Quantstamp Security Assessment Certificate

January 13th 2021 — Quantstamp Verified

AlphaHomoraV2

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

Executive Summary

Type	Leveraged yield farming and liquidity providing
Auditors	Poming Lee, Research Engineer Luís Fernando Schultz Xavier da Silveira, Security Consultant Jose Ignacio Orlicki, Senior Engineer
Timeline	2020-12-02 through 2021-01-13
EVM	Muir Glacier
Languages	Python, Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Alpha Homora v2 (hackmd readme1) Alpha Homora v2 (hackmd readme2)

Source Code

Repository	Commit
homora-v2	16a6f9a
homora-v2	f70942d

Goals

• Do functions have proper access control logic?

• Are there centralized components of the system which users should be aware?

• Do the contracts adhere to best practices?

Total Issues	**15** (11 Resolved)
High Risk Issues	**4** (4 Resolved)
Medium Risk Issues	**2** (2 Resolved)
Low Risk Issues	**4** (2 Resolved)
Informational Risk Issues	**4** (2 Resolved)
Undetermined Risk Issues	**1** (1 Resolved)

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
Undetermined	The impact of the issue is uncertain.
Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

Quantstamp has performed a security audit of the AlphaHomoraV2 project. During auditing, we found fifteen potential issues of various levels of severity: four high-severity issues, two medium-severity issues, four low-severity issues, four informational-severity findings, and one undetermined-severity finding. We also made eleven best practices recommendations. Overall, the code comment is good for this project. The documentation of the project is insufficient and the quality of the audit could be largely improved if there were more specifications that describe all the intended behaviors and precision requirements. Also, the inclusion of extensive tests and/or formal methods to assure extensive quality and behavior could also help. Normally attackers would use fuzzing techniques to find holes in any smart contract logic with substantial value locked. Avoid implementing your own arithmetic like fixed-point arithmetic, use existing implementations or standards is also advantageous to help increase the security. The Solidity Coverage does not work due to the project setup. We strongly recommend the Alpha team to find a way to fix this and obtain a code coverage report that states that all the code coverage values are at least 90% before go live, to reduce the potential risk of having functional bugs in the code. To summarize, given the dense logic, many integrations, oracle logic, borrowing, many new features and sparse documentation there are very likely still issues that we are not able to find. Quantstamp has on a best efforts basis identified 15 total issues, with 3 auditors performing audits side-by-side, however we highly suggest getting more reviews before launching v2. In particular we suggest writing many more tests, and checking for edge cases with the business logic, especially around the integrations.
disclaimer: The project scope. Quantstamp was requested to only audit `HomoraBank.sol`, everything in the `oracle` folder, and everything in the `spell` folder.
2021-01-13 update: during this reaudit, Alpha team has either brought the status of findings into fixed or acknowledged. A number of new files were added to this commit and not included in the scope of the audit. It is worth noting that there is still no unit tests and no coverage report for this project.

ID	Description	Severity	Status
QSP-1	[false positive] Missing checks to the health of a position when a borrower is borrowing	High	Fixed
QSP-2	[false positive] Missing checks to the health of a position when a borrower is withdrawing collateral	High	Fixed
QSP-3	Incorrect `share` calculation in function `borrow`	High	Fixed
QSP-4	Oracle attack is possible by manipulating a Uniswap pool	High	Fixed
QSP-5	Function `liquidate` never clears up the collateral value in the liquidated position	Medium	Fixed
QSP-6	Truncation of fixed-point could result in sensitive collateral liquidation calculation	Medium	Fixed
QSP-7	No fallback oracle if primary fails.	Low	Acknowledged
QSP-8	`HomoraBank` may not be able to return borrowed funds to integrated lending protocols during flash crash	Low	Acknowledged
QSP-9	Potentially high gas usage in `getBorrowETHValue`	Low	Fixed
QSP-10	Attacker can front-run initialization of new HomoraBank	Low	Mitigated
QSP-11	Privileged Roles	Informational	Acknowledged
QSP-12	Transmit arbitrary amount of token from a position owner to a spell contract and get locked	Informational	Acknowledged
QSP-13	Missing approval in function `setCToken`	Informational	Fixed
QSP-14	Missing input checks	Informational	Fixed
QSP-15	Integer Overflow / Underflow	Undetermined	Fixed

