Quantstamp Security Assessment Certificate

December 23rd 2021 — Quantstamp Verified

Rengo Labs

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

Executive Summary

Type	DeFi protocol
Auditors	Kacper Bąk, Senior Research Engineer Souhail Mssassi, Research Engineer
Timeline	2021-10-25 through 2021-12-15
Languages	Rust
Methods	Architecture Review, Unit Testing, Manual Review
Specification	None
Documentation Quality	Low
Test Quality	Low

Source Code

Repository	Commit
casperswap-core	3069edd
casperswap-router	9f464a6

Total Issues	**11** (10 Resolved)
High Risk Issues	**4** (4 Resolved)
Medium Risk Issues	**2** (2 Resolved)
Low Risk Issues	**3** (2 Resolved)
Informational Risk Issues	**1** (1 Resolved)
Undetermined Risk Issues	**1** (1 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 and evaluated it with respect to the following reference implementations:

1. Uniswap V2 Core,
2. Uniswap V2 Periphery, and
3. Uniswap Flash Swapper.

We have found a number of important issues which mostly caused by deviations from the original implementations. Half of the issues are of high and medium severity. Furthermore, we believe that many of the vulnerabilities could have been caught if the project was accompanied by a high quality test suite. Therefore, we recommend addressing the issues and crafting an extensive test suite with positive and negative test cases. This task should be relatively easy since all of the reimplemented contracts have proper test suites coded in Solidity.
Update: the team has addressed all the issues in the following commits: 801eaae for Uniswap V2 Core, and 237cf3f for Uniswap V2 Router.

ID	Description	Severity	Status
QSP-1	Integer Overflow / Underflow	⇈ High	Fixed
QSP-2	Unchecked Return Value	⇈ High	Fixed
QSP-3	Incorrect Check for `permissioned_pair_address`	⇈ High	Fixed
QSP-4	`remove_liquidity_cspr()` Differs from Uniswap's Implementation	⇈ High	Fixed
QSP-5	`mint_fee()` Enables Fee Only When `fee_to` Is 0x0	^ Medium	Fixed
QSP-6	`pair_for()` Does Not Sort The Tokens Before Fetching a Pair	^ Medium	Fixed
QSP-7	Allowance Double-Spend Exploit	⌄ Low	Fixed
QSP-8	Race Conditions / Front-Running	⌄ Low	Acknowledged
QSP-9	Missing Verification on Some Variables	⌄ Low	Fixed
QSP-10	`set_nonce()` Adds an Arbitrary `amount` To The Nonce	○ Informational	Fixed
QSP-11	Functions `skim()` And `sync()` Are Re-entrant	? Undetermined	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.

Findings

QSP-1 Integer Overflow / Underflow

Severity: *High Risk*

Status: Fixed

File(s) affected: `erc20/erc20/src/erc20.rs`, `wcspr/wcspr/src/wcspr.rs`, `pair/pair/src/pair.rs`, `uniswap_v2_library/uniswap_v2_library/src/uniswap_v2_library.rs`, `flash_swapper/src/flash_swapper.rs`

Description: Integer overflow/underflow occur when an integer hits its bit-size limit. Every integer has a set range; when that range is passed, the value loops back around. A clock is a good analogy: at 11:59, the minute hand goes to 0, not 60, because 59 is the largest possible minute. Integer overflow and underflow may cause many unexpected kinds of behavior and was the core reason for the `batchOverflow` attack. Here's an example with `uint8` variables, meaning unsigned integers with a range of `0..255`.

```
```
function under_over_flow() public {
    uint8 num_players = 0;
    num_players = num_players - 1; // 0 - 1 now equals 255!
    if (num_players == 255) {
        emit LogUnderflow();   // underflow occurred
    }
    uint8 jackpot = 255;
    jackpot = jackpot + 1;   // 255 + 1 now equals 0!
    if (jackpot == 0) {
        emit LogOverflow();   // overflow occurred
    }
}
```
```

Although Rust code compiled in debug mode (and ran in tests) catches the underflows and overflows, it is unclear how future-proof production code will be against these issues.
We noticed potential underflows and/or overflows in the following:

