manager, but other exception was thrown: Error: missing argument: passed to contract (count=1, expectedCount=3, code=MISSING_ARGUM ENT, version=contracts/5.2.0)

2) evm/bridge/IdeaTokenExchangeStateTransfer fail user calls token transfer before enabled: AssertionError: Expected transaction to be reverted with not-enabled, but other exception was thrown: Error: missing argument: passed to contract (count=4, expectedCount=6, code=MISSING_ARGUMENT, versi on=contracts/5.2.0)

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
avm/bridge/	98.78	57.89	96.15	97	
BridgeAVM.sol	100	61.54	100	100	
IdeaTokenExchangeStateTransferAVM.sol	96.15	50	90.91	92.86	134,135,137
IdeaTokenFactoryStateTransferAVM.sol	100	50	100	100	
InterestManagerStateTransferAVM.sol	100	50	100	100	
avm/bridge/interfaces/	100	100	100	100	
IArbSys.sol	100	100	100	100	
IIdeaTokenExchangeStateTransferAVM.sol	100	100	100	100	
IInterestManagerStateTransferAVM.sol	100	100	100	100	
avm/core/	94.25	74.22	98.44	94.3	
IdeaTokenExchangeAVM.sol	90.64	80	100	90.75	… 554,555,557
IdeaTokenFactoryAVM.sol	100	84.62	100	100	
InterestManagerBaseAVM.sol	96.55	75	100	96.55	102
InterestManagerCompoundAVM.sol	95.83	50	90	95.83	70
MultiActionWithoutUniswap.sol	100	61.11	100	100	
avm/core/interfaces/	100	100	100	100	
IInterestManagerBaseAVM.sol	100	100	100	100	
IInterestManagerCompoundAVM.sol	100	100	100	100	
evm/bridge/	21.74	12.5	37.93	21.94	
IdeaTokenExchangeStateTransfer.sol	13.48	15.38	24.24	14.85	… 335,339,340
IdeaTokenFactoryStateTransfer.sol	87.5	100	87.5	77.78	35,36
InterestManagerCompoundStateTransfer.sol	26.83	9.09	41.18	26.67	… 173,177,178
evm/bridge/interfaces/	100	100	100	100	
IERC20Bridge.sol	100	100	100	100	
IIdeaTokenExchangeStateTransfer.sol	100	100	100	100	
IInbox.sol	100	100	100	100	
IInterestManagerCompoundStateTransfer.sol	100	100	100	100	
evm/core/	97.67	81.37	98.11	97.68	
IdeaTokenExchange.sol	99.4	93.1	100	99.41	133
IdeaTokenFactory.sol	100	83.33	100	100	
InterestManagerCompound.sol	86.84	45	92.86	86.84	… ,99,100,101
evm/core/interfaces/	100	100	100	100	
IInterestManager.sol	100	100	100	100	
shared/bridge/	100	100	100	100	
IBridgeAVM.sol	**100**	**100**	**100**	**100**	
shared/compound/	100	100	100	100	