Quantstamp Audit Breakdown

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

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

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

Methodology

The Quantstamp auditing process follows a routine series of steps:

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

Toolset

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

Setup

Tool Setup:

- Truffle v5.1.33
- SolidityCoverage v0.7.11
- Mythril v0.22.10
- Slither v0.6.12

Steps taken to run the tools:

1. Installed Truffle: `npm install -g truffle`
2. Installed the solidity-coverage tool (within the project's root directory): `npm install --save-dev solidity-coverage`
3. Ran the coverage tool from the project's root directory: `./node_modules/.bin/solidity-coverage`
4. Installed the Mythril tool from Pypi: `pip3 install mythril`
5. Ran the Mythril tool on each contract: `myth a path/to/contract`
6. Installed the Slither tool: `pip install slither-analyzer`
7. Run Slither from the project directory: `slither .s`

Findings

QSP-1 [false positive] Missing checks to the health of a position when a borrower is borrowing

Severity: *High Risk*

Status: Fixed

Description: `contracts/HomoraBank.sol`: function `borrow` should check that `collateralValue > borrowValue` right after transferring the borrowed token out of the contract.

QSP-2 [false positive] Missing checks to the health of a position when a borrower is withdrawing collateral

Severity: *High Risk*

Status: Fixed

Description: `contracts/HomoraBank.sol`: function `takeCollateral` should check `require(collateralValue > borrowValue, 'position still healthy');` right after transferring the collateral out of the contract.

QSP-3 Incorrect `share` calculation in function `borrow`

Severity: *High Risk*

Status: Fixed

Description: `L355` in `contracts/HomoraBank.sol`, should be `amount.mul(totalShare).div(totalDebt)` instead of `amount.mul(totalDebt).div(totalShare)`.

QSP-4 Oracle attack is possible by manipulating a Uniswap pool

Severity: *High Risk*

Status: Fixed

Description: Uniswap oracle (https://uniswap.org/docs/v2/core-concepts/oracles/) aggregates prices from all the blocks weighted by block time into cumulative prices whereas Keep3r oracle takes 30-minute samples of Uniswap cumulative prices. The price calculations (i.e., function `price0TWAP` and `price1TWAP`) in `contracts/oracle/BaseKP3ROracle.sol` calculates the sample provided by Keep3r with a last-minute (`now`) spot price from Uniswap. This is fine as long as the accumulation weight is okay, but under heavy congestion and delays the weight (i.e., `timeElapsed` in function `currentPx0Cumu` and `currentPx1Cumu`) can be too big. And together with the (`IUniswapV2Pair(pair).getReserves()`) in `BaseKP3ROracle`, this platform could be attacked by flash loans. Several recent attacks were documented in https://samczsun.com/so-you-want-to-use-a-price-oracle/.
2020-12-18 update: Alpha team stated that only LP tokens will be used as collateral, so the price data eventually used will not be influenced by a flash-loan attack.

Exploit Scenario: Force liquidation with a flash loan attack. The attack is completed within one transaction.

1. So say a victim Alice borrows a token `T` on `UniswapV2SpellV1`.
2. The attacker Bob takes a flash loan of `N` ETH.
3. Bob buys an amount of token `T`.
4. The price of token `T` rises instantly on Uniswap.
5. `BaseKP3ROracle` from v2 is sensitive to price variations and inputs prices to `HomoraBank` to decide about under-collateralization.
6. Alice's position is underwater and can be liquidated instantly.
7. Bob liquidates the victim's position, taking a profit from discounted liquidation price.
8. Bob sells the amount of tokens `T`.
9. Bob returns the flash loan and finishes the attack.

Recommendation: Use only observations on the Keep3r oracle, use more data points, and do not fine-tune the oracle with current prices.

QSP-5 Function `liquidate` never clears up the collateral value in the liquidated position

Severity: *Medium Risk*

Status: Fixed

Description: In `contracts/HomoraBank.sol`, the function `liquidate` never clears up the collateral value in the liquidated position. With the function `takeCollateral` in its form currently, this could cause fund loss.
2020-12-18 update: Alpha team enables the function to subtract the collateral value with the bounty provided after a position being liquidated. Quantstamp would like to further suggest to consider to directly assign zero to the collateral value when bounty is larger than the collateral value of a position, in order to avoid unexpected failure of liquidation due to the line `pos.collateralSize = pos.collateralSize.sub(bounty);`.
2021-01-13 update: this one is fixed in https://github.com/AlphaFinanceLab/homora-v2/commit/233de49b1e4ec0158861b611de153bf95dcf4aab.