1. `erc20/erc20/src/erc20.rs` in the function `mint()`,
2. `erc20/erc20/src/erc20.rs` in the function `transfer_from()`,
3. `erc20/erc20/src/erc20.rs` in the function `make_transfer()`,
4. `wcspr/wcspr/src/wcspr.rs` in the function `mint()`,
5. `wcspr/wcspr/src/wcspr.rs` in the function `transfer_from()`,
6. `wcspr/wcspr/src/wcspr.rs` in the function `make_transfer()`,
7. `pair/pair/src/pair.rs` in the function `mint()`,
8. `pair/pair/src/pair.rs` in the function `transfer_from()`,
9. `pair/pair/src/pair.rs` in the function `make_transfer()`,
10. `uniswap_v2_library/uniswap_v2_library/src/uniswap_v2_library.rs` in the function `get_amount_out()`,
11. `uniswap_v2_library/uniswap_v2_library/src/uniswap_v2_library.rs` in the function `get_amount_in()`,
12. `flash_swapper/src/flash_swapper.rs`, lines 264, 265, 469.

Recommendation: To protect against underflows we recommend using the function `checked_sub()`. To protect against overflows we recommend using the function `checked_add()`.

Update: Fixed in 214c9cc (Uniswap v2 - Core) and in adfd626 (Uniswap v2 - Router).

QSP-2 Unchecked Return Value

Severity: *High Risk*

Status: Fixed

File(s) affected: `pair/pair/src/pair.rs`, `flash_swapper/src/flash_swapper.rs`, `uniswap_v2_router/uniswap_v2_router/src/transfer_helper.rs`, `uniswap_v2_router/uniswap_v2_router/src/uniswap_v2_router.rs`

Description: Most functions will return a `true` or `false` value upon success. Some functions, like `send()`, are more crucial to check than others. It's important to ensure that every necessary function is checked.
Specifically, the following code locations ignore return values:

1. `pair/pair/src/pair.rs`, lines 209, 222, 585, 590 ignore return values from `transfer()`, so a transfer may fail but `swap()` would still succeed,
2. `flash_swapper/src/flash_swapper.rs`, lines 301, 303, 510, 751, and 790,
3. `uniswap_v2_router/uniswap_v2_router/src/transfer_helper.rs`, line 16,
4. `uniswap_v2_router/uniswap_v2_router/src/uniswap_v2_router.rs`, lines 239 and L626.

Recommendation: Check return values and revert where necessary.

Update: Fixed in 88c77bc, f6dc7de, 706ccea (Uniswap v2 - Core) and in 5a9b158 (Uniswap v2 - Router).

QSP-3 Incorrect Check for `permissioned_pair_address`

Severity: *High Risk*

Status: Fixed

File(s) affected: `flash_swapper/src/flash_swapper.rs`

Description: The function `uniswap_v2_call()` reverts if it's called by a `permissioned_pair_address` (line 98). This is likely incorrect.

Recommendation: The function should revert if it's NOT called by `permissioned_pair_address`.

Update: Fixed in 00991ce (Uniswap v2 - Core).

QSP-4 `remove_liquidity_cspr()` Differs from Uniswap's Implementation

Severity: *High Risk*

Status: Fixed

File(s) affected: `uniswap_v2_router/uniswap_v2_router/src/uniswap_v2_router.rs`

Description: The function `remove_liquidity_cspr()` calls `transfer_from()` in L294, whereas the original Uniswap implementation calls `safeTransfer()`. Consequently, the original implementation sends tokens from the contract whereas the new implementation sends tokens from the caller.

Recommendation: Use `transfer()` instead of `transfer_from()` or explain why the implementations differ.

Update: Fixed in 5a9b158 (Uniswap v2 - Router).

QSP-5 `mint_fee()` Enables Fee Only When `fee_to` Is 0x0

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `pair/pair/src/pair.rs`

Description: It appears to be an error in implementation of `mint_fee()`; the fee would always be sent to 0x0.

Recommendation: Reverse the check so that the opposite happens, i.e., no fee if `fee_to` is 0x0, and fee otherwise.

Update: Fixed in f4e2742 (Uniswap v2 - Core).

QSP-6 `pair_for()` Does Not Sort The Tokens Before Fetching a Pair

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `uniswap_v2_library/uniswap_v2_library/src/uniswap_v2_library.rs`

Description: `pair_for()` does not sort the tokens before fetching a pair. Consequently, it may contradict the assumptions that Uniswap users may have.

Recommendation: Sort the tokens before returning a pair.

