Quantstamp Security Assessment Certificate

February 24th 2022 — Quantstamp Verified

LayerZero #2

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

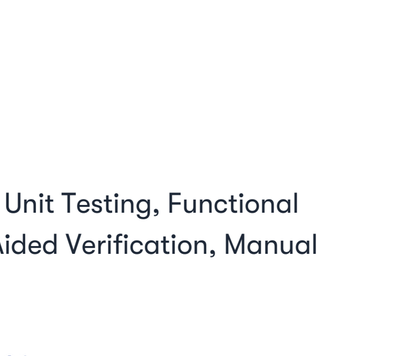
Executive Summary

Type	Decentralized Bridge
Auditors	Jose Ignacio Orlicki, Senior Engineer Jake Bunce, Research Engineer Souhail Mssassi, Research Engineer
Timeline	2022-01-24 through 2022-02-24
EVM	London
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	LayerZero Whitepaper LayerZero Blog
Documentation Quality	Medium
Test Quality	High

Source Code

Repository	Commit
stargate	ed010ab
stargate	125cf34

Total Issues	**9** (2 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	**2** (0 Resolved)
Low Risk Issues	**6** (2 Resolved)
Informational Risk Issues	**1** (0 Resolved)
Undetermined Risk Issues	0 (0 Resolved)



FAST RESPONSE TIMES

ALL ISSUES ADDRESSED

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 but with some lacking documentation in the form of inline comments. The test suite is very extensive but can be improved given the suggested changes from this report. We also recommend improving the coverage of LPTokenERC20 and Router (branch coverage of LPTokenERC20 is especially bad at 33%). We have outlined very few suggestions to better follow best practices, and recommend addressing all the findings to tighten the contracts for future deployments or contract updates. We recommend addressing all the **10** findings to harden the contracts for future deployments or contract updates. We recommend against deploying the code as-is.
Update: All issues were addresses or acknowledged for commit **125cf34**.

ID	Description	Severity	Status
QSP-1	Use Of `transfer()` Instead Of `safeTransfer()`	^ Medium	Acknowledged
QSP-2	Unrestricted Transaction Forwarding	^ Medium	Acknowledged
QSP-3	Centralization Risk	v Low	Acknowledged
QSP-4	For Loop Over Dynamic Array	v Low	Acknowledged
QSP-5	Missing Address Verification	v Low	Fixed
QSP-6	Mechanism of setting the bridge and factory could lead to a broken deployment	v Low	Acknowledged
QSP-7	Missing event for paused transfers	v Low	Fixed
QSP-8	Unclear Incentives To Avoid Collusion	v Low	Acknowledged
QSP-9	Solidity Version And SafeMath	O Informational	Acknowledged

Quantstamp Audit Breakdown

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

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

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

Methodology

The Quantstamp auditing process follows a routine series of steps:

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

Findings

QSP-1 Use Of `transfer()` Instead Of `safeTransfer()`

Severity: *Medium Risk*

Status: Acknowledged

File(s) affected: `contracts/OmniChainFungibleToken.sol (L63)`, `contracts/OmniChainFungibleToken.sol (L104)`

Description: The ERC20 standard token implementation functions also return the transaction status as a Boolean. It's good practice to check for the return status of the function call to ensure that the transaction was successful. It is the developer's responsibility to enclose these function calls with require() to ensure that, when the intended ERC20 function call returns false, the caller transaction also fails. However, it is mostly missed by developers when they carry out checks; in effect, the transaction would always succeed, even if the token transfer didn't.

Recommendation: Use the `safeTransfer()` function from the `safeERC20` implementation or put the transfer call inside an assert or require to verify that it returned true.

Update: The LayerZero team acknowledges this issue but is not a problem because the function `_transfer()` reverts in case of problems. Detailed comment says *"This is an internal additional call to the underlying ERC20 functionality. This is not an ERC20 call. It will revert if the checks do not pass and therefore having "safeTransfer" is not required. ie. it's calling _transfer which does not return a boolean at all"*.

QSP-2 Unrestricted Transaction Forwarding

Severity: *Medium Risk*

Status: Acknowledged

File(s) affected: `Bridge.sol`, `Router.sol`

Description: Forwarding transactions as data, metaprogramming, is useful but can bring serious security hazards. Take for example the AlphaHomora hack, where any malicious smart contract code (called *spells*) were allowed access to lending and combined with rounding issues generated serious financial losses. Also, for example, standard ERC-1363 allows generic transactions to be executed by third parties, this can allow ERC-20 or NFT sent to the contract to be stolen by malicious third-parties sending self-referential transactions.