Recommendation: Clear up the collateral value after a position being liquidated.

QSP-6 Truncation of fixed-point could result in sensitive collateral liquidation calculation

Severity: *Medium Risk*

Status: Fixed

Description: `contracts/oracle/ProxyOracle.sol`: multiplication is performed after a truncation division in a series of integer calculations. This leads to miscalculation and will lead to a financial loss over time or cause unexpected results. For instance, `contracts/oracle/ProxyOracle.sol`: `L77`, `L89-L90`, and `L96-L97`. In addition, taking function `asETHCollateral()` as an example:

1. getETHPx() = 100.5 and amount = 0.05.
2. Before truncation = 50.25
3. After truncation = 50.00
4. collateralFactor = 10,000
5. Final value = 50.000 and value lost close to 0.5% from original 50.25

2020-12-18 update: Alpha team stated that it is intended. The deviation is bounded by `borrowFactor`/10000 (in wei). The maximum value for `borrowFactor` value will be in the order of 10^6, bounding the error by ~100 wei, which will be less than a block's interest accrued.

Recommendation: Examine the influence of precision loss to the position health check carefully. Make sure to perform multiplications before the divisions. In addition, could make use of standard fixed-point libraries to enlarge the precision as much as possible. There is no native or favorite standard implementation yet. OpenZeppelin has future plans to include one but there are a few current widely-used libraries. Reference:

- Discussion in forum https://forum.openzeppelin.com/t/designing-fixed-point-math-in-openzeppelin-contracts/2499.
- FixidityLib (https://github.com/CementDAO/Fixidity)
- ABDK (https://github.com/abdk-consulting/abdk-libraries-solidity)
- DecimalMath (https://github.com/HQ20/contracts/tree/master/contracts/math). Also, check the results provided by Slither below:

```
UniswapV2SpellV1._optimalDepositA(uint256,uint256,uint256,uint256) (spell/UniswapV2SpellV1.sol#70-86) performs a multiplication on the result of a division:
        -c = _c.mul(1000).div(amtB.add(resB)).mul(resA) (spell/UniswapV2SpellV1.sol#80)
ProxyOracle.convertForLiquidation(address,address,uint256,uint256) (oracle/ProxyOracle.sol#63-78) performs a multiplication on the result of a division:
        -amountOut = amountIn.mul(oracleIn.source.getETHPx(tokenIn)).div(oracleIn.source.getETHPx(tokenOutUnderlying)) (oracle/ProxyOracle.sol#73-76)
        -amountOut.mul(oracleIn.liqIncentive).mul(oracleOut.liqIncentive).div(10000 * 10000) (oracle/ProxyOracle.sol#77)
ProxyOracle.asETHCollateral(address,uint256,uint256) (oracle/ProxyOracle.sol#81-91) performs a multiplication on the result of a division:
        -ethValue = oracle.source.getETHPx(tokenUnderlying).mul(amount).div(2 ** 112) (oracle/ProxyOracle.sol#89)
        -ethValue.mul(oracle.collateralFactor).div(10000) (oracle/ProxyOracle.sol#90)
ProxyOracle.asETHBorrow(address,uint256) (oracle/ProxyOracle.sol#94-98) performs a multiplication on the result of a division:
        -ethValue = oracle.source.getETHPx(token).mul(amount).div(2 ** 112) (oracle/ProxyOracle.sol#96)
        -ethValue.mul(oracle.borrowFactor).div(10000) (oracle/ProxyOracle.sol#97)
```

QSP-7 No fallback oracle if primary fails.

Severity: *Low Risk*

Status: Acknowledged

Description: If Keep3r workers stop updating their oracles due to on-chain or off-chain problems, or any of those services is killed by their organizations, `BaseKP3ROracle` has no alternative source of prices and most services of `HomoraBank` such as main `execute()` service stops working.
2020-12-18 update: Alpha team stated that they will add a secondary oracle later.

Recommendation: Add fail-safe mechanism, secondary oracle, or even calculate price data based on the results gathered from multiple data sources.