Update: Fixed in adfd626 (Uniswap v2 - Router).

QSP-7 Allowance Double-Spend Exploit

Severity: *Low Risk*

Status: Fixed

File(s) affected: `erc20/erc20/src/erc20.rs`, `wcspr/wcspr/src/wcspr.rs`, `pair/pair/src/pair.rs`

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.

Update: Fixed in 70274b8, 81e5d6e, 97508e1 (Uniswap v2 - Core).

QSP-8 Race Conditions / Front-Running

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `pair/src/pair.rs`

Description: A block is an ordered collection of transactions from all around the network. It's possible for the ordering of these transactions to manipulate the end result of a block. A producer attacker can take advantage of this by generating and moving transactions in a way that benefits themselves.
Specifically, in the `mint_fee()` function located in `pair/src/pair.rs#L657` , the `treasury_fee` is used in calculation for the liquidity, however these variable can also be changed from the `set_treasury_fee()` function which can cause a race condition and result a miscalculation in the liquidity.

Recommendation: Race condition issues are typically difficult to address and are of low severity. We describe it here mostly for informational purposes.

QSP-9 Missing Verification on Some Variables

Severity: *Low Risk*

Status: Fixed

File(s) affected: `uniswap_v2_router/src/uniswap_v2_router.rs`, `uniswap_v2_core/pair/pair.rs`

Description: Some arguments are not checked for validity:

1. in the `add_liquidity()` function located in `uniswap_v2_router/src/uniswap_v2_router.rs#L45` , the `amount_a_desired` and `amount_b_desired` variables are not verified, in fact anyone can inject these parameters with the value 0.
2. in the `add_liquidity_cspr()` function located in `uniswap_v2_router/src/uniswap_v2_router.rs#L214` , the `amount_token` is not verified, in fact anyone can inject it with the value 0.
3. in the `mint_fee()` function located in `uniswap_v2_core/pair/pair.rs#L658` , we are dividing by denominator without verifying its value thus we can divide by 0.

Recommendation: Add the required checks.

Update: Fixed in 6f09359 (Uniswap v2 - Core) and in adfd626 (Uniswap v2 - Router).

QSP-10 `set_nonce()` Adds an Arbitrary `amount` To The Nonce

Severity: *Informational*

Status: Fixed

File(s) affected: `erc20/erc20/src/erc20.rs`, `pair/pair/src/pair.rs`

Description: The function `set_nonce()`may add an arbitrary `amount` to the nonce. It is unclear why `amount` is needed and why nonce isn't simply incremented.

Recommendation: Increment the nonce instead of adding an arbitrary value or provide an explanation why the current functionality is needed.

Update: Fixed in 6f09359 (Uniswap v2 - Core).

QSP-11 Functions `skim()` And `sync()` Are Re-entrant

Severity: *Undetermined*

Status: Fixed

File(s) affected: `pair/pair/src/pair.rs`

Description: Unlike in Uniswap, both functions are re-entrant.

Recommendation: Add a mutex to protect against re-entrancy.

Update: Fixed in d14fd07 (Uniswap v2 - Core).

Adherence to Specification

Assuming that the reference implementations act as specification, the provided implementation deviates from the specification in a few key locations (as indicated in the list of vulnerabilities).

Code Documentation

The code comes with very little inline documentation. We recommend documenting the code.

Adherence to Best Practices

1. `erc20/utils/contract-utils/src/contract_context.rs#11`: magic constant. The meaning of 2 is not immediately clear.
2. A lot of code clones, e.g., `contract-utils` in multiple locations.
3. Overall, a lot of boilerplate code and clones. We recommend improving code reusability by using macros and functions.
4. `flash_swapper/src/flash_swapper.rs` 74-88 code clones.