Recommendation: Consider including white-listing features, at least during a launch period, to mitigate the risk of malicious smart contracts combined with other issues. Consider including blacklisting features to avoid self-referential transactions that can allow malicious users to manipulate the protocol (ie. filter out sending reflective transactions to LayerZero endpoints on-chain).

Update: The LayerZero team acknowledges this issue but is not a problem because they already have whitelisting of the contract. The detailed comment says *"We/the dao control the addition of any external smart contracts to the system(pools), whitelisting is just as safe as controlling these calls with onlyOwner via multisig. The hack mentioned in the suggestion refers to contracts where users had the ability to arbitrarily identify their own contracts(spells). This is not the same risk profile as our implementation. ie. Whitelisting is the same as having us control what contracts can be called/wired into the system."*.

QSP-3 Centralization Risk

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `contracts/Bridge.sol (L403)`

Description: In the contract `Bridge`, the role `owner` has the authority over the following functions:

- Approve tokens to spend.
- Change the bridge address.

Any comprise to the `owner` account may allow the hacker to take advantage of this.

Recommendation: We advise the client to carefully manage the `owner` account's private key to avoid any potential risk of being hacked.

Update: The LayerZero team acknowledges this issue but is not a problem because they are introducing MultSig wallets for DAO Governance. The detailed comment was that it is *"Noted and is part of the DOA governance we are introducing with multisgs etc."*.

QSP-4 For Loop Over Dynamic Array

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `contracts/LPStaking.sol (L163)`, `contracts/Pool.sol (L376)`, `contracts/Pool.sol (L498)`

Description: When smart contracts are deployed or their associated functions are invoked, the execution of these operations always consumes a certain quantity of gas, according to the amount of computation required to accomplish them. Modifying an unknown-size array that grows in size over time can result in a Denial-of-Service attack. Simply by having an excessively huge array, users can exceed the gas limit, therefore preventing the transaction from ever succeeding.

Recommendation: Avoid actions that involve looping across the entire data structure. If you really must loop over an array of unknown size, arrange for it to consume many blocs and thus multiple transactions. Consider flagging pools that need to be updated, and only iterate over those pools that need an update.

Update: The LayerZero team acknowledges this issue but is not a problem because they are aware of the limitations. The detailed comment was that it is *"Necessary, but we are aware there can be limitations if the loop becomes too big."*.

QSP-5 Missing Address Verification

Severity: *Low Risk*

Status: Fixed

File(s) affected: `contracts/StartgateFeeLibraryV01.sol (L16)`, `contracts/Bridge.sol (L204)`, `contracts/Factory.sol (L35)`, `contracts/Factory.sol (L52)`, `contracts/LPStaking.sol (L104)`, `contracts/Pool.sol (L404)`

Description: Certain functions lack a safety check in the address, the address-type argument should include a zero-address test, otherwise, the contract's functionality may become inaccessible or tokens may be burned in perpetuity.

Recommendation: It’s recommended to undertake further validation prior to user-supplied data. The concerns can be resolved by utilizing a whitelist technique or a modifier.

Update: Fixed in this [commit](https://github.com/ryanzarick/stargate/commit/125cf34dd370efba40896ba619b0e34e6ba 73e54).

QSP-6 Mechanism of setting the bridge and factory could lead to a broken deployment

Severity: *Low Risk*

Status: Acknowledged

Description: The docstrings in `setBridgeAndFactory()` indicate that these values should only be set once. A better pattern for this is to use the constructor which will allow for immutable variable assignment at deploy time. Same applies to the Bridge `setRouter()` and Factory `setRouter()`.

Exploit Scenario: 1) Contracts are deployed and operational. 2) Actor with the `onlyOwner` role calls `setBridgeAndFactory()` with the zero address for the bridge and factory contract addresses. 3) There is no ability to change these to the correct contract addresses.

Recommendation: Set these one-time variable assignments at deploy time in the constructor.