QSP-8 `HomoraBank` may not be able to return borrowed funds to integrated lending protocols during flash crash

Severity: *Low Risk*

Status: Acknowledged

Description: During a flash crash, the price of assets drop suddenly. Under this condition, the liquidators might not be fast enough (or incentivized enough) to liquidate the collaterals. Even eventually the liquidators successfully liquidate all the collaterals, the liquidation price could be very low and the amount of borrowed token being repaid could be unexpectedly small. This might cause `HomoraBank` contract to hold insufficient amounts of borrowed tokens that can be used to repay the debt.
2020-12-18 update: Alpha team stated that collateral and borrow factor will be set appropriately in order to serve as a buffer when price drops suddenly.

Recommendation: Auto-liquidation mechanism could be developed to mitigate this risk. Reference: https://app.nuo.network/

QSP-9 Potentially high gas usage in `getBorrowETHValue`

Severity: *Low Risk*

Status: Fixed

Description: Potentially high gas usage in `getBorrowETHValue` as the number of banks (i.e., supported tokens) increases.
2020-12-18 update: Alpha team fixes this issue by using a bitmap to iterate over banks debt.

Recommendation: A solution is to make `debtShareOf` into a linked list of its non-zero entries.

```
 // Example
struct Node {
uint debt;
address previous;
address next;
}
struct Position {
    …
mapping(address => Node) debtShareOf;
}
```

QSP-10 Attacker can front-run initialization of new HomoraBank

Severity: *Low Risk*

Status: Mitigated

Description: In `contracts/HomoraBank.sol`: any two calls to `initialize()` depend on ordering. The first caller becomes the governor, an attacker can front-run any HomoraBank initialization and cause a Denial-of-Service.
2020-12-18 update: Alpha team stated that they will deploy the contract and finish the initialization within one transaction.

Recommendation: If upgrades to this contract are planned, use widely-used or standard libraries for upgradeability. Don't manually deploy new versions.

QSP-11 Privileged Roles

Severity: *Informational*

Status: Acknowledged

Description: (a) The `governor` of contract `contracts/HomoraBank.sol` can use the function `withdrawReserve` to withdraw any amount of tokens from the contract. (c) The `governor` of contract `contracts/oracle/ProxyOracle.sol` can manipulate the price oracles that are used in the system, at any time. (b) The `governor` of contract `contracts/oracle/SimpleOracle.sol` can manipulate the price data used in the system, at any time.
2020-12-18 update: Alpha team stated that they will communicate this information with end-users.

Recommendation: These privileged operations and their potential consequences should be clearly communicated to (non-technical) end-users via publicly available documentation.

QSP-12 Transmit arbitrary amount of token from a position owner to a spell contract and get locked

Severity: *Informational*

Status: Acknowledged

Description: `contracts/HomoraBank.sol`: function `transmit` can be called by a position owner through the function `HomoraCaster.cast` and transfer any amount of token to the `target` address specified when calling `HomoraCaster.cast()`. Users could lose their fund if there are no methods in the destination spell contract that can send the asset back.
2020-12-18 update: Alpha team stated that they will communicate the best practice of writing good spells with end-users, and make sure the ones provided by Alpha team will be audited.

QSP-13 Missing approval in function `setCToken`

Severity: *Informational*

Status: Fixed

Description: `contracts/HomoraBank.sol`: function `setCToken` should `safeApprove` the newly added `cToken`.

QSP-14 Missing input checks

Severity: *Informational*

Status: Fixed

Description: `contracts/HomoraBank.sol`: function `initialize` should check if `IOracle _oracle` is not `0x0`.

QSP-15 Integer Overflow / Underflow

Severity: *Undetermined*

Status: Fixed

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

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

`SafeMath` was not enforced for arithmetic operations. This would greatly increase the chances of this dapp having underflow/overflow issues and lead to unexpected results. For instance, in `BaseKP3ROracle.sol`, `L28`, `L32`, `L35`, `L44`, `L48`, `L51`, `L61`, `L62`, and `L73`.
2020-12-18 update: Alpha team considered there is no need for using library `SafeMath` for the operations pointed out, and the overflow is intended by design. In addition, QuantStamp would also like to point out that `L57` could conceivably overflow in the future (year 2038 problem).
2021-01-13 update: It is confirmed that for `L55` the `uint32` overflow is an expected behavior. See https://uniswap.org/whitepaper.pdf section 2.2.1 for more details.