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
ICToken.sol	100	100	100	100	
IComptroller.sol	100	100	100	100	
shared/core/	100	81.25	100	100	
IdeaToken.sol	100	100	100	100	
IdeaTokenVault.sol	100	86.67	100	100	
MultiAction.sol	100	78	100	100	
shared/core/interfaces/	100	100	100	100	
IIdeaToken.sol	100	100	100	100	
IIdeaTokenExchange.sol	100	100	100	100	
IIdeaTokenFactory.sol	100	100	100	100	
IIdeaTokenVault.sol	100	100	100	100	
shared/core/nameVerifiers/	97.26	95	100	97.26	
DomainNoSubdomainNameVerifier.sol	100	100	100	100	
IIdeaTokenNameVerifier.sol	100	100	100	100	
MirrorNameVerifier.sol	100	100	100	100	
ShowtimeNameVerifier.sol	100	100	100	100	
SubstackNameVerifier.sol	100	100	100	100	
TwitterHandleNameVerifier.sol	90	83.33	100	90	27
YoutubeChannelNameVerifier.sol	93.33	90	100	93.33	33
shared/erc20/	81.58	50	70.59	81.58	
ERC20.sol	81.58	50	70.59	81.58	… 183,184,281
shared/proxy/	67.5	33.33	75	70.21	
AdminUpgradeabilityProxy.sol	64.71	37.5	70	70	… 70,79,80,81
IProxyAdmin.sol	100	100	100	100	
Proxy.sol	100	100	100	80	27
ProxyAdmin.sol	30	0	50	30	… 41,42,43,52
UpgradeabilityProxy.sol	100	50	100	100	
shared/spells/	100	100	100	100	
AddMarketSpell.sol	100	100	100	100	
ChangeLogicAndCallSpell.sol	100	100	100	100	
ChangeLogicSpell.sol	100	100	100	100	
SetPlatformFeeSpell.sol	100	100	100	100	
SetPlatformOwnerSpell.sol	100	100	100	100	
SetTimelockAdminSpell.sol	100	100	100	100	
SetTimelockDelaySpell.sol	100	100	100	100	
SetTokenOwnerSpell.sol	100	100	100	100	
SetTradingFeeSpell.sol	100	100	100	100	
shared/test/	51.67	28.75	57.65	53.2	
ITestUniswapV2Callee.sol	100	100	100	100	
ITestUniswapV2ERC20.sol	100	100	100	100	
ITestUniswapV2Factory.sol	100	100	100	100	
ITestUniswapV2Pair.sol	100	100	100	100	
Math.sol	66.67	25	50	75	8,21
TestCDai.sol	73.68	50	78.57	73.68	… 124,125,129
TestComptroller.sol	**100**	**100**	**100**	**100**	
TestERC20.sol	50	100	66.67	50	36

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
TestTransferHelper.sol	25	12.5	25	25	8,9,14,15,25,26
TestUniswapV2ERC20.sol	19.23	0	22.22	22.22	… 84,91,92,93
TestUniswapV2Factory.sol	70.59	30	40	72.22	21,42,43,47,48
TestUniswapV2Library.sol	90.91	40	87.5	90.91	34,35,36
TestUniswapV2Pair.sol	63.11	45.65	75	65.66	… 194,195,200
TestUniswapV2Router02.sol	26.27	8	36.36	27.73	… 332,343,353
TestWETH.sol	100	50	100	100	
UQ112x112.sol	100	100	100	100	
shared/timelock/	100	79.17	100	100	
DSPause.sol	100	75	100	100	
DSPauseProxy.sol	100	100	100	100	
IDSPause.sol	100	100	100	100	
shared/uniswap/	100	100	100	100	
IUniswapV2Factory.sol	100	100	100	100	
IUniswapV2Router01.sol	100	100	100	100	
IUniswapV2Router02.sol	100	100	100	100	
shared/util/	100	58.33	100	100	
Initializable.sol	100	50	100	100	
MinimalProxy.sol	100	50	100	100	
Ownable.sol	100	75	100	100	
shared/weth/	100	100	100	100	
IWETH.sol	100	100	100	100	
All files	**78.59**	**59.37**	**77.95**	**78.64**	

Istanbul reports written to ./coverage/ and ./coverage.json Error in plugin solidity-coverage: 😓 2 test(s) failed under coverage.