Update: The LayerZero team acknowledges this issue but is not a problem because due to circular dependencies init calls cannot be placed everywhere. Also, they consider that if zero addresses are placed, it can still be change now. The detailed comment by the LayerZero team was that *"Circular dependencies prevent us from calling all these init calls inside of all the constructors. That being said I have added the router address inside of the bridge.sol and factory.sol constructors. Also made them immutable. 😉 "3) There is no ability to change these to the correct contract addresses." This exploit scenario is false. The one time initialize block is a check if the address is 0x0, therefore if the owner sets them to 0x0, they wont be blocked on subsequent calls until they are explicitly set to something non ZERO_ADDRESS. I have added another check to makde sure none of them can be set to 0x0 anyways though."*

QSP-7 Missing event for paused transfers

Severity: *Low Risk*

Status: Fixed

File(s) affected: `OmnichainFungibleToken.sol`

Description: Transfers of this token can be paused with the `paused` bool. Emitting an event is useful for people to track this event in production.

Recommendation: Emit and event when sending tokens is paused and unpaused.

Update: Fixed in this [commit](https://github.com/ryanzarick/stargate/commit/125cf34dd370efba40896ba619b0e34e6ba 73e54).

QSP-8 Unclear Incentives To Avoid Collusion

Severity: *Low Risk*

Status: Acknowledged

Description: One of the main features of the system design is the incorporation of independents Oracle and Relayer agents that do not collude with each other. Given that, we did not find in the documentation or implementation features to incentivize the separation of concerns between Oracle and Relayer, how these stakeholders are rewarded for valid behavior or punished for inappropriate behavior. Failed or missing incentives can result in low engagement of open participants (low number of Relayers), or the possibility of collusion when the value of the assets involved in the protocol increases over time (Oracle providers such as Chainlink or its employees can be tempted to collude with Relayers).

Recommendation: Is recommended to mitigate with ordering (change internal state before external calls) or block with reentrancy guards (example `ReentrancyGuard.sol` modifiers) all potential reentrancy situations.

Update: The LayerZero team acknowledges this issue but is not a problem because applications can specify which sets of relayers/oracles they want to use. The detailed comment by the LayerZero team was that *"This is more of a layerZero concern(different audits). That being said, applications can specify which sets of relayers/oracles they trust. They can choose their own, or go with defaults."*.

QSP-9 Solidity Version And SafeMath

Severity: *Informational*

Status: Acknowledged

Description: The version of Solidity in use across the project is 0.7.6. From versions >=0.8.0 SafeMath is included in the compiler so developers do not need to include this library or remember to use it correctly.

Recommendation: Use a version of Solidity >=0.8.0.

Update: The LayerZero team acknowledges this issue but is not a problem because version 0.8.* is not gas efficient enough for them and they have all the tests needed for SafeMath. The detailed comment by the LayerZero team was that *"8+ is not as gas efficient and we have tests for all the instances of safemath we need."*.

Code Documentation

Missing more online comments in smart contracts usually adds to maintainability and audits although is common for devs to avoid or implement them when the code is more stable.

