0.7

Liquity Process Quality Review

Score: 96%

Overview

This is a Process Quality Review of Liquity completed on May 31st 2021. It was performed using the Process Review process (version 0.7) and is documented here. The review was performed by Nic of DeFiSafety. Check out our Telegram.

The final score of the review is **96%**, a **PASS**. The breakdown of the scoring is in Scoring Appendix. For our purposes, a pass is 70%.

Summary of the Process

Very simply, the review looks for the following declarations from the developer's site. With these declarations, it is reasonable to trust the smart contracts.

- **Here are my smart contracts on the blockchain**
- **Here is the documentation that explains what my smart contracts do**
- **Here are the tests I ran to verify my smart contract**
- **Here are the audit(s) performed on my code by third party experts**
- **Here are the admin controls and strategies**

Disclaimer

views to change. All information is subject to possible correction. Information may quickly become unreliable for various reasons, including changes in market conditions or economic circumstances.

Chain

This section indicates the blockchain used by this protocol.

> **Chain:** Ethereum

Guidance:

Ethereum
Binance Smart Chain
Polygon
Terra
Avalanche
Celo
Solana

Code and Team

This section looks at the code deployed on the Mainnet that gets reviewed and its corresponding software repository. The document explaining these questions is here. This review will answer the questions;

1) Are the executing code addresses readily available? (%)
2) Is the code actively being used? (%)
3) Is there a public software repository? (Y/N)
4) Is there a development history visible? (%)
5) Is the team public (not anonymous)? (Y/N)

1) Are the executing code addresses readily available? (%)

> **Answer:** 100%

They are available at website https://docs.liquity.org/documentation/resources#contract-addresses, as indicated in the Appendix.

Guidance:

100% Clearly labelled and on website, docs or repo, quick to find

70% Clearly labelled and on website, docs or repo but takes a bit of looking
40% Addresses in mainnet.json, in discord or sub graph, etc
20% Address found but labeling not clear or easy to find
0% Executing addresses could not be found

2) Is the code actively being used? (%)

> **Answer:** 100%

Activity is 250 transactions a day on contract *LQTYStaking.sol*, as indicated in the Appendix.

Guidance:

100% More than 10 transactions a day
70% More than 10 transactions a week
40% More than 10 transactions a month
10% Less than 10 transactions a month
0% No activity

3) Is there a public software repository? (Y/N)

> **Answer:** Yes

GitHub: https://github.com/liquity/dev.

Is there a public software repository with the code at a minimum, but normally test and scripts also (Y/N). Even if the repo was created just to hold the files and has just 1 transaction, it gets a Yes. For teams with private repos, this answer is No.

4) Is there a development history visible? (%)

> **Answer:** 100%

With 2737 commits and 42 branches, this is a robust software repo.

This checks if the software repository demonstrates a strong steady history. This is normally demonstrated by commits, branches and releases in a software repository. A healthy history demonstrates a history of more than a month (at a minimum).

Guidance:

100% Any one of 100+ commits, 10+branches
70% Any one of 70+ commits, 7+branches

50% Any one of 50+ commits, 5+branches
30% Any one of 30+ commits, 3+branches
0% Less than 2 branches or less than 10 commits

5) Is the team public (not anonymous)? (Y/N)

> **Answer:** Yes

Team members' identities are all public at https://www.liquity.org/team.

For a yes in this question the real names of some team members must be public on the website or other documentation. If the team is anonymous and then this question is a No.

Documentation

This section looks at the software documentation. The document explaining these questions is here.

Required questions are;

6) Is there a whitepaper? (Y/N)
7) Are the basic software functions documented? (Y/N)
8) Does the software function documentation fully (100%) cover the deployed contracts? (%)
9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)
10) Is it possible to trace from software documentation to the implementation in code (%)

6) Is there a whitepaper? (Y/N)

> **Answer:** Yes

Location: At the bottom of https://github.com/liquity/dev.

7) Are the basic software functions documented? (Y/N)

> **Answer:** Yes

There is robust software function documentation at https://github.com/liquity/dev#public-user-facing-functions.

8) Does the software function documentation fully (100%) cover the deployed contracts? (%)

> **Answer:** 100%

All of the Liquity smart contracts have their software functions detailed in depth at https://github.com/liquity/beta/blob/main/README.md#core-smart-contracts.