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

```
8a7931b3bac0b669ada449c60cc32ae9746d69bb93784d50d5d6f91eb5cc64f6 ./contracts/shared/weth/IWETH.sol
6e2f47ef45bd7973879b2ed989e46b4e430b6b5415a2e02005a3d5295a022936 ./contracts/shared/util/Initializable.sol
bac982496a39bffccce725750111101aea7759ae10ca9dcd7e59d32d76cd740a ./contracts/shared/util/MinimalProxy.sol
31c3612f85c6f5e47b853b29926fb39434326c67d170089e6e54abe5f3b59aab ./contracts/shared/util/Ownable.sol
b96c90a8a3f53579a41f1c7b226e9d60d1c8fe3685120244c73bb50d2112705e ./contracts/shared/uniswap/IUniswapV2Factory.sol
4906a17a33ae04d3c5e2484a2abf560757635fff6e9def01fd01325e0c56b2a5 ./contracts/shared/uniswap/IUniswapV2Router01.sol
8c46984762fe779e33aac5dcd000c49d9e1fcd06dec919bde64343a8a1c4fbc1 ./contracts/shared/uniswap/IUniswapV2Router02.sol
3933e328a83ca0ed0e1bc2ffea20452dfe788eae92495777e42f9e50060d9464 ./contracts/shared/timelock/DSPause.sol
fe233d21760315e56993d27fab5c67f2ebdb44983d9397fb470a1b9bcb566ca0 ./contracts/shared/timelock/DSPauseProxy.sol
5da80c2fcde0537585267b9a4df4c4e47266f16bc1030cf99bd0ec37c2e429c6 ./contracts/shared/timelock/IDSPause.sol
20d18e6f5bbb85e9d1704e223390f1723e77ecd1f072752b5b1d725feeaae721 ./contracts/shared/test/ITestUniswapV2Callee.sol
b48a9fa8910ba5033c1d9009e495d2955072edf4d6dd99aa3e39197eca28dbff ./contracts/shared/test/ITestUniswapV2ERC20.sol
000bdc13fce3c1482e72f287584b53edb0f2de55c53f1fa289878b27cb740b50 ./contracts/shared/test/ITestUniswapV2Factory.sol
6ca2f67c659cde24d890105a643f1abb31a5d28dca17e13bad5e1da4d0a23eb5 ./contracts/shared/test/ITestUniswapV2Pair.sol
c4b6ec5144bdb7042dfc53929f4aefbbab5221825fb84a9714f19f8a3eed7af6 ./contracts/shared/test/Math.sol
08937c2981cfb6a25bb82083b213878e926757a42485fd714897d9b7b9afbc92 ./contracts/shared/test/TestCDai.sol
589a2b44ce07337199bf31b8662c45b92874fae338767db72bb949f7a768a2bc ./contracts/shared/test/TestComptroller.sol
50fcab09ae7bfc1723c79a725fceabd7b3786db779eea8d93164fca0100ec1e8 ./contracts/shared/test/TestERC20.sol
0b9aeeec94247af2baeea176a404ef32b3de462735403e9b4cddb3ff6a7ed16d ./contracts/shared/test/TestTransferHelper.sol
3a3eb4e3d55e399db3190c838e176af392dc71288d9ac9030ff9d2c9e7b21f69 ./contracts/shared/test/TestUniswapV2ERC20.sol
```

7344a505403682368d3093dae9021d0d7fdfa4706e53f052b18a1d906f2384bf ./contracts/shared/test/TestUniswapV2Factory.sol

2f7493bc37548e31de0dcd4e5df5b53d0c1d1b7438490376a3f2f3de12d905e2 ./contracts/shared/test/TestUniswapV2Library.sol

4d0a75d92e09668fd27206df14d9dce133856562bbff006854de608c4d289c4b ./contracts/shared/test/TestUniswapV2Pair.sol

a29e0aefb63716a4243f026f96bd290748ebc4736fe94dcd76eaedd4b939ce4b ./contracts/shared/test/TestUniswapV2Router02.sol

0fe9ba5a6b91fcd999b025ec1749a4699e93fc5656570635e9507dac48f3489d ./contracts/shared/test/TestWETH.sol

b7c1ae6b7b7a0518350c70e9043550597a2cfce6db9ca868328cc1bbb2724bcf ./contracts/shared/test/UQ112x112.sol

5e516bf03c8f1175c54773eabecb66033ddd6fb49ef52a8c3db027235233ea87 ./contracts/shared/spells/AddMarketSpell.sol