Adherence to Best Practices

- On L37 of `OmnichainFungibleToken.sol` there is a redundant casting of `endpoint` to `ILayerZeroEndpoint` because it has already been cast.
- Lint Errors

```
Bridge.sol
   64:2  error  Line length must be no more than 120 but current length is 133  max-line-length
   89:2  error  Line length must be no more than 120 but current length is 124  max-line-length
   91:2  error  Line length must be no more than 120 but current length is 144  max-line-length
   94:2  error  Line length must be no more than 120 but current length is 140  max-line-length
  101:2  error  Line length must be no more than 120 but current length is 130  max-line-length
  103:2  error  Line length must be no more than 120 but current length is 126  max-line-length
  125:2  error  Line length must be no more than 120 but current length is 134  max-line-length
  139:2  error  Line length must be no more than 120 but current length is 123  max-line-length
  197:2  error  Line length must be no more than 120 but current length is 121  max-line-length
  233:2  error  Line length must be no more than 120 but current length is 134  max-line-length
  300:2  error  Line length must be no more than 120 but current length is 140  max-line-length

Factory.sol
  52:2  error  Line length must be no more than 120 but current length is 122  max-line-length

LPTokenERC20.sol
  109:2  error  Line length must be no more than 120 but current length is 132  max-line-length

OmnichainFungibleToken.sol
   90:2  error  Line length must be no more than 120 but current length is 145  max-line-length
  110:2  error  Line length must be no more than 120 but current length is 131  max-line-length
  119:2  error  Line length must be no more than 120 but current length is 134  max-line-length

Pool.sol
   55:2  error  Line length must be no more than 120 but current length is 132  max-line-length
   67:2  error  Line length must be no more than 120 but current length is 128  max-line-length
```

```
   72:2  error  Line length must be no more than 120 but current length is 124  max-line-length
  111:2  error  Line length must be no more than 120 but current length is 124  max-line-length
  208:2  error  Line length must be no more than 120 but current length is 128  max-line-length
  269:2  error  Line length must be no more than 120 but current length is 133  max-line-length

Router.sol
   51:2  error  Line length must be no more than 120 but current length is 127  max-line-length
   56:2  error  Line length must be no more than 120 but current length is 136  max-line-length
   57:2  error  Line length must be no more than 120 but current length is 135  max-line-length
  127:2  error  Line length must be no more than 120 but current length is 125  max-line-length
  187:2  error  Line length must be no more than 120 but current length is 133  max-line-length
  274:2  error  Line length must be no more than 120 but current length is 140  max-line-length
  317:2  error  Line length must be no more than 120 but current length is 132  max-line-length
  329:2  error  Line length must be no more than 120 but current length is 143  max-line-length
  400:2  error  Line length must be no more than 120 but current length is 141  max-line-length
  407:2  error  Line length must be no more than 120 but current length is 123  max-line-length

interfaces/ILayerZeroEndpoint.sol
   8:2  error  Line length must be no more than 120 but current length is 196  max-line-length
  10:2  error  Line length must be no more than 120 but current length is 184  max-line-length
  14:2  error  Line length must be no more than 120 but current length is 134  max-line-length

interfaces/ILayerZeroUserApplicationConfig.sol
  14:2  error  Line length must be no more than 120 but current length is 137  max-line-length

 ✓ 36 problems (36 errors, 0 warnings)
```