Recommendation: Consider using the `SafeMath` library for all of the arithmetic operations

Automated Analyses

Mythril

Mythril reported no issues.

Slither

- Slither reported some reentrancy findings. After examining by QuantStamp they are determined as false positives.
- Slither listed the precision issues that could be improved through changing the orders, as mentioned in our findings.
- Slither suggested that several functions could be declared as external, as mentioned in our findings:

Code Documentation

For the code comments, we suggest several improvements:

1. [fixed] Consider adding explanations to the formula in `L77`-`L85` of `contracts/spell/UniswapV2SpellV1.sol` in order to check if this implementation sticks to the specification.
2. [fixed] `contracts/HomoraBank.sol`: `L144`, `L162`: "the list" -> "a list".
3. [fixed] `contracts/HomoraBank.sol`: `L320`: "execution" -> "execute".
4. [fixed] `contracts/HomoraBank.sol`: `L346`: typo "tha".
5. [fixed] `BasicSpell.sol`: `L107`: there is an extra "bank".
6. [fixed] `BasicSpell.sol`: `L97`, `L107`: missing "@param" for the token argument.

Adherence to Best Practices

The code does not fully adhere to best practices. In particular:

1. [fixed] Consider adding checks to make sure that the `cToken`s are all distinct. Although `cToken`s are set by the governor, this could be done by accident and could lead to catastrophic results whenever two `bank`s share a same `cToken` and messes up the debt calculation for both `bank`s. This is because both `bank`s would be borrowing from the same `cToken` and the `cToken` is consulted to set the `bank`s' `totalDebt`.

2. [fixed] `contracts/HomoraBank.sol`: function `repayInternal`, consider also performing `amountCall = oldDebt` when `amountCall` is larger than `oldDebt` to avoid `revert` under this condition.

3. [fixed] `contracts/spell/UniswapV2SpellV1.sol`: function `removeLiquidity` in `L182-L190`, consider also performing the assignments of `amtARepay`, `amtBRepay`, and `amtLPRepay` when the argument input is larger than the borrowed balance to avoid `revert` under this condition.

4. [acknowledged] `contracts/spell/BasicSpell.sol` does not have a permission check to function `ensureApprove`. This is acceptable since the Alpha team claimed that all assets should not be stored inside a spell contract. However, in reality this design has not been enforced by code because according to the Alpha team they want end users to design their own spell contracts without any limitation. This will introduce additional risk vectors that need to be taken into consideration.

5. [acknowledged] Should always be very careful about the whitelisted collateral tokens. The price data can be very easily manipulated if the oracle is based on a Uniswap liquidity pool data and the liquidity is very small (or small enough). And this could lead to catastrophic results.

6. [fixed] `contracts/HomoraBank.sol`: Consider checking that the bank exists in `withdrawReserve`

7. [fixed] `contracts/HomoraBank.sol`: Consider checking that the position is active in `liquidate`.

8. [fixed] The event `SetETHPx` of `SimpleOracle.sol` is never emitted.

9. [acknowledged] Spells calling `safeApprove()` with biggest integer `uint(-1)` approval is not a good pattern for security. New Spells extensions in the future might need approval for a limited amount of tokens to be safe. And should decrease the allowance whenever that allowance is not needed any more.

10. [fixed] `contracts/HomoraBank.sol`: consider checking `Position.collToken != 0x0` in the following functions: `liquidate`, `getCollateralETHValue`, `execute`.