Guidance:

100% All contracts and functions documented
80% Only the major functions documented
79-1% Estimate of the level of software documentation
0% No software documentation

9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)

> Answer: 31%

Code examples are in the Appendix. As per the SLOC, there is 31% commenting to code (CtC).

The Comments to Code (CtC) ratio is the primary metric for this score.

Guidance:

100% CtC > 100 Useful comments consistently on all code
90-70% CtC > 70 Useful comment on most code
60-20% CtC > 20 Some useful commenting
0% CtC < 20 No useful commenting

How to improve this score

This score can improve by adding comments to the deployed code such that it comprehensively covers the code. For guidance, refer to the SecurEth Software Requirements.

10) Is it possible to trace from software documentation to the implementation in code (%)

> **Answer:** 100%

Clear traceability between software documentation and code implementation in https://github.com/liquity/dev#public-user-facing-functions.

Guidance:

100% Clear explicit traceability between code and documentation at a requirement level for all code
60% Clear association between code and documents via non explicit traceability

40% Documentation lists all the functions and describes their functions
0% No connection between documentation and code

Testing

This section looks at the software testing available. It is explained in this document. This section answers the following questions;

11) Full test suite (Covers all the deployed code) (%)
12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)
13) Scripts and instructions to run the tests (Y/N)
14) Report of the results (%)
15) Formal Verification test done (%)
16) Stress Testing environment (%)

11) Is there a Full test suite? (%)

> **Answer:** 100%

Code examples are in the Appendix. As per the SLOC, there is 287% test per code (TtC).

This score is guided by the Test to Code ratio (TtC). Generally a good test to code ratio is over 100%. However the reviewers best judgement is the final deciding factor.

Guidance:

100% TtC > 120% Both unit and system test visible
80% TtC > 80% Both unit and system test visible
40% TtC < 80% Some tests visible
0% No tests obvious

12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)

> **Answer:** 98%

There is an indication of code coverage in the README.md of their main GitHub repository at https://github.com/liquity/dev#coverage.

Guidance:

100% Documented full coverage
99-51% Value of test coverage from documented results
50% No indication of code coverage but clearly there is a reasonably complete set

of tests
30% Some tests evident but not complete
0% No test for coverage seen

13) Scripts and instructions to run the tests (Y/N)

> ✓ **Answer:** Yes

Test instructions are available at https://github.com/liquity/dev#running-tests.

14) Report of the results (%)

> ✓ **Answer:** 100%

A fully detailed Liquity test report is available at
https://github.com/liquity/dev/blob/main/packages/contracts/test-report.md.

Guidance:

100% Detailed test report as described below
70% GitHub Code coverage report visible
0% No test report evident

15) Formal Verification test done (%)

> ⚠ **Answer:** 0%

No Formal Verification test of Liquity was found.

16) Stress Testing environment (%)

> ✓ **Answer:** 100%

There is Rinkeby testnet testing evidence at
https://github.com/liquity/dev/blob/7e5c38eff92c7de7b366ec791fd86abc2012952c/packages/contracts/mainnetDeployment/rinkebyDeploymentOutput.json

---

Security

This section looks at the 3rd party software audits done. It is explained in this document. This section answers the following questions;

17) Did 3rd Party audits take place? (%)
18) Is the bounty value acceptably high?

17) Did 3rd Party audits take place? (%)

> **Answer:** 100%

Trails of Bits did a Liquity Proxy Contracts Report on March 5th 2021

Trails of bits delivered their Liquity Protocol and Stability Pool Final Report on March 25th 2021

Coinspect did a Liquity audit on March 30th 2021

Trails of Bits did a Liquity security assessment on January 13th 2021

Liquity was launched April 5th 2021

Guidance:

100% Multiple Audits performed before deployment and results public and implemented or not required
90% Single audit performed before deployment and results public and implemented or not required
70% Audit(s) performed after deployment and no changes required. Audit report is public
20% No audit performed
0% Audit Performed after deployment, existence is public, report is not public and no improvements deployed OR smart contract address' not found, question

18) Is the bounty value acceptably high (%)

> **Answer:** 70%

Liquity's bug bounty program is as low as $500, and as high as $250,000.