2ad8def3c4b7882006bf28bd4101e976fa15b7253fca55f47915f71bec7cf41d ./contracts/shared/spells/ChangeLogicAndCallSpell.sol

a2a61726ce3e1011e76e6ac265ea64ca692036842437838eef5af9cedd4e911d ./contracts/shared/spells/ChangeLogicSpell.sol

00c5a1c124b58dca2b702ead0421e818f8b31d20f1cd40ad3eb41674b7528705 ./contracts/shared/spells/SetPlatformFeeSpell.sol

89e57d731a6dd6f44aa215b5594ef79d3858d1cd7793f0398a75d8078ee8f6a0 ./contracts/shared/spells/SetPlatformOwnerSpell.sol

c351f2e82472578fe3c8c07acab4a0a92e8ac6adec5617d629d3dcfe3991e65b ./contracts/shared/spells/SetTimelockAdminSpell.sol

7d5bc69e3f8beeb7d827877f5db87bde7deffd745120c787e187cf0b5ddc418b ./contracts/shared/spells/SetTimelockDelaySpell.sol

0218b756baf0c27802a352bfaf5f71c36a1c488dbf1376e7ba4cda15caa421f2 ./contracts/shared/spells/SetTokenOwnerSpell.sol

b8b36478d9871c06fc65aa517f385b694ca75fd26a52b003f2d01b2b9a2939e0 ./contracts/shared/spells/SetTradingFeeSpell.sol

e76389ff74c898efdc6104d7861f0a56922030cc25701292f606192d86d65e21 ./contracts/shared/proxy/AdminUpgradeabilityProxy.sol

3be53abb3e64a320572dd831e5145642f033a7b34f41d02112351d255b0e8a77 ./contracts/shared/proxy/IProxyAdmin.sol

aa5b0064faf705747aa703cccb4adb12abb1ac2f86ef21fc5dd5cca2fedda363 ./contracts/shared/proxy/Proxy.sol

665beeef4e7ac2d0a632a2917a922d2e856360b12d2e738f22c0cfabc72e93cb ./contracts/shared/proxy/ProxyAdmin.sol

7683bd187515213810770c4490201bdde9cdea0ddadd6b51079264fc6990d0a5 ./contracts/shared/proxy/UpgradeabilityProxy.sol

046bf40ac0446439f033cd6002314999910ff65a89fee8a4e38cc53a277336a3 ./contracts/shared/erc20/ERC20.sol

4e3729376c550abee152f2a2cceb4e4fc1ba7c2f8042b4a33e9866d958c19671 ./contracts/shared/core/IdeaToken.sol

7392aae47f3eedd8dda6efd8b202edbf5c7b815985e61a238009a25a4407ddc5 ./contracts/shared/core/IdeaTokenVault.sol

22cea1d06a41e8c245975da4ec807937b36b2b3cfe07ab5f24628a9e9b2b3a8e ./contracts/shared/core/MultiAction.sol

9174d91d4d07137326796d6a8b5de1ae84ab24c7f0636813bb396d018c497167 ./contracts/shared/core/nameVerifiers/DomainNoSubdomainNameVerifier.sol

895452dddb78e0cc13ecdc9964d762e27a1b441cbcdf8abc5c288d404956d36a ./contracts/shared/core/nameVerifiers/IIdeaTokenNameVerifier.sol

c55fe2165d1fbe05c17531273d83ac1cf262cf91c3d4239e3022bd782c649f1b ./contracts/shared/core/nameVerifiers/MirrorNameVerifier.sol

b94c5d3710595f0dd733c4fa3b02ea38ff7592ae3c6f385a2bca943a83a02245 ./contracts/shared/core/nameVerifiers/ShowtimeNameVerifier.sol

bad7aedaa0ae33ae5f83fd311d9484a7b06ec4376d5a70df85195b28ac28aa27 ./contracts/shared/core/nameVerifiers/SubstackNameVerifier.sol

d70f8ee076f70ebfe03491d6d322ba5a1f02ff44101df9230594f5522faaa6cf ./contracts/shared/core/nameVerifiers/TwitterHandleNameVerifier.sol

ebd830254d1a72714190c62fe284e69d2351a1899298d2457f396b3774def08b ./contracts/shared/core/nameVerifiers/YoutubeChannelNameVerifier.sol