Test Results

Test Suite Results

The number of tests climbed to 193 test cases for 13 modules, around 15 test cases per module on average. We consider the testing suite very complete and extensive, although reported issues in this report might need to be considered to add news test cases. Detailed output is included below. LPTokenERC20 has only 2 test cases.

```
$ npx hardhat test
  Bridge
     ✓ constructor() reverts for 0x0 LZ endpoint
     ✓ renounceOwnership() doesnt affect ownership
     ✓ lzReceive() reverts for non LZ endpoint
     ✓ lzReceive() reverts for mismatched bridgeLookup
     ✓ setRouter() reverts when bridge is 0x0
     ✓ setBridge()
     ✓ setBridge() reverts when bridge already set
     ✓ setBridge() reverts for non owner
     ✓ setGasAmount() reverts for non owner
     ✓ setGasAmount() reverts for invalid function type
     ✓ setGasAmount() with valid function type
     ✓ approveTokenSpender() reverts for non owner
     ✓ approveTokenSpender() approves amount
     ✓ setUseLayerZeroToken() reverts for non owner
     ✓ setUseLayerZeroToken() called from owner
     ✓ quoteLayerZeroFee() with TYPE_SWAP_REMOTE returns valid fee
     ✓ quoteLayerZeroFee() with TYPE_ADD_LIQUIDITY returns valid fee
     ✓ quoteLayerZeroFee() with TYPE_REDEEM_LOCAL_CALL_BACK returns valid fee
     ✓ quoteLayerZeroFee() with TYPE_WITHDRAW_REMOTE returns valid fee
     ✓ call setConfig() as non owner reverts (1227ms)

  Factory
     ✓ allPoolsLength()
     ✓ setRouter() reverts if router address has been set
     ✓ createPool() reverts if creatPair() is called for existing _poolId
     ✓ createPool() increments allPoolsLength() (221ms)
     ✓ createPool() reverts when called by non router
     ✓ renounceOwnership() doesnt affect ownership

  LPStaking
     ✓ constructor() reverts for 0x0 params
     ✓ stake a token into pid 0 (166ms)
     ✓ adding duplicate token reverts
     ✓ stake a token into pid 0 when amount is to large (134ms)
     ✓ call only owner function then renounce ownership followed by another only owner function should not revert
     ✓ call getMultiplier with _to field equal to bonus end block
     ✓ call getMultiplier with _from field less than the bonus end block

  LPTokenERC20
     ✓ call approve and expect a Approval event
     ✓ permit() - TODO

  StargateToken
     ✓ (simple-0) user0-endpoint0 sends to user1-endpoint4  (41ms)
     ✓ (simple-1) user0-endpoint0 sends to user1-endpoint1  (38ms)
     ✓ (simple-2) user0-endpoint0 sends to user0-endpoint0 (39ms)
     ✓ (complex-3}  (3093ms)
     ✓ initial balances of main and children (token contract)
     ✓ initial balances of main and children (users)
     ✓ sending oft cross chains (74ms)
     ✓ estimateSendTokensFee()

  Pool
     ✓ constructor() reverts for 0x0 params
     ✓ Should return the proper pool settings
     ✓ Should create a proper pool connection
     ✓ mint() reverts when called by non Router
     ✓ Should fail to mint with no chainpaths
     ✓ Should fail to mint with no weights for chainpaths
     ✓ Should mint to the user
     ✓ Should transferFrom the user to alice after approved (58ms)
     ✓ Should fail to transferFrom the user to alice because of no approval (55ms)
     ✓ Should set weight for chain
     ✓ Should return correct chainPaths length
     ✓ Should properly allocation to two pools based on weights (66ms)
     ✓ Should add to balance for remote chain
     ✓ redeemLocal()
     ✓ redeemLocal() reverts if path is not activated
     ✓ creditChainPath() emits event
     ✓ swapRemote() emits event (40ms)
     ✓ withdrawMintFeeBalance() emits event (47ms)
     ✓ redeemLocalCallback() emits event when _amountToMintSD is > 0 (46ms)
     ✓ setup to call _delta() where total > _amountSD (91ms)
     ✓ redeemLocalCheckOnRemote() emits event
     ✓ createChainPath() and setWeightForChainPath() emit correct event(s)
     ✓ setFee() emits correct event
     ✓ swap() reverts when called by non Router
     ✓ swap() reverts if swapStop called
     ✓ swap() reverts if chainPath not active
     ✓ sendCredits() reverts when called by non Router
     ✓ sendCredits() emits event (47ms)
     ✓ redeemRemote() reverts when _from is 0x0
     ✓ redeemLocal() reverts when _from is 0x0
     ✓ redeemRemote() reverts when called by non Router
     ✓ redeemRemote() reverts
     ✓ activateChainPath() reverts when called on already activated path
     ✓ createChainPath() reverts when duplicate chainpath tried to be created
     ✓ activateChainPath() reverts when called on a cp that doesnt exist
     ✓ redeemLocal() reverts when called by non Router
     ✓ creditChainPath() reverts when called by non Router
     ✓ swapRemote() reverts when called by non Router
     ✓ redeemLocalCallback() reverts when called by non Router
     ✓ redeemLocalCheckOnRemote() reverts when called by non Router
     ✓ createChainPath() reverts when called by non Router
     ✓ setWeightForChainPath() reverts when called by non Router
     ✓ setWeightForChainPath() reverts when no chainPaths have been created yet
     ✓ setFee() reverts when called by non Router
     ✓ setFee() reverts cumulative fee exceeds 100%
     ✓ setFeeLibrary() sets properly
     ✓ setFeeLibrary() reverts by non-router
     ✓ setSwapStop() sets properly
     ✓ setSwapStop() reverts by non-router
     ✓ setDeltaParam() reverts by non-router
     ✓ setDeltaParam() reverts if basis points are wrong
     ✓ setDeltaParam() emits event
     ✓ callDelta() reverts by non-router
     ✓ callDelta() can be called by router
     ✓ withdrawProtocolFeeBalance() reverts when called by non Router
     ✓ withdrawMintFeeBalance() reverts when called by non Router
     ✓ withdrawMintFeeBalance() called by Router with mintFeeBalance equal to 0
     ✓ withdrawProtocolFeeBalance() called by Router with protocolFeeBalance equal to 0
