Quantstamp Security Assessment Certificate

July 30th 2021 — Quantstamp Verified

Reflexer Staking and Auction House

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

Executive Summary

Type	DeFi protocol
Auditors	Kacper Bąk, Senior Research Engineer Jose Ignacio Orlicki, Senior Engineer Mohsen Ahmadvand, Senior Research Engineer
Timeline	2021-06-29 through 2021-07-21
EVM	Muir Glacier
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	None
Documentation Quality	Low
Test Quality	High

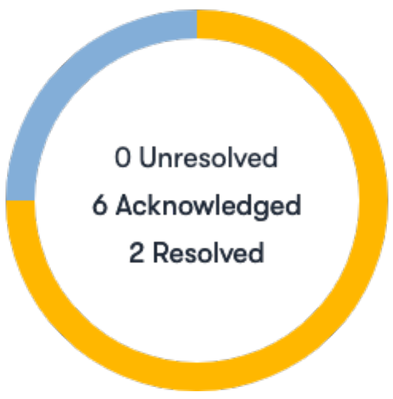
Source Code

Repository	Commit
geb-lender-first-resort	6945d87

Goals

- Can funds get locked up in the contract?
- Are computations implemented correctly?

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

In our audit, we identified 8 issues in total. One issue is deemed as high severity due to its potential impact on the user funds. The auction deadlines are susceptible to manipulations by miners, a minimum duration need to be set (informational severity). Additionally, three low severity and three undetermined issues were detected. We recommend improving the documentation. We performed a manual review of the test suite and consider it to be of good quality.

ID	Description	Severity	Status
QSP-1	Unsafe Transfers Could Lead to Fund Losses	High	Fixed
QSP-2	Privileged Roles and Ownership	Low	Acknowledged
QSP-3	Missing Input Validation	Low	Fixed
QSP-4	Can Lock Into Zero Authorized Adresses	Low	Acknowledged
QSP-5	Manipulable Auction Deadlines	Informational	Acknowledged
QSP-6	`restartAuction()` Doesn't Check if the Contract Is Enabled	Undetermined	Acknowledged
QSP-7	Anyone Can Terminate Ongoing Auctions via `terminateAuctionPrematurely()`	Undetermined	Acknowledged
QSP-8	Every Exit Request Postpones the Deadline Further	Undetermined	Acknowledged

Quantstamp Audit Breakdown

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

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

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

Methodology

The Quantstamp auditing process follows a routine series of steps:

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

Toolset

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

Setup

Tool Setup:

- Slither v0.7.1

Steps taken to run the tools:

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

Findings

QSP-1 Unsafe Transfers Could Lead to Fund Losses

Severity: *High Risk*

Status: Fixed

File(s) affected: `StakedTokenAuctionHouse.sol`, `GebLenderFirstResortRewards.sol`

Description: The `StakedTokenAuctionHouse` contract uses the function `transferFrom()` in an unsafe manner since the return value is unchecked in lines 305 and 333. In case that the transfer fails the transaction proceeds assuming that the transfer went through. This could potentially lead to fund losses for the user or the contract.
The same problem materialises in the `GebLenderFirstResortRewards.sol` contract. It does not check the return value of two `transfer` calls:

- `transfer()` in `GebLenderFirstResortRewards` on L429
- `transfer()` in `GebLenderFirstResortRewards` on L473

Recommendation: The return value of `transferFrom()` calls need to be verified and if needed the transaction shall be reverted. Alternatively, consider using `safeTransferFrom()`.

QSP-2 Privileged Roles and Ownership

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `StakedTokenAuctionHouse.sol`, `GebLenderFirstResortRewards.sol`

Description: Smart contracts will often have `owner` variables or authorized accounts to designate persons 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.