3ee96d7a586bcdd01e6aaf7c1ef5a877dcb2f029f96eea10dc892a9ddd5b59b6 ./contracts/shared/core/interfaces/IIdeaToken.sol

2a3295cc1df784bd6e8f10c261312071d861edaabe0d8d78749681aada7a16b0 ./contracts/shared/core/interfaces/IIdeaTokenExchange.sol

258496e06e20576f1b2d045783a6b75eda6e99571c3ada81a695ce1ecb847bd4 ./contracts/shared/core/interfaces/IIdeaTokenFactory.sol

2703533630c850f4dd50aba2f971363dfb958e056fc7a5ea7f545f425139eb5b ./contracts/shared/core/interfaces/IIdeaTokenVault.sol

39fa9d194d73b0dd5a06f3bb17d0607ed8bd01527a691786e36abb6f6ba5a91c ./contracts/shared/compound/ICToken.sol

e829ab90a544cfbef4bee1b84c7dbb2267fba5d0676a2b3952c5fe586561f723 ./contracts/shared/compound/IComptroller.sol

61b9f7b72ade7d77122328de3e57a4d01f25eab50b5b43617c496a0a3b095a32 ./contracts/shared/bridge/IBridgeAVM.sol

eb93525e6ba2373c383252160848a5a97d9cb40ff8b646016cc199164cad5dbf ./contracts/evm/core/IdeaTokenExchange.sol

b70a590c843e2625e336002053caa15267c935662ffc00870365ec97aa77e3fa ./contracts/evm/core/IdeaTokenFactory.sol

d9fb3280d7f033704ded648504092841ae750bade4dfa70a942965abb84c1d8e ./contracts/evm/core/InterestManagerCompound.sol

903b05632edbcb346902792225315414070217ed3a417b0766b0c76828138d19 ./contracts/evm/core/interfaces/IInterestManager.sol

d10d621d1681a3aed3280b70dc896e244f0d80f62c7df0f35d56775a9e50e867 ./contracts/evm/bridge/IdeaTokenExchangeStateTransfer.sol

008eabbe2605b7e833abedcfe8d58f00c50fa89e739061e468752b5b78ec3cea ./contracts/evm/bridge/IdeaTokenFactoryStateTransfer.sol

859497aea09a3a99a5e216a5b2e4efb5490babce7bb1ebd07eb54359e0acc59e ./contracts/evm/bridge/InterestManagerCompoundStateTransfer.sol

5760b48f6d5f7fcc73dbc2bf7b247d052f2ad0f0370a3135e9889330f0ca288c ./contracts/evm/bridge/interfaces/IERC20Bridge.sol

3b73a05ec8913be1e22dece6b18b25e93d8fe8784343ff40839cf9a03be02c92 ./contracts/evm/bridge/interfaces/IIdeaTokenExchangeStateTransfer.sol

638cae2267f84259f9cb2b0a41c2e9fb4af98b87484dd48846ceccf982e59d30 ./contracts/evm/bridge/interfaces/IInbox.sol

30325871f2480fcaf6311e392a511371b0b34273ac67b9ea127e3f2a6277aaff ./contracts/evm/bridge/interfaces/IInterestManagerCompoundStateTransfer.sol

e4308c708b66706c630f43360eeb52632316f7494c5843977cd1cc13391ef598 ./contracts/avm/core/IdeaTokenExchangeAVM.sol

3fed342ce710e2e1f016d39d1942387dcb890e99630b2c73a60ec105e1abdd0c ./contracts/avm/core/IdeaTokenFactoryAVM.sol

9e6c4534f10378e6e4e65fe41d1823b9f90b363b580e6c5106029fb3b2e64f06 ./contracts/avm/core/InterestManagerBaseAVM.sol

27cf26d66c18931d66d6d4abfc45f41d18db0846f20f140febea0b3e7756e55c ./contracts/avm/core/InterestManagerCompoundAVM.sol