Test Results

Test Suite Results

All tests executed successfully. We reviewed the test suite, and given a number of important issues, we recommend expanding the test suite significantly to ensure that the code works as expected. Furthermore, a good test suite would contain both positive and negative test cases.

```
running 9 tests
test erc20_tests::test_calling_construction ... ok
test erc20_tests::test_erc20_approve ... ok
test erc20_tests::test_erc20_deploy ... ok
test erc20_tests::test_erc20_burn ... ok
test erc20_tests::test_erc20_mint ... ok
test erc20_tests::test_erc20_transfer ... ok
test erc20_tests::test_erc20_transfer_from ... ok
test erc20_tests::test_erc20_transfer_from_too_much ... ok
test erc20_tests::test_erc20_transfer_with_same_sender_and_recipient ... ok
```

```
test result: ok. 9 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 11.85s

running 7 tests
test factory_tests::test_calling_construction ... ok
test factory_tests::test_factory_create_pair ... ok
test factory_tests::test_factory_deploy ... ok
test factory_tests::test_factory_set_fee_to ... ok
test factory_tests::test_factory_set_fee_to_setter ... ok
test factory_tests::test_factory_set_white_list ... ok
test factory_tests::test_factory_set_white_list_with_non_owner ... ok

test result: ok. 7 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 17.62s

running 2 tests
test flash_swapper_tests::test_flash_swapper_deploy ... ok
test flash_swapper_tests::test_calling_construction ... ok

test result: ok. 2 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 3.33s

running 15 tests
test pair_tests::test_calling_construction ... ok
test pair_tests::test_pair_approve ... ok
test pair_tests::test_pair_deploy ... ok
test pair_tests::test_pair_burn ... ok
test pair_tests::test_pair_initialize ... ok
test pair_tests::test_pair_set_treasury_fee_percent ... ok
test pair_tests::test_pair_mint ... ok
test pair_tests::test_pair_skim ... ok
test pair_tests::test_pair_swap ... ok
test pair_tests::test_pair_sync ... ok
test pair_tests::test_pair_transfer ... ok
test pair_tests::test_pair_transfer_from ... ok
test pair_tests::test_pair_transfer_from_too_much ... ok
test pair_tests::test_pair_transfer_too_much ... ok
test pair_tests::test_pair_transfer_with_same_sender_and_recipient ... ok

test result: ok. 15 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 54.62s

running 10 tests
test wcspr_tests::test_calling_construction ... ok
test wcspr_tests::test_wcspr_approve ... ok
test wcspr_tests::test_wcspr_deploy ... ok
test wcspr_tests::test_wcspr_deposit ... ok
test wcspr_tests::test_wcspr_deposit_zero_amount ... ok
test wcspr_tests::test_wcspr_transfer ... ok
test wcspr_tests::test_wcspr_transfer_from ... ok
test wcspr_tests::test_wcspr_transfer_from_too_much ... ok
test wcspr_tests::test_wcspr_transfer_too_much ... ok
test wcspr_tests::test_wcspr_withdraw ... ok

test result: ok. 10 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 10.31s

running 7 tests
test uniswap_v2_library_tests::test_library_deploy ... ok
test uniswap_v2_library_tests::quote ... ok
test uniswap_v2_library_tests::test_uniswap_get_amount_in ... ok
test uniswap_v2_library_tests::test_uniswap_get_amount_out ... ok
test uniswap_v2_library_tests::test_uniswap_get_amounts_in ... ok
test uniswap_v2_library_tests::test_uniswap_get_amounts_out ... ok
test uniswap_v2_library_tests::test_uniswap_get_reserves ... ok

test result: ok. 7 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 62.44s

running 13 tests
test uniswap_tests::add_liquidity ... ok
test uniswap_tests::add_liquidity_cspr ... ok
test uniswap_tests::remove_liquidity ... ok
test uniswap_tests::remove_liquidity_cspr ... ok
test uniswap_tests::remove_liquidity_with_permit ... ok
test uniswap_tests::remove_liquidity_cspr_with_permit ... ok
test uniswap_tests::swap_exact_cspr_for_tokens ... ok
test uniswap_tests::swap_cspr_for_exact_tokens ... ok
test uniswap_tests::swap_exact_tokens_for_cspr ... ok
test uniswap_tests::swap_exact_tokens_for_tokens ... ok
test uniswap_tests::swap_tokens_for_exact_cspr ... ok
test uniswap_tests::swap_tokens_for_exact_tokens ... ok
test uniswap_tests::test_uniswap_deploy ... ok

test result: ok. 13 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 133.25s
```