Guidance:

100% Bounty is 10% TVL or at least $1M AND active program (see below)
90% Bounty is 5% TVL or at least 500k AND active program
80% Bounty is 5% TVL or at least 500k
70% Bounty is 100k or over AND active program
50% Bounty is 100k or over
40% Bounty is 50k or over

20% Bug bounty program bounty is less than 50k
0% No bug bounty program offered

Active program means a third party actively driving hackers to the site. Inactive program would be static mention on the docs.

Access Controls

This section covers the documentation of special access controls for a DeFi protocol. The admin access controls are the contracts that allow updating contracts or coefficients in the protocol. Since these contracts can allow the protocol admins to "change the rules", complete disclosure of capabilities is vital for user's transparency. It is explained in this document. The questions this section asks are as follow;

19) Can a user clearly and quickly find the status of the admin controls?
20) Is the information clear and complete?
2`) Is the information in non-technical terms that pertain to the investments?
22) Is there Pause Control documentation including records of tests?

19) Can a user clearly and quickly find the status of the admin controls (%)

> **Answer:** 100%

Admin controls can be found at https://github.com/liquity/dev/blob/3d7c9e9e373957cd4eeb5b120e8b996dbfafff7e/README.md#contract-ownership-and-function-permissions.

Guidance:

100% Clearly labelled and on website, docs or repo, quick to find
70% Clearly labelled and on website, docs or repo but takes a bit of looking
40% Access control docs in multiple places and not well labelled
20% Access control docs in multiple places and not labelled
0% Admin Control information could not be found

20) Is the information clear and complete (%)

> **Answer:** 100%

All contracts are described as immutable at https://docs.liquity.org/faq/general#can-liquity-be-upgraded-or-changed.

Guidance:

All the contracts are immutable -- 100% OR
All contracts are clearly labelled as upgradeable (or not) -- 30% AND
The type of ownership is clearly indicated (OnlyOwner / MultiSig / Defined Roles) -- 30% AND
The capabilities for change in the contracts are described -- 30%

21) Is the information in non-technical terms that pertain to the investments (%)

> **Answer:** 100%

Guidance:

100%	All the contracts are immutable
90%	Description relates to investments safety and updates in clear, complete non-software l language
30%	Description all in software specific language
0%	No admin control information could not be found

22) Is there Pause Control documentation including records of tests (%)

> **Answer:** 100%

All contracts are automated and immutable upon launch, but no evidence of Pause Control or similar function.

Note: They do have something called "Recovery Mode" which may be relevant to this section.

Guidance:

100%	All the contracts are immutable or no pause control needed and this is explained OR
100%	Pause control(s) are clearly documented and there is records of at least one test within 3 months
80%	Pause control(s) explained clearly but no evidence of regular tests
40%	Pause controls mentioned with no detail on capability or tests
0%	Pause control not documented or explained

Appendices

Author Details

The author of this review is Rex of DeFi Safety.

Email : rex@defisafety.com Twitter : @defisafety

I started with Ethereum just before the DAO and that was a wonderful education. It showed the importance of code quality. The second Parity hack also showed the importance of good process. Here my aviation background offers some value. Aerospace knows how to make reliable code using quality processes.

I was coaxed to go to EthDenver 2018 and there I started SecuEth.org with Bryant and Roman. We created guidelines on good processes for blockchain code development. We got EthFoundation funding to assist in their development.

Process Quality Reviews are an extension of the SecurEth guidelines that will further increase the quality processes in Solidity and Vyper development.

DeFiSafety is my full time gig and we are working on funding vehicles for a permanent staff.