9f124ad22e1759e36ec2b3ecfeed9b23405867c8929e4227f1f57fd3c745582e ./contracts/avm/core/MultiActionWithoutUniswap.sol

a2cbdb684e2127db823777dbb040477bfdebd00f5640a886b884b7d66bf4273e ./contracts/avm/core/interfaces/IInterestManagerBaseAVM.sol

8ee30d941b321aeb5f59caa503ff2f16104ac3cc3ba37f33ed6f760f3fc0befc ./contracts/avm/core/interfaces/IInterestManagerCompoundAVM.sol

e21cdeb3f1e2a70201b8596c0f65fd611c19284650595f351f252e70073aa06a ./contracts/avm/bridge/BridgeAVM.sol

c20c1d5ac9a82a94ac1972cea0926ab7b56cbdae1b8ede1a8c2e40f18c06c97b ./contracts/avm/bridge/IdeaTokenExchangeStateTransferAVM.sol

56049f375308e4e61a88dcd7b348c6a63750e147bafaf4e85196526117f5151e ./contracts/avm/bridge/IdeaTokenFactoryStateTransferAVM.sol

91f36d35f37defc6db8b89a29601a40fc7bd2799ec8abba9779efcd3b258b6a5 ./contracts/avm/bridge/InterestManagerStateTransferAVM.sol

4910f2d761e8ddb23a759208ff720acbf5f62fd5c24e07a3696a0dd55d698c57 ./contracts/avm/bridge/interfaces/IArbSys.sol

8fd2cce2091e1d900c80137a81016274ea21bb5dd101d7505e8f934e8bb8469d ./contracts/avm/bridge/interfaces/IIdeaTokenExchangeStateTransferAVM.sol

e323349b0b0497d29321ac5becc25260863bc715c69965b1ac38b18c1f098f98 ./contracts/avm/bridge/interfaces/IInterestManagerStateTransferAVM.sol

Tests

9a7fef63aee2467d545b504047eba2f2aa18f55de9ce340f383495fe2978236e ./test/contracts/evm/timelock/DSPause.test.js

466176a0fa4eafb50c8849b3f53ef92a115e59bb81846de1b512113412a158c6 ./test/contracts/evm/timelock/DSPauseProxy.test.js

d555bb925455b2d2f5e1628f4b958fbe9dde60a5dc514e68b2a388e9157f04dd ./test/contracts/evm/spells/AddMarketSpell.test.js

8b34ed14f33758707dc9b40dd5e58deac6973f8b6f974d12c5021d7a2dde943f ./test/contracts/evm/spells/ChangeLogicAndCallSpell.test.js

8c69a7d04c90fb5dc82440216cfc61ccf784180c4aa70c6e3dab2e266f2c6f35 ./test/contracts/evm/spells/ChangeLogicSpell.test.js

9458183eb05da63c7ef51b5dd7cd5cbc7c9485de8cf9a5667bdf12016bc8d46d ./test/contracts/evm/spells/SetPlatformFeeSpell.test.js

5aedbc7f203c284f3ee3f84d840197f7925c01b1e8a45a80ebcf75149ba35e1e ./test/contracts/evm/spells/SetPlatformOwnerSpell.test.js

bd721a86d50562c50cc8fac62f4b9d7d2b183821732c560c34f5f98c65463041 ./test/contracts/evm/spells/SetTimelockAdminSpell.test.js

3bfe5e3328a3f45c75264894a276415883e92516f6a5f310afabc9171f50471d ./test/contracts/evm/spells/SetTimelockDelaySpell.test.js

e6f568262b8585c40471ef79f7db3b58743bea40bcb97f1268cbe2605ed94768 ./test/contracts/evm/spells/SetTokenOwnerSpell.test.js

