

SMART CONTRACT CODE COMPARISON REPORT

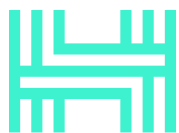


This report may contain confidential information about IT systems and the intellectual property of the Customer. This report is not meant to verify the secureness of the Customers' system. If the original system contains any security vulnerabilities, the same vulnerabilities can be present in the reviewed code.

The report can be disclosed publicly after prior consent by another Party. Any subsequent publication of this report shall be without mandatory consent.

Document

Name	Smart Contract Code Comparison Report for DCNTRL Network
Type	Staking; ERC20 token; Proxy; Pools; Lending and Borrowing system
Platform	EVM
Language	Solidity
Methodology	Link
Website	-
Changelog	26.07.2023 - Initial Review



HACKEN

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Introduction	4
Scope	4
Executive Summary	8
Difference	9
Disclaimers	10

Introduction

Hacken OÜ (Consultant) was contracted by DCNTRL Network (Customer) to conduct a Smart Contract Code Comparison. This report presents information about the conformity of a customer code with an original fork.

Scope

The scope of the project includes review and security analysis of the following smart contracts from the provided repository:

Initial review scope

Original Code	https://github.com/liquity/dev/
Original Code Commit	652331ced2474cfb9e4da11d2926bdac074be300
Forked Code	https://github.com/tenfinance/Decntral-contracts/tree/audit
Forked Code Commit	4f51760b0f08317a6145c6d5aad29b2313241441
Contracts	<p>File: Decantral/contracts/contracts/ActivePool.sol SHA3: 82686c4fc86db751ea3309f158faa4680a1f601474c29c35738a9c59c00f0f5a</p> <p>File: Decantral/contracts/contracts/BorrowerOperations.sol SHA3: 5cd4cd9b0ee629109bdf84cc93a29de76f89321c88e2638f9d50b8ee26811152</p> <p>File: Decantral/contracts/contracts/CollSurplusPool.sol SHA3: 366752cb969b4c51beafd30cb53bdbae351dcfeaa74d39fb4f56a5eb0dcd2987</p> <p>File: Decantral/contracts/contracts/DefaultPool.sol SHA3: 4a4ea8fea9d61f0ced9d204a75ee8afe93d583704627cab83008d2f2530ff3b9</p> <p>File: Decantral/contracts/contracts/GasPool.sol SHA3: 8a2b3b9dcd2b2fe1d43f3f94782dd2396bf305348b7ba546ee8e39f16a8ab7e7</p> <p>File: Decantral/contracts/contracts/HintHelpers.sol SHA3: 5c4a51ce740afd13280b867ca1a80b476163f125523e71aa180e8350e604c36f</p> <p>File: Decantral/contracts/contracts/LUSDToken.sol SHA3: e4de3538cb1be424ce8f80a024d1e4b8b3c5b3a7c35b8b3a158468bdbb23c398</p> <p>File: Decantral/contracts/contracts/Migrations.sol SHA3: e266c46d04ec769b4550eaa5dc2155f6017b387f131c794611bbc83e8a107942</p> <p>File: Decantral/contracts/contracts/MultiTroveGetter.sol SHA3: f61176ddbadd2030ee9bc5a9f3bd58a3c54cf58fcc468416f3a3721cefa77da</p> <p>File: Decantral/contracts/contracts/PriceFeed.sol SHA3: 8ea9da9309ef7837b6e75cf71681b4ff19db8e9c4b6fdbce37481d1ea38c852c</p> <p>File: Decantral/contracts/contracts/SortedTrove.sol SHA3: 2db461f8cd5a56f177c1418bd644501635c8b4a89179259c67bbfe3de69fd928</p> <p>File: Decantral/contracts/contracts/StabilityPool.sol SHA3: cfbc9150920d72f2f4d39a1230df9ead5703632e29eb54b13ab489c0abe4d796</p>