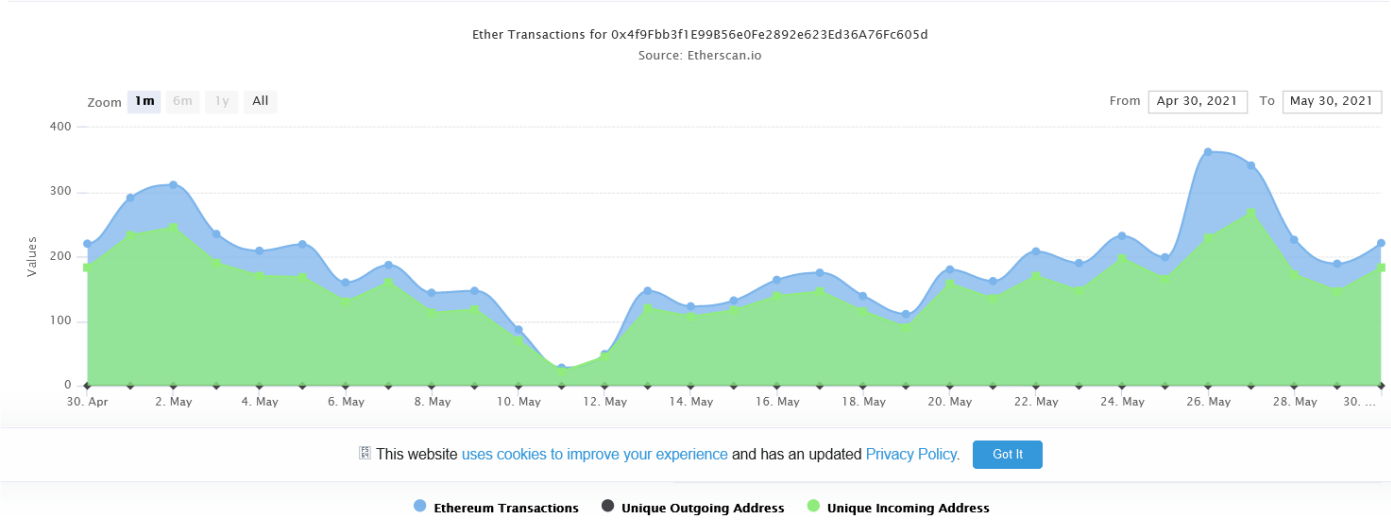
Scoring Appendix

	Total	Liquity	
PQ Audit Scoring Matrix (v0.7)	**Points**	**Answer**	**Points**
Total	**260**		248.45
Code and Team			**96%**
1) Are the executing code addresses readily available? (%)	**20**	100%	20
2) Is the code actively being used? (%)	**5**	100%	5
3) Is there a public software repository? (Y/N)	**5**	y	5
4) Is there a development history visible? (%)	**5**	100%	5
5) Is the team public (not anonymous)? (Y/N)	**15**	Y	15
Code Documentation			
6) Is there a whitepaper? (Y/N)	**5**	Y	5
7) Are the basic software functions documented? (Y/N)	**10**	Y	10
8) Does the software function documentation fully (100%) cov	**15**	100%	15
9) Are there sufficiently detailed comments for all functions w	**5**	31%	1.55
10) Is it possible to trace from software documentation to the	**10**	100%	10
Testing			
11) Full test suite (Covers all the deployed code) (%)	**20**	100%	20
12) Code coverage (Covers all the deployed lines of code, or ex	**5**	98%	4.9
13) Scripts and instructions to run the tests? (Y/N)	**5**	Y	5
14) Report of the results (%)	**10**	100%	10
15) Formal Verification test done (%)	**5**	0%	0
16) Stress Testing environment (%)	**5**	100%	5
Security			
17) Did 3rd Party audits take place? (%)	**70**	100%	70
18) Is the bug bounty acceptable high? (%)	**10**	70%	7
Access Controls			
19) Can a user clearly and quickly find the status of the admin	**5**	100%	5
20) Is the information clear and complete	**10**	100%	10
21) Is the information in non-technical terms	**10**	100%	10
22) Is there Pause Control documentation including records of	**10**	100%	10
Section Scoring			
Code and Team	50	100%	
Documentation	45	92%	
Testing	50	90%	
Security	80	96%	
Access Controls	35	100%	