0bcc07e13995f035075a218ba25f8c38587aa93298a012432e960e46248f4a58 ./test/contracts/evm/spells/SetTradingFeeSpell.test.js

f02d6552cef95484d6a43342b4c3dde141f8666b8fee0595482585561467712c ./test/contracts/evm/nameVerifiers/DomainNoSubdomainNameVerifier.test.js

a3d1d979b9525866e0b5515e74badfbc065d881cf5338db1dc609e22991ab075 ./test/contracts/evm/nameVerifiers/MirrorNameVerifier.test.js

b5d1138a7c6d3935afb426b2fcf59452f86b3436bce99fcc0cbf5f5eb971d016 ./test/contracts/evm/nameVerifiers/ShowtimeNameVerifier.test.js

2cab595dbcfc03b421fca91ef8386dff410d778f2f5efb78b5f611e64f188287 ./test/contracts/evm/nameVerifiers/SubstackNameVerifier.test.js

7eb1f7c08fc46b66fc75e0e22f36f1c45c95bb9f5f987032fa424e7c2a8be191 ./test/contracts/evm/nameVerifiers/TwitterHandleNameVerifier.test.js

30839e6ae3b160a6eb1efbcfb23202e8bb29de6f4dbc30f8e7ea9660bb7b35e0 ./test/contracts/evm/nameVerifiers/YoutubeChannelNameVerifier.test.js

b725774ef010a0e63f82ffca3faa4cc2a6d2c42eec369d36b787d4d548307305 ./test/contracts/evm/core/IdeaToken.test.js

4a4b2e6c752e8a4cf1e7416e06b5d1081d4739aadbedfcef4c9364d1f92e575c ./test/contracts/evm/core/IdeaTokenExchange.test.js

aec96eb63708dfc58ed69a2372e31c5dbc002e6975581ec4ebd5c6c3433aa8fe ./test/contracts/evm/core/IdeaTokenFactory.test.js

2fd0286a07d9bed120699f9f70603f0ca79c7e7f67f678710838f62c1213638a ./test/contracts/evm/core/IdeaTokenVault.test.js

8fb20175b6dce99e476fc4e39f05f1731fdb2e88c60fb79a6c4a38f60baaa0f1 ./test/contracts/evm/core/InterestManagerCompound.test.js

c2e66d53b1f26ec7463838ea6de93cc3324604ea448def3c335042ab04d58b96 ./test/contracts/evm/core/MultiAction.test.js

a3170280a7e7ff71eed13e0b5129ece34f72aab2bbc8fffc7ce0a9cfbde6ac73 ./test/contracts/evm/bridge/IdeaTokenExchangeStateTransfer.test.js

ec9104d1e235c207fa97f18033ed1eabea817eaf0ffa85216afc27405559f0f6 ./test/contracts/evm/bridge/IdeaTokenFactoryStateTransfer.test.js

bcb2543fefb202a84c0fffbf8fe0baf1c2f4dc099d8f944a9ebcf2fc345e7ecb ./test/contracts/evm/bridge/InterestManagerCompoundStateTransfer.test.js

2228f820aa531df5fcb796cee006257cd2e667e2ab5a17aa2a4951eac10f5f01 ./test/contracts/avm/timelock/DSPause.test.js

38a008a52d44bfe1e9f70c4320e38100d08fa8e9c70b8a2d1faaf04a7ecd6dd1 ./test/contracts/avm/timelock/DSPauseProxy.test.js

a69e84cbfc0c30366c5d07464becf889311c0e256df670fa744da2b29fb001c2 ./test/contracts/avm/spells/AddMarketSpell.test.js

b60a0cdc61806f7a3a8dde6a58b0e1b1f9ea267c83d35e1f547e995847734b67 ./test/contracts/avm/spells/ChangeLogicSpell.test.js

a13c14400038909eb0ae470a415dea328fea0abd8d0e919af2a7cdcdc2dd5a1c ./test/contracts/avm/spells/SetPlatformFeeSpell.test.js

21537ffd889d1107f37787ad8ca5315d7d4838a618f6b458a3af473762cb0b64 ./test/contracts/avm/spells/SetPlatformOwnerSpell.test.js