QSP-3 Missing Input Validation

Severity: *Low Risk*

Status: Fixed

File(s) affected: `GebLenderFirstResortRewards.sol`, `StakedTokenAuctionHouse.sol`

Description: Arguments of type address are not checked to be non-zero in `TokenPool.constructor()`. Furthermore, the function `modifyParameters()` can potentially set invalid addresses to sensitive variables `accountingEngine` and `tokenBurner`. Also, `minBidDecrease` can be set to zero leading to `newMinBid` being always set to 1 in `restartAuction()`.

Recommendation: Add checks to verify that the input values are valid (i.e., non-zero, and the type of underlying contracts matches the expected types).

QSP-4 Can Lock Into Zero Authorized Adresses

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `StakedTokenAuctionHouse.sol`, `GebLenderFirstResortRewards.sol`

Description: In both contracts, as an authorized address can remove its own address from the `authorizedAccounts` mapping, you can get locked by mistake or malicious intention into a state with zero authorized accounts.

Recommendation: Consider disallowing an address to remove itself when calling `removeAuthorization()`. Also, you can count the number of authorized addresses and stop the self-removal of an authorized address only when it is the last authorized account (`counter == 1`).

QSP-5 Manipulable Auction Deadlines

Severity: *Informational*

Status: Acknowledged

File(s) affected: `StakedTokenAuctionHouse.sol`, `GebLenderFirstResortRewards.sol`

Description: The contract allows authorized users to change `totalAuctionLength`, which sets the deadline for auctions by adding it to the current datetime (`now`). The authorized users can set the length to an arbitrarily small value, which could potentially let short-length auctions be won by accounts benefiting the authorized users. More importantly, the datetime (`now`) can be potentially manipulated by the miners. So, every time there is a lucrative auction, miners are incentivized to supply smaller or larger values, depending on the auction state, for the datetime (`now`).

Recommendation: This deadline needs to conform to a secure minimum value (hours or days).

QSP-6 `restartAuction()` Doesn't Check if the Contract Is Enabled

Severity: *Undetermined*

Status: Acknowledged

File(s) affected: `StakedTokenAuctionHouse.sol`

Description: The function `restartAuction()` works even when the contract is not enabled (unlike other methods). Also, it can be called by anyone (no authorization checks).

Recommendation: Add the necessary checks. If this is the intended behavior, make it explicit via comments in the code.

QSP-7 Anyone Can Terminate Ongoing Auctions via `terminateAuctionPrematurely()`

Severity: *Undetermined*

Status: Acknowledged

File(s) affected: `StakedTokenAuctionHouse.sol`

Description: `terminateAuctionPrematurely()` has no authorization in place. A user can pay the fees and stop an auction by sending staked tokens to the token burner contract. This can increase the staked token value by burning a number of such tokens compensating the paid ETH value for gas.

Recommendation: Consider adding authorization to the terminate function. If this is the intended behavior, it should be made explicit by comments.

QSP-8 Every Exit Request Postpones the Deadline Further

Severity: *Undetermined*

Status: Acknowledged

File(s) affected: `GebLenderFirstResortRewards.sol`

Description: On every `requestExit` the deadline is pushed by the `exitDelay` value. Assuming an `exitDely` of 1 day, if a user submits an `exitRequest` today and another one day after, the earliest day to call `exit()` would be two days after the initial call.

Recommendation: Please explain whether this is the intended behavior. It appears that every `exitRequest()` should have its own exit deadline and be independent of future requests.

Automated Analyses

Slither

Slither did not report any significant issues.

Adherence to Specification

1. `modifyParameters(bytes32 parameter, address addr)` checks if `contractEnabled` is `true`, but `modifyParameters(bytes32 parameter, uint256 data)` does not. Why? **Update:** fixed.

Adherence to Best Practices

1. `StakedTokenAuctionHouse.totalOnAuctionDebt()` should be declared external. **Update:** fixed.