     ✓ createChainPath() x6 and mint() which calls _distribute fees (146ms)
     ✓ createChainPath() x10 and mint() which calls _distribute fees (268ms)
     ✓ createChainPath() x50 and mint() which calls _distribute fees (2147ms)

  Pool State
     ✓ error free add liquidity, mint and swap etc. (420ms)
     ✓ swap() lzTxParams transfers extra gas (148ms)
```

```
    ✓ redeemRemote() lzTxParams transfers extra gas (158ms)
    ✓ redeemLocal() lzTxParams transfers extra gas (258ms)
    ✓ Mass test, check for dust leak, uncomment if you wish to run
    ✓ withdrawMintFees() does not create balance issues (166ms)
    ✓ mintAndSwap() should revert because balances when total deficit is reached is distributed pro-rata (1891ms)
    ✓ mintAndSwap().verbose 2 chains 2 tokens sharing liquididty (2068ms)

  Router
    ✓ addLiquidity() reverts for non existant pool
    ✓ createPool() reverts when token is 0x0
    ✓ setBridgeAndFactory() reverts when bridge and factory are half set (70ms)
    ✓ swap() - TODO
    ✓ redeemRemote() - TODO
    ✓ redeemLocal() - TODO
    ✓ sendCredits() - Reverts when refund address is 0x0
    ✓ sendCredits() - TODO
    ✓ quoteLayerZeroFee() - TODO
    ✓ retryRevert() - reverts when theres nothing to try to retry
    ✓ revertRedeemLocal() - reverts when theres nothing to try to retry
    ✓ retryRevert() - TYPE_REDEEM_LOCAL_CALL_BACK_REMOTE - TODO
    ✓ retryRevert() - TYPE_REDEEM_LOCAL_CALL_BACK_LOCAL - TODO
    ✓ retryRevert() - TYPE_SWAP_REMOTE_LOCAL - TODO
    ✓ clearCachedSwap() reverts when nothing to clean
    ✓ creditChainPath() reverts when caller is not Bridge
    ✓ removeLiquitidyRemote() reverts when caller is not Bridge
    ✓ redeemLocalCallback() reverts when caller is no Bridge
    ✓ swapRemote() reverts when caller is no Bridge
    ✓ createPool() reverts when caller is not the dao
    ✓ createChainPath() reverts when caller is not the dao
    ✓ setWeightForChainPath() reverts when caller is not the dao
    ✓ setProtocolFeeOwner() reverts when caller is not the dao
    ✓ setProtocolFeeOwner() when caller is the dao
    ✓ setProtocolFeeOwner() with address set to zero should revert
    ✓ setMintFeeOwner() reverts when caller is not the dao
    ✓ setMintFeeOwner() when caller is the dao
    ✓ setMintFeeOwner() with address set to zero should revert
    ✓ setFees() reverts when caller is not the dao
    ✓ setFeeLibrary() reverts when caller is not the Owner
    ✓ setSwapStop() reverts when caller is not the Owner
    ✓ setFeeLibrary() when caller is Owner
    ✓ setSwapStop() when caller is the Owner
    ✓ callDelta() anyone can call
    ✓ withdrawMintFee() reverts when caller is not the mintFeeOwner
    ✓ withdrawMintFee() when caller is the mintFeeOwner
    ✓ withdrawProtocolFee() reverts when caller is not the protocolFeeOwner
    ✓ withdrawProtocolFee() reverts when caller is not the protocolFeeOwner (50ms)
    ✓ quoteLayerZeroFee() with no revert

  Staking
    ✓ constructor() reverts for 0x0 params
    ✓ enter() reverts when amount is 0
    ✓ leave() reverts when _share is 0
    ✓ call enter when no xStargate exists
    ✓ call enter when totalShares and totalStargate are greater than 0
    ✓ call enter when no xStargate exists followed by leave

  Stargate singlechain w/ LayerZeroEndpointMock
    ✓ addLiquidity()  (111ms)
    ✓ lets swap em up!  (141ms)

  Stargate LPer (singlechain w/ LayerZeroEndpointMock)
    ✓ test remove liquidity from both sides (219ms)
    ✓ test remove Liquidity And Redeem On Remote from both sides and revertRedeemLocal should revert (158ms)

  StargateToken
    ✓ name
    ✓ symbol
    ✓ decimals
    ✓ mints deployer some initial supply
    ✓ renounceOwnership() doesnt affect ownership
    ✓ lzReceive can mint to address (67ms)
    ✓ call setConfig() as non owner reverts
    ✓ call setDestination() as non owner reverts
    ✓ owner sendTokens()
    ✓ call pause as non owner reverts
    ✓ owner can pause
    ✓ no one can sendTokens when paused

  SwapMath
alice lp++ 5000 to A
alice lp++ 5000 to B
alice lp++ 5000 to C
carol swap 10 from A to B
carol swap 10 from B to A
carol swap 30 from C to A
     ✓ no fee swap test, vanilla delta (406ms)
removed liquidity from local
removed liquidity from remote
alice lp++ 5000 to A
alice lp++ 5000 to B
alice lp++ 5000 to C
carol swaps 1000 from A to B not OK
    book audit OK
carol swaps 1000 A to B OK
    book audit OK
carol swaps 1000 from B to A OK
    book audit OK
carol swap 30 from C to A
    book audit OK
     ✓ swap test, with sg and lp fee, vanilla delta (554ms)
removed liquidity from local
removed liquidity from remote
alice lp++ 5000 to A
alice lp++ 5000 to B
alice lp++ 5000 to C
carol swaps 1000 from A to B not OK
    book audit OK
carol swaps 1000 A to B OK
    book audit OK
carol swaps 1000 from B to A OK
    book audit OK
carol swap 30 from C to A
    book audit OK
     ✓ swap test, with all fee, vanilla delta (634ms)
removed liquidity from local
removed liquidity from remote
alice lp++ 5000 to A
alice lp++ 5000 to B
alice lp++ 5000 to C
carol swap 120 A to B
    book audit OK
carol swap 120 A to C
    book audit OK
mint and approve chainD token to Alice
mint and approve chainD token to Alice
provide liquidity to chain D OK
provide liquidity to chain A and send credit to D OK
carol swap 120 D to A
     ✓ add in a new stargateD, alice addLiquidity, no fee, then swap() (1517ms)
removed liquidity from local
amount > cp.balance, adjusted amountLP
amount > cp.balance, adjusted amountLP
removed liquidity from remote
alice lp++ 5000 to A
alice lp++ 5000 to B
alice lp++ 5000 to C
alice instant redeem local success
alice instant redeem local success
alice redeem local
     ✓ should be able to instant withdraw with deltaCredit (544ms)
removed liquidity from local
removed liquidity from remote


  178 passing (1m)
```