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

```
a5149e928e64e1c60b8d2280e5ef7e385ebe79dbd4d860eb1018250a81de4b55 ./transfer_helper.rs
2e9656eef68ef9e5c3ff65c6f7c69787cc174c102b04fcf90c8a3300f5fb6ad5 ./uniswap_v2_router.rs
c290e2bb651bafcac76df9f453b926121199745caef32b257da137c234e9ab0d ./config.rs
7fe7addbc2228d1a6d5f56c310ce9b3a6e4f228363953242345e300d594fd027 ./lib.rs
9694b9ef58037ff7fe57297c15e6a50f220d4955ea8c0bc9fe55fe392c677727 ./data.rs
5eda941ac56416a358948d3672cdae6a28aba56c28e604f51acac5fa4f696fc0 ./uniswap_v2_library.rs
7866c91be8c0e4742b6a11b943c396eec1851a117581a07617880f6f5c82549a ./config.rs
2376ca113557de30a76708f6ca2041431394956d0459d28c6016ffc13c2a3dd2 ./lib.rs
a78dab169d46e8cd6bd9244141fd8bc76a62ece45ba5e937eed1efccb563986e ./data.rs
3dd28bf91238c14407769c8277f4373c9a01790352832e8f3d0c2c6729af6f60 ./wcspr.rs
4feeaec232d3507c7e85cc5773fb214cd1dc9dafeff34b2ee99a8ba590f03309 ./lib.rs
f9cf55a85196c1e2a8149a1443050a9439b3208830c4a7823c1f6215b0f4c9d6 ./data.rs
efc9db18db4c5e92e9435f9cc9c423086b47525a445ff5c26ed87fd479b4b0bd ./lib.rs
86414fd7a8814e4f161185f498b3ac395ee5bf940f69de89fb0691d89ac3065f ./pair.rs
2d28055fcc9918fe23f3ed823b26a8274c905299a312ee2f7309d8cc2b7331a9 ./data.rs
530620e8495b77380947115ee139cd03297535f188867dad1a0849a0b5a80cab ./lib.rs
614e8833fb9854027325bf6ddcda043b75bea98e676d617b54e3441cad9f03f8 ./data.rs
c7a87925d4c1111cf04fbacc84b6ef9547a77832b8cfb0500f7daa3f2a1f5042 ./flash_swapper.rs
bcdba8ffe4c2d2035258f0428ea24df55ad123fccf34e504b0fa9731906cb4c0 ./factory.rs
f1b82bc5fcd9691203a9e25b17b0bba5b292d9c2414c372196086715ddff49d4 ./lib.rs
a2f4d03faf859aa916de5e0b69c5462a018cf60ea3f7615da3593bc405afbb94 ./data.rs
fb93a2da65158adeb70491ef567079783f6ab59523adf4e57cc045d563d753da ./src/lib.rs
42c51dcf980e1fddd42ed29a7c16f4c36d5834d0bd92b32ddd38fe9bb2e71e0b ./src/data.rs
```

b2c2400addf4a855663a54d5487728f9f3553be9a003351bdbe58a3b2db99237 ./src/erc20.rs

Tests

ae9c529ada29174c3ce9a186ad82b688ce8f36c2b507decd5eab77453cbccc40 ./build.rs

1bc17fbe996404962648bb4de45ce70b4906e526832449bd4a738e3160cb3d5b ./integration_tests.rs

3a62e090dfbd5bb31f262f556fde6f512195703c2f50699edb4756fb413ea73e ./mappings.rs

36175ab23f09a91f47dfd62778864c7f2df26bd4bce1ba62802d59306825a75d ./main.rs

d1e7d7708d4bfb7206038d4db3f0f6cb4b749d1f12215bb2b61776f27d9b53c0 ./uniswap_instance.rs

5e5c2e9e3f066d68170b540eeb44cc7e4ae4c16e87e3d27f587883ab4bd5c430 ./lib.rs

e811f3e60b6cf3ea41a540c198601107c83e55a37021a875e0da84b89097e432 ./uniswap_tests.rs

0ab56c216f1bdf65320ad303c16a3da7f2d096dba9ce1a95410fc7986b0437ef ./lib.rs

11f329be098cc956197c2adcd143af9788dd4d1d478d43d6489b8c42fb85c19b ./uniswap_v2_library_instance.rs

f6a3ffd7492c565b6c7b951309dde5a7d74d3e38fe1ae2b213d394aca89467fb ./uniswap_v2_library_tests.rs