Test Results

Test Suite Results

All tests executed successfully. After manual review of the test suite, we consider it to be of good quality, however, the used testing framework is unable to report coverage in an automated way.

```
Running 21 tests for src/test/AutoRewardDripper.t.sol:AutoRewardDripperTest
[PASS] testFail_transfer_token_unauthorized() (gas: 4197)
[PASS] test_remove_authorization() (gas: 3722)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4183)
[PASS] test_transfer_token_out() (gas: 30233)
[PASS] testFail_transfer_token_null_dst() (gas: 1475)
[PASS] testFail_setup_null_token() (gas: 34807)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1534)
[PASS] test_drip_reward() (gas: 201541)
[PASS] testFail_transfer_token_null_amount() (gas: 1453)
[PASS] testFail_modify_parameters_invalid_last_block() (gas: 1550)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1513)
[PASS] testFail_add_authorization_unauthorized() (gas: 4161)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4246)
[PASS] test_correct_setup() (gas: 11515)
[PASS] test_add_authorization() (gas: 25701)
[PASS] test_modify_parameters() (gas: 40999)
[PASS] testFail_setup_null_requestor() (gas: 34879)
[PASS] testFail_modify_parameters_invalid_reward_per_block() (gas: 1502)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4260)
[PASS] testFail_setup_null_timeline() (gas: 34931)
[PASS] testFail_drip_unauthorized() (gas: 2355)

Running 41 tests for src/test/GebLenderFirstResort.t.sol:GebLenderFirstResortTest
[PASS] testFail_modify_parameters_invalid_min_tokens_to_keep() (gas: 1584)
[PASS] testFail_join_unnaproved() (gas: 11541)
[PASS] test_remove_authorization() (gas: 3767)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4207)
[PASS] testFail_setup_invalid_auctionHouse() (gas: 59995)
[PASS] testFail_modify_parameters_invalid_system_coins_to_request() (gas: 1600)
[PASS] testFail_modify_parameters_null_address() (gas: 1531)
[PASS] testFail_modify_parameters_invalid_exit_delay() (gas: 1697)
[PASS] test_join_2() (gas: 147937)
[PASS] test_request_exit() (gas: 156049)
[PASS] testFail_exit_underwater() (gas: 205198)
[PASS] testFail_modify_parameters_invalid_max_concurrent_auctions() (gas: 1648)
[PASS] testFail_exit_no_request() (gas: 136357)
[PASS] testFail_join_underwater() (gas: 52825)
[PASS] testFail_setup_invalid_minStakedTokensToKeep() (gas: 59946)
[PASS] testFail_join_invalid_ammount() (gas: 12007)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1626)
[PASS] test_exit() (gas: 207423)
[PASS] test_join() (gas: 110604)
[PASS] test_slashing_2_users() (gas: 1702278)
[PASS] testFail_setup_invalid_accountingEngine() (gas: 60033)
[PASS] testFail_modify_parameters_invalid_tokens_to_auction() (gas: 1574)
[PASS] testFail_requestExit_null_amount() (gas: 106724)
[PASS] test_setup() (gas: 12400)
[PASS] testFail_setup_invalid_maxDelay() (gas: 59986)
[PASS] testFail_join_cant_join() (gas: 34442)
[PASS] testFail_setup_invalid_tokensToAuction() (gas: 59991)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1561)
[PASS] testFail_add_authorization_unauthorized() (gas: 4206)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4379)
```

```
[PASS] test_add_authorization() (gas: 25790)
[PASS] testFail_setup_invalid_safeEngine() (gas: 60070)
[PASS] test_modify_parameters() (gas: 27280)