11. [fixed] Consider using `external` declaration for functions not used in other functions. Functions only called externally by other contracts or users can be only declared as `external`, gas is saved and attackers are given less internal functions and control in case of vulnerabilities. This way they cannot be called from other `internal` or `public` functions. For instance, 1) `setPendingGovernor()` and `acceptGovernor()` in `/contracts/Governable.sol`, 2) `initialize()` in `/contracts/HomoraBank.sol`: `/contracts/interfaces/IKeep3rV1Oracle.sol`: `WETH()`, and 3) `factory()` in `/contracts/interfaces/IKeep3rV1Oracle.sol`. Consider also checking the results provided by Slither below:

```
supportsInterface(bytes4) should be declared external:
        - ERC165.supportsInterface(bytes4) (OpenZeppelin/openzeppelin-contracts@3.2.0/contracts/introspection/ERC165.sol#35-37)
setCompleted(uint256) should be declared external:
        - Migrations.setCompleted(uint256) (Migrations.sol#16-18)
initialize(IOracle,uint256) should be declared external:
        - HomoraBank.initialize(IOracle,uint256) (HomoraBank.sol#103-115)
WETH() should be declared external:
        - IKeep3rV1Oracle.WETH() (interfaces/IKeep3rV1Oracle.sol#10)
factory() should be declared external:
        - IKeep3rV1Oracle.factory() (interfaces/IKeep3rV1Oracle.sol#12)
balanceOfBatch(address[],uint256[]) should be declared external:
        - ERC1155.balanceOfBatch(address[],uint256[]) (OpenZeppelin/openzeppelin-contracts@3.2.0/contracts/token/ERC1155/ERC1155.sol#98-117)
setApprovalForAll(address,bool) should be declared external:
        - ERC1155.setApprovalForAll(address,bool) (OpenZeppelin/openzeppelin-contracts@3.2.0/contracts/token/ERC1155/ERC1155.sol#122-127)
safeTransferFrom(address,address,uint256,uint256,bytes) should be declared external:
        - ERC1155.safeTransferFrom(address,address,uint256,uint256,bytes) (OpenZeppelin/openzeppelin-contracts@3.2.0/contracts/token/ERC1155/ERC1155.sol#139-166)
safeBatchTransferFrom(address,address,uint256[],uint256[],bytes) should be declared external:
        - ERC1155.safeBatchTransferFrom(address,address,uint256[],uint256[],bytes) (OpenZeppelin/openzeppelin-contracts@3.2.0/contracts/token/ERC1155/ERC1155.sol#171-207)
setPendingGovernor(address) should be declared external:
        - Governable.setPendingGovernor(address) (Governable.sol#22-24)
acceptGovernor() should be declared external:
        - Governable.acceptGovernor() (Governable.sol#27-31)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-as-external
```

Test Results

Test Suite Results

No unit tests, only functional tests on brownie mainnet-fork. One out of 12 functional tests failed.