Code Coverage

The code coverage is overall very good, statement coverage is above 90% with the exception of LPTokenERC20 and Router, branch coverage is above 90% with the exception of the same contract (branch coverage of 33% for LPTokenERC20 is very bad).

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	89.64	87.85	87.68	89.86	
Bridge.sol	90.67	96.88	72	90.79	… 247,250,253
Factory.sol	100	100	100	100	
LPStaking.sol	90.79	83.33	100	90.67	… 175,176,245
LPTokenERC20.sol	71.88	33.33	72.73	72.73	… 130,131,132
OmnichainFungibleToken.sol	75	91.67	50	75.86	… 132,135,139
Pool.sol	97.09	93.18	100	97.09	… 551,552,553
Router.sol	81.36	73.68	100	82.68	… 410,414,423
Staking.sol	100	100	100	100	
StargateToken.sol	100	100	100	100	
contracts/interfaces/	100	100	100	100	
ILayerZeroEndpoint.sol	100	100	100	100	
ILayerZeroReceiver.sol	100	100	100	100	
ILayerZeroUserApplicationConfig.sol	100	100	100	100	
IStargateFeeLibrary.sol	100	100	100	100	
IStargateReceiver.sol	100	100	100	100	
IStargateRouter.sol	100	100	100	100	
All files	**89.64**	**87.85**	**87.68**	**89.86**	