[PASS] test_slashing() (gas: 313044)
[PASS] test_auction_ancestor_tokens() (gas: 214078)
[PASS] testFail_auction_ancestor_tokens_abovewater() (gas: 114562)
[PASS] testFail_auction_ancestor_tokens_abovewater_2() (gas: 156446)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4260)
[PASS] testFail_setup_invalid_systemCoinsToRequest() (gas: 60035)
[PASS] test_protocol_underwater() (gas: 62047)
[PASS] test_exit_forced_underwater() (gas: 222781)

Running 17 tests for src/test/GebLenderFirstResortRewards.t.sol:GebLenderFirstResortRewardsSameTokenTest
[PASS] test_join_2() (gas: 197931)
[PASS] test_rewards_dripper_depleated() (gas: 348335)
[PASS] test_exit() (gas: 235944)
[PASS] test_exit_rewards_1(uint256,uint256) (runs: 100)
[PASS] test_rewards_after_slashing() (gas: 462710)
[PASS] test_join() (gas: 160574)
[PASS] test_slashing_2_users() (gas: 1881272)
[PASS] test_rewards_over_long_intervals() (gas: 1748900)
[PASS] test_setup() (gas: 18386)
[PASS] test_rewards_dripper_depleated_recharged() (gas: 351428)
[PASS] test_get_rewards_externally_funded() (gas: 357145)
[PASS] test_exit_rewards_2_users2(uint256) (runs: 100)
[PASS] test_get_rewards() (gas: 338171)
[PASS] test_auction_ancestor_tokens() (gas: 295589)
[PASS] test_rewards_change_dripper_emission() (gas: 300603)
[PASS] test_deposit_rewards() (gas: 335409)
[PASS] test_protocol_underwater() (gas: 62179)

Running 54 tests for src/test/GebLenderFirstResortRewards.t.sol:GebLenderFirstResortRewardsTest
[PASS] testFail_modify_parameters_invalid_min_tokens_to_keep() (gas: 1607)
[PASS] testFail_join_unnaproved() (gas: 16269)
[PASS] test_remove_authorization() (gas: 3745)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4207)
[PASS] testFail_setup_invalid_auctionHouse() (gas: 62577)
[PASS] testFail_modify_parameters_invalid_system_coins_to_request() (gas: 1667)
[PASS] testFail_modify_parameters_null_address() (gas: 1554)
[PASS] testFail_modify_parameters_invalid_exit_delay() (gas: 1676)
[PASS] test_join_2() (gas: 197931)
[PASS] test_request_exit() (gas: 216145)
[PASS] testFail_exit_underwater() (gas: 238513)
[PASS] testFail_modify_parameters_invalid_max_concurrent_auctions() (gas: 1692)
[PASS] testFail_exit_no_request() (gas: 160860)
[PASS] testFail_request_exit_null_amount() (gas: 161440)
[PASS] testFail_join_underwater() (gas: 55436)
[PASS] test_rewards_dripper_depleated() (gas: 367016)
[PASS] testFail_setup_invalid_minStakedTokensToKeep() (gas: 62506)
[PASS] testFail_join_invalid_ammount() (gas: 14684)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1671)
[PASS] test_multi_user_diff_proportions() (gas: 2836210)
[PASS] test_exit() (gas: 235922)
[PASS] testFail_setup_invalid_rewardsDripper() (gas: 62690)
[PASS] testFail_exit_before_deadline() (gas: 216631)
[PASS] test_exit_rewards_1(uint256,uint256) (runs: 100)
[PASS] test_rewards_after_slashing() (gas: 483871)
[PASS] test_join() (gas: 160618)
[PASS] test_slashing_2_users() (gas: 1881316)
[PASS] testFail_setup_invalid_accountingEngine() (gas: 62571)
[PASS] testFail_modify_parameters_invalid_tokens_to_auction() (gas: 1597)
[PASS] test_rewards_over_long_intervals() (gas: 1750470)
[PASS] test_setup() (gas: 19598)
[PASS] testFail_setup_invalid_maxDelay() (gas: 62457)
[PASS] testFail_join_cant_join() (gas: 37141)