66fc76f380067e29f57d23869639cf7074fa6932aa8703fe3581280561816493 ./constants.rs

fccf68a46059fe37b6f168826a7c55a62cd5927eee17d2556b55882f8b3dbf7d ./main.rs

deef9945d03d01e6a9dd7b0c16c836b71a606aa15bde6065449b498e62384add ./utils.rs

4e2eb97a15065e7ca3a01a840b38df05b01ecf1fce6ca893c8d7a1b761143583 ./constants.rs

85de47863357d781fe9882d3eea1a2115c3654a033cc24f43e0d8a680f42c3d0 ./main.rs

deef9945d03d01e6a9dd7b0c16c836b71a606aa15bde6065449b498e62384add ./utils.rs

1ea35de660f6436b3476a89932fc34d579909ca453c5864e3ca37612e1682d7e ./constants.rs

96964f78b23149af6c2cedcc554f58dededa6a8ad3ceebc19eab8bbc9c1c347b ./wcspr_tests.rs

0ef78039a9ba9d18d1c67787dcc3185e57f24345c055c022021d8a5f73e1b9f5 ./lib.rs

455763e181f38b59b97fc0ce9252a831a5cdff5852347ae6c02309f379eb3bf9 ./wcspr_instance.rs

1a64509a720581e4986d42ebec5bb60c459888736b4de2f0a854f7083cd928df ./mappings.rs

b1b5afe87e1237306e2563c45ffa722943aec00d37aea73a29def0aa7e84c950 ./main.rs

1a64509a720581e4986d42ebec5bb60c459888736b4de2f0a854f7083cd928df ./mappings.rs

b1b5afe87e1237306e2563c45ffa722943aec00d37aea73a29def0aa7e84c950 ./main.rs

5be88be35cf46d79a195156ed3d148c381c7f81071b416d4c34a67fc59da1915 ./lib.rs

6cc28f108eab9f414293b58d0e6f67032bd466eb932034b36a9c83ebf171ef8a ./pair_instance.rs

69a95bd93b73d9831b0bf9205dabd87009ec865321ce571c7488a0a949696e29 ./pair_tests.rs

ee7121b3a06ef0f31b8ed231b1eddced36a135c7f1b7802bf0bddcd42a7f7eec ./test.rs

986e393ffeb206a88eec060c1ebd256dfbf85fadb5276066af419a7c48cb19ce ./lib.rs

027d6a14f50b41a81e677731e907c5161189620618066748e51f13f37e12a1c0 ./data.rs

b37eddcdb34db6d0369cd705a88f75f21dc2e9c7183c24a388ac577d646d3d0e ./test_instance.rs

a3c6456f9a39c2b91404b43b3081847ea06aa360df26e07be58ea717e4d5f031 ./flash_swapper_tests.rs

2eb68f1351ebb1e94739b084082559c91794f438c5c42cc2aa9d8a9251e377f9 ./lib.rs

bc7ac0717e6c168248ae1ee736dda2428be128d2e73d302bae45ae33409bfaac ./flash_swapper_instance.rs

20200946ba5e1192598b89f096b4567a10c0356a648333242802862a479528ef ./factory_instance.rs

3e6c8f8592465bcb17a2b1dd42f0aaef18acb479ad662e0e2b7185b6f403fcb4 ./lib.rs

7b87784042ef2a93beb0740c037718e8c9576ca7313ba8ac071a9a6cbdfc6219 ./factory_tests.rs

cc60afa7a35c2a57926666a36c3e8023f294c52ed53f63e2e7fdac92f5df613a ./mappings.rs

a27c3420502f6588f01e24a63b3c0d2b718a30a6c0648f74bccc312359a91dea ./main.rs

cc60afa7a35c2a57926666a36c3e8023f294c52ed53f63e2e7fdac92f5df613a ./mappings.rs

a27c3420502f6588f01e24a63b3c0d2b718a30a6c0648f74bccc312359a91dea ./main.rs

f3b918e51d57e362531b9e3cf16ba8d47b76d16e98c3b06cc3ec40c667ec439a ./src/lib.rs

7624764193e906681d3abffac75c3ae12bc6896877d98e3f54ebb97b5312bb95 ./src/erc20_tests.rs

ccb19dcea87585afb78fb41ce04bad5958a3d047845539fd93528a58c6f64420 ./src/erc20_instance.rs

Changelog

- 2021-11-05 - Initial report
- 2021-12-07 - 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.