<p>File: Decantral/contracts/contracts/TroveManager.sol SHA3: 6d683bf153d6823d84bf9a77eb03c16800a9a49aea60cb3ad5d1c38b0b861c42</p> <p>File: Decantral/contracts/contracts/Dependencies/AggregatorV3Interface.sol SHA3: 20053c8ab2e4fa2989e820b38348f1d62f22a9e9f5d9b812d5238c6f314bc99d</p> <p>File: Decantral/contracts/contracts/Dependencies/BaseMath.sol SHA3: ac70420f08054d851315ead0fe4e615891466c0ca436df191a328fc062a2a6b5</p> <p>File: Decantral/contracts/contracts/Dependencies/CheckContract.sol SHA3: c865abf71b573a7bb223b2cf5643ba32b481a9b06502bdc3535d95425d19e4ca</p> <p>File: Decantral/contracts/contracts/Dependencies/console.sol SHA3: 4b403eaa84e057afe3e75dd5fdca7f7130235d27548378d2ea2588397003c0f7</p> <p>File: Decantral/contracts/contracts/Dependencies/IERC20.sol SHA3: d292fd04b9cd5081fef856aa13c313502afe51063814881b35d21f94e846e6f</p> <p>File: Decantral/contracts/contracts/Dependencies/IERC2612.sol SHA3: e7d06b91184926445f3c652f3b6b6db843010490832548d0295e810e745206e5</p> <p>File: Decantral/contracts/contracts/Dependencies/ITellor.sol SHA3: b9f0533221ad331a513a8a0633e6778dd899967998096b158b3479df33d28b3e</p> <p>File: Decantral/contracts/contracts/Dependencies/LiquidityBase.sol SHA3: fbef5bf37c095039f54bfdc098056e7b71bdd9bf21c1db374c9097873035ee3a</p> <p>File: Decantral/contracts/contracts/Dependencies/LiquidityMath.sol SHA3: 183da240e3616e79d6f793d6b25785d248922a520c48eaf5341e2530ca759926</p> <p>File: Decantral/contracts/contracts/Dependencies/LiquiditySafeMath128.sol SHA3: 787c493db547cc6f2198cbc8c5171ff0712d48e4695ca325a3c467f9561d6aef</p> <p>File: Decantral/contracts/contracts/Dependencies/Ownable.sol SHA3: 943072ab79269f30e20878bde01b4c8105c3162bdbcd398e312a6610588fcdab</p> <p>File: Decantral/contracts/contracts/Dependencies/SafeMath.sol SHA3: 682e2cb6211f15be5bedcd8c7fde4308333edc138b659e2d7e2d1afe18dcb06f</p> <p>File: Decantral/contracts/contracts/Dependencies/TellorCaller.sol SHA3: b0a2c148751e716b5bef24bb16575f6c7955a63350c0253e56084a69ed1b4184</p> <p>File: Decantral/contracts/contracts/Integrations/LUSDUdToLUSDEth.sol SHA3: 0b30edc8f0f61ad336c3a5b09956c4328be2f2091773a05b51822482941c5ae6</p> <p>File: Decantral/contracts/contracts/Interfaces/IActivePool.sol SHA3: 6db1ac5ddefd570bbd26e1c2c879008877db8619872644896318fdafa3a187a4</p> <p>File: Decantral/contracts/contracts/Interfaces/IBorrowerOperations.sol SHA3: 95970b09900ccf8915206e9e24ed0accf4d916dc2a9c4e479a7033a45e970ab5</p> <p>File: Decantral/contracts/contracts/Interfaces/ICollSurplusPool.sol SHA3: d00693699d8b8c3846642159500ee7535972516c35ef68b3b8bd833331522d64</p> <p>File: Decantral/contracts/contracts/Interfaces/ICommunityIssuance.sol SHA3: a4488ab8b853c6509d57e4ac48ff6f13da1ca18bbced1528c1b416a37c413425</p> <p>File: Decantral/contracts/contracts/Interfaces/IDefaultPool.sol SHA3: 6984e1fcab40c39fde6c9d3269869805ce35faf2758d5e71baa2e7ab232f13d2</p>