Executing Code Appendix


```
{
  "chainId": 1,
  "version": "5174ecd0da4842157aba989499200d690b7e374f",
  "deploymentDate": 1617611590000,
  "bootstrapPeriod": 1209600,
  "totalStabilityPoolLQTYReward": "32000000",
  "liquidityMiningLQTYRewardRate": "0.367430922986478542",
  "_priceFeedIsTestnet": false,
  "_uniTokenIsMock": false,
  "_isDev": false,
  "startBlock": 12178551,
  "addresses": {
    "activePool": "0xDf9Eb223bAFBE5c5271415C75aeCD68C21fE3D7F",
    "borrowerOperations": "0x24179CD81c9e782A4096035f7eC97fB8B783e007",
    "troveManager": "0xA39739EF8b0231DbFA0DcdA07d7e29faAbCf4bb2",
    "collSurplusPool": "0x3D32e8b97Ed5881324241Cf03b2DA5E2EBcE5521",
    "communityIssuance": "0xD8c9D9071123a059C6E0A945cF0e0c82b508d816",
    "defaultPool": "0x896a3F03176f05CFbb4f006BfCd8723F2B0D741C",
    "hintHelpers": "0xE84251b93D9524E0d2e621Ba7dc7cb3579F997C0",
    "lockupContractFactory": "0x2eBeF24dA09489218Ba2BECb01867F6DaAeDcD4B",
    "lqtyStaking": "0x4f9Fbb3f1E99B56e0Fe2892e623Ed36A76Fc605d",
    "priceFeed": "0x4c517D4e2C851CA76d7eC94B805269Df0f2201De",
    "sortedTroves": "0x8FdD3fbFEb32b28fb73555518f8b361bCeA741A6",
    "stabilityPool": "0x66017D22b0f8556afDd19FC67041899Eb65a21bb",
    "gasPool": "0x9555b042F969E561855e5F28cB1230819149A8d9",
    "unipool": "0xd37a77E71ddF3373a79BE2eBB76B6c4808bDF0d5",
    "lusdToken": "0x5f98805A4E8be255a32880FDeC7F6728C6568bA0",
    "lqtyToken": "0x6DEA81C8171D0bA574754EF6F8b412F2Ed88c54D",
    "multiTroveGetter": "0xFc92d0E9Fa35df17E3A6d9F40716ca2cE749922B",
    "uniToken": "0xF20EF17b889b437C151eB5bA15A47bFc62bfF469"
```


Code Used Appendix



Example Code Appendix

```
// SPDX-License-Identifier: MIT

pragma solidity 0.6.11;

import "../Dependencies/BaseMath.sol";
import "../Dependencies/SafeMath.sol";
import "../Dependencies/Ownable.sol";
import "../Dependencies/CheckContract.sol";
import "../Dependencies/console.sol";
import "../Interfaces/ILQTYToken.sol";
import "../Interfaces/ILQTYStaking.sol";
import "../Dependencies/LiquityMath.sol";
import "../Interfaces/ILUSDToken.sol";

contract LQTYStaking is ILQTYStaking, Ownable, CheckContract, BaseMath {
    using SafeMath for uint;

    // --- Data ---
    string constant public NAME = "LQTYStaking";

    mapping( address => uint) public stakes;
    uint public totalLQTYStaked;

    uint public F_ETH;  // Running sum of ETH fees per-LQTY-staked
    uint public F_LUSD; // Running sum of LQTY fees per-LQTY-staked

    // User snapshots of F_ETH and F_LUSD, taken at the point at which their latest deposi
    mapping (address => Snapshot) public snapshots;

    struct Snapshot {
        uint F_ETH_Snapshot;
        uint F_LUSD_Snapshot;
    }

    ILQTYToken public lqtyToken;
    ILUSDToken public lusdToken;

    address public troveManagerAddress;
    address public borrowerOperationsAddress;
    address public activePoolAddress;

    // --- Events ---

    event LQTYTokenAddressSet(address _lqtyTokenAddress);
    event LUSDTokenAddressSet(address _lusdTokenAddress);
    event TroveManagerAddressSet(address _troveManager);
    event BorrowerOperationsAddressSet(address _borrowerOperationsAddress);
    event ActivePoolAddressSet(address _activePoolAddress);

    event StakeChanged(address indexed staker, uint newStake);
    event StakingGainsWithdrawn(address indexed staker, uint LUSDGain, uint ETHGain);
    event F_ETHUpdated(uint _F_ETH);
```

```
53      event F_LUSDUpdated(uint _F_LUSD);
54      event TotalLQTYStakedUpdated(uint _totalLQTYStaked);
55      event EtherSent(address _account, uint _amount);
56      event StakerSnapshotsUpdated(address _staker, uint _F_ETH, uint _F_LUSD);
57
58      // --- Functions ---
```

SLOC Appendix

Solidity Contracts

Language	Files	Lines	Blanks	Comments	Code	Complex
Solidity	83	12383	2408	2364	7611	551

Comments to Code 2364/7611 = 31%

Javascript Tests

Language	Files	Lines	Blanks	Comments	Code	Complex
JavaScript	33	36360	8389	6096	21875	298

Tests to Code 21875/7611 = 287%