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

```
4ecac97441b697dc3ec17bd81f052316a6fd89bd3692ef3d8f2e83f02fc9b0ea ./contracts/LPStaking.sol
a6743207fd2c71aee625cd80ddd2aa504f110d43b975312f2bd238a7af6a2f63 ./contracts/Factory.sol
95e39c5925870fbb390c11c62b377e295d2638dd0d9c4faf96fd2e5baa694877 ./contracts/Pool.sol
1a7e6e24c696d98da8809cf95f1317e6d001e7b4800f524855e5fb66b10ff1c9 ./contracts/Bridge.sol
fcb9419aaab336c4c9efb3159e7d8af12607d0a7ff2526396c85a1df23865841 ./contracts/LPTokenERC20.sol
c102be6043e9d6d6be012f50db15a1ec051ecfabdc16386c2a0d5b36df713325 ./contracts/StargateToken.sol
71fad578f851f77dd11771bec73c838cc27c8521a3b1230b5be7a2f3eb5dedc4 ./contracts/OmnichainFungibleToken.sol
7664ea69cf5b5da21d4f90a1deff5ad9d58880f7c0c52c997dbc1ff719fb4457 ./contracts/Router.sol
52cc616773aeebaf7da6a4021370062b18151baf5c8ac8d2e162745390bfb61b ./contracts/Staking.sol
84f12afeab73920c7e22f967cf39ac462e27bb42873da9010b2917dc9beb89e4 ./contracts/interfaces/IStargateRouter.sol
1312650cb9baf8a0ab69bca273fc9e38d8e41038891957cd8ba75dfacbad41fd ./contracts/interfaces/IStargateReceiver.sol
af0c15b42c47173326e384eadc5ddda50be769b691c0399dd9ea452b1bfbbeab ./contracts/interfaces/ILayerZeroEndpoint.sol
1511ad1ebb4e2cf4e9932ff1a3bbcaa0c1aadaef560e004554a709967482beda ./contracts/interfaces/ILayerZeroReceiver.sol
2a5966def85d40f82c7da2d8219e4bdc73b2a2f6e507117297a115f02556a302 ./contracts/interfaces/ILayerZeroUserApplicationConfig.sol
9660f4443882935c96e1d7e3fe26b0b5fdf4164b281f9210fd761beddc72e45b ./contracts/interfaces/IStargateFeeLibrary.sol
a0097cfbf35c939a4dc1ad6cd9d655c4e0732d4e1936776a8c103d5469b4cafc ./contracts/libraries/StargateFeeLibraryV01.sol
6bc24afb1868dfb8b41bc969fb8b9c804893f9d52f258dbad62ad2860a97af86 ./contracts/mocks/MockTokenWithDecimals.sol
e061cc44889a8cd1e7f129a70a67beaf08098ccbabd3ad868ebbce9d8c05dfcd ./contracts/mocks/MockToken.sol
52bdb1775bd05505a89426c103e73b28aa66f94ac1ab6187aed511bbfc45bfbf ./contracts/mocks/LayerZeroEndpointMock.sol
18babd68d11db0f15aa4d02f2328a1af1dea96e2ed1466c73f7e602d52b3f0e6 ./contracts/mocks/MockTokenNoInitialMint.sol
595c56b714430ab6f991b21fa81e62663dfc3501659672c6b738f39403ee24f0 ./contracts/mocks/LayerZeroMultiEndpointMock.sol
```

Tests

```
0e18f5706efc069034e40b786d4bc76efc84ee6e931e84fbd4bd7f4c868c9a07 ./test/oft.test.js
c97225112c609b1740f4fac769ea77f48e08857b42c1cffae5d0178334de0429 ./test/PoolState.test.js
ba1355c685c2fcd22c72aad0ce5090f96dae3ceaf77467b50f224559051818e5 ./test/Factory.test.js
a460261a26bef8fff3ca2c3c97353a5621639dfe41f8bf3d21eeee9a8b336a31 ./test/Pool.test.js
560401a29cf416d13a7d4366bc4fa07ee264032dba9a71c149310fee771ffcc6 ./test/LPTokenERC20.test.js
07ec760bc1121ee92c1759402e08b9f3e2b5737160e017a6c55692539b82f171 ./test/Stargate.test.js
81cf787834ae2658c2d6bdf0f6ced6b630eac45165916404ebb5538904442560 ./test/Staking.test.js
bdfccf2c2b301dd24c89621b196082b5080e75902e41e6d10005e4be1d2131b4 ./test/LPStaking.test.js
cd084fc8e84b1e11d86d72db0943259594037250eb820dcb0861d88fa0fb3641 ./test/StargateToken.test.js
c2a50a3e9f0826bec005998b756104de98df67df21705ea3c9e3c206592846f0 ./test/Bridge.test.js
4a02a6c0c9a2cc096321c8a08595f67d8eb236df9a2966d74fc73dc5d2a32f98 ./test/SwapMath.test.js
160a1da3f6ef49c47eee66a06a3271381fa797738e5f589f40f6bbb866b1f611 ./test/Router.test.js
77956b7903da8f6603a5379562496aabf047c1ba27a2ce90f28d27fbd0349f39 ./test/util/poolstateHelpers.js
231b1ff8ad0fee6fb0c33fab701dc14f0c612d6b0fbf77fac9c67d1a1b29cd59 ./test/util/globalBook.js
019b62f0df8d5fd2bfebaef430112787220e235d2b54b7e37ef79108462cc9fc ./test/util/helpers.js
```

Changelog

- 2022-02-11 - Initial report
- 2022-02-24 - Reaudit report (125cf34)

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.