<p>File: Decantral/contracts/contracts/Interfaces/ILiquidityBase.sol SHA3: b900239ed716313a9eb5c3eba128f83c5814ea85eeb9c4280858ffdf50c547b7</p> <p>File: Decantral/contracts/contracts/Interfaces/ILockupContractFactory.sol SHA3: d095732a475adc51fb9df334296fb658967433fc8ec93e18efee7e0742d102da</p> <p>File: Decantral/contracts/contracts/Interfaces/ILQTYStaking.sol SHA3: 698579d937bd2ec83ab9d016f5ffdf361c09e63ff7177605cd3dfb72ecf5d4f1</p> <p>File: Decantral/contracts/contracts/Interfaces/ILQTYToken.sol SHA3: e5b70c1529e631bd827b79e8913a4d1f60b345fefbae71e4ca52dac5334ef205</p> <p>File: Decantral/contracts/contracts/Interfaces/ILUSDToken.sol SHA3: b795934d9fa46ebdfed7826d1e21e54c8fbab9b5249e064982faaf2d560584ff</p> <p>File: Decantral/contracts/contracts/Interfaces/IPool.sol SHA3: 7d3c21683d3b760d7d4b5e9afa3f6000a3a7d24ab4e28c4263cc74d9fc4e3cf3</p> <p>File: Decantral/contracts/contracts/Interfaces/IPriceFeed.sol SHA3: 8d48df3a41c673b5d2a6436eae6f1f43aac0da4171c464cadee605554c75bcc</p> <p>File: Decantral/contracts/contracts/Interfaces/ISortedTrove.sol SHA3: de33e496aa9229850220d9a78f9014331a2e8aec4570ca20253b4e6505947364</p> <p>File: Decantral/contracts/contracts/Interfaces/IStabilityPool.sol SHA3: 56681153ca0f9eccf3e5b1705d327490fa168addfd9e5acfb0c87b57377fe7b3</p> <p>File: Decantral/contracts/contracts/Interfaces/ITellorCaller.sol SHA3: fc029867ad983bdc13f83bfa0b41e8af1c43d5f897acd64c02b54d3f1292df6a</p> <p>File: Decantral/contracts/contracts/Interfaces/ITroveManager.sol SHA3: 69198a8f864358fef8e478835dbf014a3185e7afa8088c805ff4c79ea4c18fe8</p> <p>File: Decantral/contracts/contracts/LPRewards/Unipool.sol SHA3: 597e8f160bb89e8e9558a40461f94218e40b4a454d48a3564761d0c9c03452bb</p> <p>File: Decantral/contracts/contracts/LPRewards/Dependencies/Address.sol SHA3: 166f169f68491a5e28a30490adee9a5d9c87e017d52a8cca4c7125f586d2954c</p> <p>File: Decantral/contracts/contracts/LPRewards/Dependencies/SafeERC20.sol SHA3: 7700b58cfcb402f5102c83aaa131492fd371196cf5ec229f004c534ceabb1a38</p> <p>File: Decantral/contracts/contracts/LPRewards/Interfaces/ILPTokenWrapper.sol SHA3: 9fef251ed05da75b7086c016a8adeb0a12df72e55db5f15c16f9f604a6347e3e</p> <p>File: Decantral/contracts/contracts/LPRewards/Interfaces/IUnipool.sol SHA3: d57c99e11d3a5658033c83aea7e35834603a5d064c46f7d6500b4c27e752954a</p> <p>File: Decantral/contracts/contracts/LQTY/CommunityIssuance.sol SHA3: 624c3f4522e6eaa43b0eb6593d9e9d1a1c8171e79d52693bda49a289495382fc</p> <p>File: Decantral/contracts/contracts/LQTY/LockupContract.sol SHA3: 61b49620fba90f5767488122224d350a2f42dee04e0811fb6ae548ec1b8ba3f7</p> <p>File: Decantral/contracts/contracts/LQTY/LockupContractFactory.sol SHA3: 1f054c2326f8178ef55ae30062fd654ed2dbd0c7ca5f98d45f1967eeddef216d</p> <p>File: Decantral/contracts/contracts/LQTY/LQTYStaking.sol SHA3: 14b2a2bb235002d3712e079182787b23b12d0a215b42ef8e93c0aadb56e1b717</p>
--

File: Decantral/contracts/contracts/LQTY/LQTYToken.sol SHA3: 5b2a6ee64e95b9a5cf6020763b0cbbd9cff55661cab444d80aa176b805510196
File: Decantral/contracts/contracts/Proxy/BorrowerOperationsScript.sol SHA3: f0382ce2145e870e1ebcf6d11a66a922216c6ee4f59b53544378d6fb373251be
File: Decantral/contracts/contracts/Proxy/BorrowerWrappersScript.sol SHA3: c6f7eff24b023e5e3967cefe5ef9f42daebdb0f6a408c591687355c6c0231c28
File: Decantral/contracts/contracts/Proxy/ETHTransferScript.sol SHA3: 7ed66ac4962c62410879b10692f488cb3f42326c9c461b103cf8b05973bf0286
File: Decantral/contracts/contracts/Proxy/LQTYStakingScript.sol SHA3: c8cc14cf625b0ff58c73092ea121d6a66e13e7475018560bd4da1632c7e5f9ad
File: Decantral/contracts/contracts/Proxy/StabilityPoolScript.sol SHA3: bfdb48f1dfc0552291a24d7a03f3461e2315089ac3d03ef21b1f6664c2c404c1
File: Decantral/contracts/contracts/Proxy/TokenScript.sol SHA3: 70de8408b2b91b4bc32187420fb2c6b4189efb6d1d9946436ecb37286bad6685
File: Decantral/contracts/contracts/Proxy/TroveManagerScript.sol SHA3: de8814041c33b1edbfac22d8c0c920f3ab49a64a346bccd09400cf274a30bda7

Executive Summary

The customer code is intended to be a fork of Liquidity protocol. All the differences, if any, are mentioned in the Difference section of the report, and their secureness and correctness cannot be guaranteed by this review.

Summary

The code is an exact copy of the Liquidity protocol.
During the review, auditors found no differences between the source of the fork (original repo) and the fork itself.



Difference

No difference between the original contracts and forked contracts found.

Disclaimers

Hacken Disclaimer

The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the Consultant cannot guarantee the explicit security of the audited smart contracts.