[PASS] testFail_setup_invalid_tokensToAuction() (gas: 62573)
[PASS] test_rewards_dripper_depleated_recharged() (gas: 370148)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1632)
[PASS] testFail_add_authorization_unauthorized() (gas: 4251)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4335)
[PASS] test_get_rewards_externally_funded() (gas: 375870)
[PASS] test_add_authorization() (gas: 25768)
[PASS] test_pending_rewards() (gas: 306365)
[PASS] testFail_setup_invalid_safeEngine() (gas: 62608)
[PASS] test_get_rewards() (gas: 356853)
[PASS] test_modify_parameters() (gas: 31544)
[PASS] test_auction_ancestor_tokens() (gas: 295634)
[PASS] test_exit_rewards_2_users(uint256) (runs: 100)
[PASS] testFail_auction_ancestor_tokens_abovewater() (gas: 165424)
[PASS] testFail_auction_ancestor_tokens_abovewater_2() (gas: 207353)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4327)
[PASS] testFail_setup_invalid_systemCoinsToRequest() (gas: 62573)
[PASS] test_rewards_change_dripper_emission() (gas: 319367)
[PASS] test_deposit_rewards() (gas: 354056)
[PASS] test_protocol_underwater() (gas: 62157)
[PASS] test_exit_forced_underwater() (gas: 252219)

Running 18 tests for src/test/GebLenderFirstResortRewardsVested.t.sol:GebLenderFirstResortRewardsVestedSameTokenTest
[PASS] test_join_2() (gas: 197931)
[PASS] test_rewards_dripper_depleated() (gas: 348691)
[PASS] test_exit() (gas: 235856)
[PASS] test_exit_rewards_1(uint256,uint256) (runs: 100)
[PASS] test_rewards_after_slashing() (gas: 462912)
[PASS] test_join() (gas: 160508)
[PASS] test_slashing_2_users() (gas: 1881052)
[PASS] test_rewards_over_long_intervals() (gas: 1750544)
[PASS] test_setup() (gas: 21794)
[PASS] test_rewards_dripper_depleated_recharged() (gas: 352250)
[PASS] test_get_rewards_externally_funded() (gas: 357879)
[PASS] test_exit_rewards_2_users2(uint256) (runs: 100)
[PASS] test_get_rewards() (gas: 338993)
[PASS] test_escrow_rewards_twice() (gas: 345633)
[PASS] test_auction_ancestor_tokens() (gas: 295457)
[PASS] test_rewards_change_dripper_emission() (gas: 301447)
[PASS] test_deposit_rewards() (gas: 336253)
[PASS] test_protocol_underwater() (gas: 62113)

Running 55 tests for src/test/GebLenderFirstResortRewardsVested.t.sol:GebLenderFirstResortRewardsVestedTest
[PASS] testFail_modify_parameters_invalid_min_tokens_to_keep() (gas: 1659)
[PASS] testFail_join_unnaproved() (gas: 16269)
[PASS] test_remove_authorization() (gas: 3746)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4230)
[PASS] testFail_setup_invalid_auctionHouse() (gas: 64143)
[PASS] testFail_modify_parameters_invalid_system_coins_to_request() (gas: 1667)
[PASS] testFail_modify_parameters_null_address() (gas: 1510)
[PASS] testFail_modify_parameters_invalid_exit_delay() (gas: 1676)
[PASS] test_join_2() (gas: 197931)
[PASS] test_request_exit() (gas: 214900)
[PASS] testFail_exit_underwater() (gas: 238491)
[PASS] testFail_modify_parameters_invalid_max_concurrent_auctions() (gas: 1701)
[PASS] testFail_exit_no_request() (gas: 160860)
[PASS] testFail_request_exit_null_amount() (gas: 161418)
[PASS] testFail_join_underwater() (gas: 55436)
[PASS] test_rewards_dripper_depleated() (gas: 367372)
[PASS] testFail_setup_invalid_minStakedTokensToKeep() (gas: 64072)
[PASS] testFail_join_invalid_ammount() (gas: 14684)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1723)