74d924d025e7ffb231fe3f33c38d179127118b391ec84640d151abf15eb27d20 ./test/contracts/avm/spells/SetTimelockAdminSpell.test.js

e2d3b0b7584379b107e5db1dac8ca3647451270ba50e63d42f6fcf1e43b5452e ./test/contracts/avm/spells/SetTimelockDelaySpell.test.js

d835c75441902c70be80181f73643974b534c5d14242a59e914aeb19fda53ca1 ./test/contracts/avm/spells/SetTokenOwnerSpell.test.js

578c289d0785689c0e671c3d257e1ea7d52559462b4b88d7fe1e29c6089f6ead ./test/contracts/avm/spells/SetTradingFeeSpell.test.js

180af4f737d3e84c60cd55239d38d55c31f1106140fc956c10ae5d3937c1b5d5 ./test/contracts/avm/nameVerifiers/DomainNoSubdomainNameVerifier.test.js

ecfafa113deba38080920c67da6e2ee2940d526c8bcd9df1d76e26b5128bb591 ./test/contracts/avm/nameVerifiers/MirrorNameVerifier.test.js

7c2645dd9cc86383caac32c4a8912bdac8ab3123f55a3bc5b100be1fb63439bd ./test/contracts/avm/nameVerifiers/ShowtimeNameVerifier.test.js

3b62e3ebbcddab05e55705b4d4b485d10d37e031e80332bbbbf81c9a4805acaf ./test/contracts/avm/nameVerifiers/SubstackNameVerifier.test.js

177a8f24e9e0bfa0ddf1460c82044000b6bfa0490ad539a1c4e876715b74cdba ./test/contracts/avm/nameVerifiers/TwitterHandleNameVerifier.test.js

bd5e50dd7dd27d285ea950b5aa5a3b54aee7ff8f6ceb92478cd8ed5774194832 ./test/contracts/avm/nameVerifiers/YoutubeChannelNameVerifier.test.js

90cab02c977c083d0246f8b6c2b8a3a7f12f62d9134e424a048a2603d5536ed4 ./test/contracts/avm/core/IdeaToken.test.js

2ad5c2b9e632031c43a35f665b5fcaad66e4ba7cd707592e00a92cabc7ba6179 ./test/contracts/avm/core/IdeaTokenExchange.test.js

2955a5eecd0aebb997f50aa75fba4731c698b20919cf6f09d900dc1484a9cce0 ./test/contracts/avm/core/IdeaTokenFactory.test.js

266d24f56daafe868512e62dedd2505bef06df99b4f124c4eef9b97929734934 ./test/contracts/avm/core/IdeaTokenVault.test.js

9be43df132947cb6cdb6164a4caddd21b1709fdd0284049d6303ee9445fdde1d ./test/contracts/avm/core/InterestManagerCompound.test.js

83eea7700518c54a7d07dfe659806158b3ecd9d90eb40917bf77434b5f600c6e ./test/contracts/avm/core/MultiAction.test.js

226cffc191ccda0ba7f36e1c351813e54aef74b7684232bb4652d3a994c77290 ./test/contracts/avm/core/MultiActionWithoutUniswap.test.js

067271befe135f817f5c38bd8dc44708eb2058c101a5dfbb0ee68055e6f9838e ./test/contracts/avm/bridge/BridgeAVM.test.js

08eeeb1e755a4fcba200511fac7ac4db7f3af4ced6d109a7e4bd411c9046c607 ./test/contracts/avm/bridge/IdeaTokenExchangeStateTransferAVM.test.js

aaeb698e506f5c2ef2f8c27e68317ca728cf76170da0fb95de7368347deed631 ./test/contracts/avm/bridge/IdeaTokenFactoryStateTransferAVM.test.js

361f883c6814b8a7ba6c62dfe14b725929fb1c05d5abc19a09298e1333b31664 ./test/contracts/avm/bridge/InterestManagerStateTransferAVM.test.js

Changelog

- 2021-07-27 - Initial report
- 2021-08-16 - Reaudit 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.

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.