[PASS] test_multi_user_diff_proportions() (gas: 2840320)
[PASS] test_exit() (gas: 235834)
[PASS] testFail_setup_invalid_rewardsDripper() (gas: 64256)
[PASS] testFail_exit_before_deadline() (gas: 216609)
[PASS] test_exit_rewards_1(uint256,uint256) (runs: 100)
[PASS] test_rewards_after_slashing() (gas: 484073)
[PASS] test_join() (gas: 160552)
[PASS] test_slashing_2_users() (gas: 1881096)
[PASS] testFail_setup_invalid_accountingEngine() (gas: 64137)
[PASS] testFail_modify_parameters_invalid_tokens_to_auction() (gas: 1597)
[PASS] test_rewards_over_long_intervals() (gas: 1752114)
[PASS] test_setup() (gas: 21630)
[PASS] testFail_setup_invalid_maxDelay() (gas: 64023)
[PASS] testFail_join_cant_join() (gas: 37119)
[PASS] testFail_setup_invalid_tokensToAuction() (gas: 64139)
[PASS] test_rewards_dripper_depleated_recharged() (gas: 370992)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1614)
[PASS] testFail_add_authorization_unauthorized() (gas: 4251)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4402)
[PASS] test_get_rewards_externally_funded() (gas: 376604)
[PASS] test_add_authorization() (gas: 25724)
[PASS] test_pending_rewards() (gas: 306699)
[PASS] testFail_setup_invalid_safeEngine() (gas: 64239)
[PASS] test_get_rewards() (gas: 357675)
[PASS] test_modify_parameters() (gas: 31282)
[PASS] test_escrow_rewards_twice() (gas: 401862)
[PASS] test_auction_ancestor_tokens() (gas: 295502)
[PASS] test_exit_rewards_2_users(uint256) (runs: 100)
[PASS] testFail_auction_ancestor_tokens_abovewater() (gas: 165380)
[PASS] testFail_auction_ancestor_tokens_abovewater_2() (gas: 207309)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4283)
[PASS] testFail_setup_invalid_systemCoinsToRequest() (gas: 64139)
[PASS] test_rewards_change_dripper_emission() (gas: 320211)
[PASS] test_deposit_rewards() (gas: 354900)
[PASS] test_protocol_underwater() (gas: 62091)
[PASS] test_exit_forced_underwater() (gas: 252220)

Running 21 tests for src/test/RewardDripper.t.sol:RewardDripperTest
[PASS] testFail_transfer_token_unauthorized() (gas: 4174)
```

```
[PASS] test_remove_authorization() (gas: 3610)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4094)
[PASS] test_transfer_token_out() (gas: 30198)
[PASS] testFail_transfer_token_null_dst() (gas: 1452)
[PASS] testFail_setup_null_token() (gas: 34186)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1482)
[PASS] test_drip_reward() (gas: 82263)
[PASS] testFail_transfer_token_null_amount() (gas: 1430)
[PASS] testFail_modify_parameters_invalid_last_block() (gas: 1550)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1579)
[PASS] testFail_add_authorization_unauthorized() (gas: 4183)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4246)
[PASS] test_correct_setup() (gas: 4489)
[PASS] testFail_setup_null_reward() (gas: 34411)
[PASS] test_add_authorization() (gas: 25722)
[PASS] test_modify_parameters() (gas: 11589)
[PASS] testFail_setup_null_requestor() (gas: 34147)
[PASS] testFail_modify_parameters_invalid_reward_per_block() (gas: 1524)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4348)
[PASS] testFail_drip_unauthorized() (gas: 2355)

Running 42 tests for src/test/StakedTokenAuctionHouse.t.sol:StakedTokenAuctionHouseTest
[PASS] testFail_increase_bid_size_invalid_amountToBuy() (gas: 2412)
[PASS] test_restart_auction() (gas: 9825)
[PASS] test_remove_authorization() (gas: 3745)
[PASS] testFail_increase_bid_size_insufficient_increase() (gas: 3278)
[PASS] test_terminate_auction_prematurely() (gas: 82299)
[PASS] testFail_remove_authorization_unauthorized() (gas: 4095)
[PASS] testFail_modify_parameters_null_address() (gas: 1465)
[PASS] testFail_setup_null_token() (gas: 127242)
[PASS] testFail_start_auction_null_coins_requested() (gas: 2025)
[PASS] testFail_restart_auction_invalid() (gas: 1338)
[PASS] testFail_modify_parameters_disabled_address() (gas: 3672)
[PASS] testFail_modify_parameters_invalid_param_uint() (gas: 1729)
[PASS] test_start_auction() (gas: 5611)
[PASS] testFail_terminate_auction_prematurely_no_bid() (gas: 3766)
[PASS] testFail_increase_bid_size_expired() (gas: 35916)
[PASS] testFail_increase_bid_size_finished() (gas: 3601)
[PASS] testFail_modify_parameters_invalid_param_address() (gas: 1618)
[PASS] testFail_add_authorization_unauthorized() (gas: 4161)
[PASS] testFail_modify_parameters_unauthorized_uint() (gas: 4290)
[PASS] test_correct_setup() (gas: 6170)
[PASS] testFail_settle_auction_disabled() (gas: 38517)
[PASS] test_add_authorization() (gas: 25658)
[PASS] testFail_start_auction_invalid_coins_requested() (gas: 2041)
[PASS] testFail_setup_null_safeEngine() (gas: 127182)
[PASS] testFail_restart_already_bid() (gas: 35870)
[PASS] testFail_start_auction_null_accounting_engine() (gas: 1509)
[PASS] testFail_modify_parameters_disabled_uint() (gas: 3703)
[PASS] testFail_settle_auction_early() (gas: 37286)
[PASS] test_modify_parameters() (gas: 49360)
[PASS] test_settle_auction() (gas: 79012)
[PASS] testFail_modify_parameters_unauthorized_address() (gas: 4327)
[PASS] testFail_modify_parameters_null_uint() (gas: 1452)
[PASS] test_increase_bid_size() (gas: 53993)
[PASS] testFail_modify_parameters_invalid_Min_bid_increase() (gas: 1745)
[PASS] testFail_modify_parameters_invalid_uint() (gas: 1518)
[PASS] testFail_restart_auction_before_finish() (gas: 3005)
[PASS] testFail_terminate_auction_prematurely_enabled() (gas: 34004)
[PASS] testFail_start_auction_disabled() (gas: 3683)
[PASS] testFail_settle_auction_no_bids() (gas: 4710)
[PASS] testFail_start_auction_null_amount_to_sell() (gas: 1979)
[PASS] testFail_modify_parameters_invalid_bid_increase() (gas: 1688)
[PASS] testFail_increase_bid_size_disabled() (gas: 3540)

Running 4 tests for src/test/StakedTokensToKeepSetter.t.sol:StakedTokensToKeepSetterTest
[PASS] test_set_when_tiny_staked() (gas: 167416)
[PASS] test_set_when_nothing_staked() (gas: 15776)
[PASS] test_setup() (gas: 5887)
[PASS] test_set_when_large_stake() (gas: 252804)
```

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

```
4065cce696cfd0dadbb97da031410cca91e3006c948fa0a0119ae4a0d0162284 ./src/GebLenderFirstResortRewards.sol

967a121286d68309fb0cfae71a7cc46e1d1c983928c64a411e40df3b0ea449b3 ./src/auction/StakedTokenAuctionHouse.sol
```

Tests

```
d164ec9a139e0df8fe87b32a30020c895c03b2fc8eabeef87872d80b73860013 ./test/GebLenderFirstResortRewards.t.sol

c4f9f2b7df0fbe129d12200cbe59c87f9bcb9fc633c434507894307bffe31260 ./test/StakedTokenAuctionHouse.t.sol
```

Changelog

- 2021-07-09 - Initial report
- 2021-07-21 - Revised report based on commit `ed7d63d`

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.