2021-01-14 update: Alpha Team stated that the failures from these test cases are possibly due to inconsistent contract name in test scripts and top token holder change (the script depends on top token holders to set up initial user funds for testing). These failures do not affect the core logic of the tests and are fixed in later commits.

```
Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'uniswap_spell_eth_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462815   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462816   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0x1ebc59c18f9a5055c0716b447bb88b1eaa47cc00276d4ae17a9d34677fa503e2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  SimpleOracle.setETHPx confirmed - Block: 11462817   Gas used: 38057 (0.32%)


Transaction sent: 0x6c91272d1e90416a862a2a1078a868ce3178139d7d96a3c4bcdb7dfd394972fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  ProxyOracle.constructor confirmed - Block: 11462818   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0x4856a201ead1f639457d2a0f785d38c5ef9ec921e6e0e0401f094aa8d6bfc089
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462819   Gas used: 31221 (0.26%)


Transaction sent: 0x7009c041cb8b44c67c5ece3a0bc8a2e10b5bfeddbb04a9b23273d71c3dbf0fb2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  UniswapV2Oracle.constructor confirmed - Block: 11462820   Gas used: 384200 (3.20%)
  UniswapV2Oracle deployed at: 0x6b4BDe1086912A6Cb24ce3dB43b3466e6c72AFd3


Transaction sent: 0x0b05cc58b11a7d91637e88135ec930f8c247b749090198cdc3ac702d45816ad2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  ProxyOracle.constructor confirmed - Block: 11462821   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9
```

```
Transaction sent: 0xdcd3f1e318654223e624c7e99290b66229f1c4f4fb5dd0c80e7d27ca11f408a5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462822   Gas used: 31221 (0.26%)


Transaction sent: 0x5c2009eef35f87ffe5adafea4790d4a782edc193275de2a6fdd56f6c0bd172a9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  ProxyOracle.setOracles confirmed - Block: 11462823   Gas used: 56847 (0.47%)


Transaction sent: 0xb714d7c0888a739ce9a7dc616c8cc9cbedb1565373887681864742a38ce5b1c3
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  HomoraBank.constructor confirmed - Block: 11462824   Gas used: 3700237 (30.84%)
  HomoraBank deployed at: 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472


Transaction sent: 0x1b1e4b5d9674dfbe391cc5a1e7697fc0fdfa085ec073775da35f274c3e4b8212
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.initialize confirmed - Block: 11462825   Gas used: 187114 (1.56%)


Transaction sent: 0xf059664a2c3542e5b464bddf28c34c2aad4d901354969ec8a8041a6258234896
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  ICEtherEx.mint confirmed - Block: 11462826   Gas used: 97948 (0.82%)


Transaction sent: 0x69978afc486a2daea613a819e8508bd83eda5b7cca0765c03abc3909f3ddf2dd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  ICEtherEx.transfer confirmed - Block: 11462827   Gas used: 49998 (0.42%)


Transaction sent: 0xbd77d05b5693ea3fc465627ffb86c413662d6491babdc4d6a2b8be7a2d43f53b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IComptroller.enterMarkets confirmed - Block: 11462828   Gas used: 45842 (0.38%)


Transaction sent: 0xeb781da7538d7b500e87479a6841bda2934bddf04d7ac0c75bfffec190578fd1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  HomoraBank.addBank confirmed - Block: 11462829   Gas used: 60895 (0.51%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 100000000000 Tether USD to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x28e371d752102f642a04252768343e726d046dc1ae598f0d875feb8b58de2529
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 649

  IERC20Ex.transfer confirmed - Block: 11462830   Gas used: 41209 (0.34%)

sending from 0x397FF1542f962076d0BFE58eA045FfA2d347ACa0 1000000000000000000000 Wrapped Ether to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x919bee03b7d4ba7abc9359fef4cc73fd37557d5e478a2c65db4a88a4b4857a64
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462831   Gas used: 36818 (0.31%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0x740920a745bcbb15275beb3c69e33b22820bd6828bb4bf9cd27d9a3f100b18cc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 650

  IERC20Ex.transfer confirmed - Block: 11462832   Gas used: 41209 (0.34%)

sending from 0x397FF1542f962076d0BFE58eA045FfA2d347ACa0 1000000000000000000000 Wrapped Ether to 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0xd7cc7451fa324eda6359ff0e5a1939a7f02da56d9382119d83a25084889433e5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IERC20Ex.transfer confirmed - Block: 11462833   Gas used: 36818 (0.31%)

Alice usdt balance 100000000000
Alice weth balance 100000000000000000000

Transaction sent: 0x91b2b45e70204284af05a07bc5fe306a71b5e3c34dd464697a60270e27cd601a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 714

  IERC20Ex.transfer confirmed - Block: 11462834   Gas used: 35972 (0.30%)


Transaction sent: 0x97ca3326753fd5bc8c25e4ab79de88b6382a79edd959fc6cc3fc65168eecc769
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 715

  IERC20Ex.transfer confirmed - Block: 11462835   Gas used: 35972 (0.30%)


Transaction sent: 0x54635050f65027c2b84e20e9554c4261fbf2a867ad47c60e38b0750f41776341
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462836   Gas used: 31297 (0.26%)


Transaction sent: 0x1b3f45d4648f863a05d03697186badb445b50cfcfa7c0be11b88039c2c93aca1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462837   Gas used: 31297 (0.26%)


Transaction sent: 0xe061e78695659266cbe8749b86bd915c5bcc86bf636acb1cc94b72575dbfb1e5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462838   Gas used: 29264 (0.24%)


Transaction sent: 0x63f3662305ddbf3f755cb39a6a6bd3a3eb9a41f2e3f80a562579c9158b23fe97
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462839   Gas used: 29286 (0.24%)


Transaction sent: 0x9fe9c84714771d84206186dcff798116e44df81a3d2c4c5cb25be8fa25970b4a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12

  UniswapV2SpellV1.constructor confirmed - Block: 11462840   Gas used: 2407923 (20.07%)
  UniswapV2SpellV1 deployed at: 0x2c15A315610Bfa5248E4CbCbd693320e9D8E03Cc


Transaction sent: 0xf5f29f44def3415c78b59cb86457ec45e1bebceabd0a640155f7f274936841ae
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13

  UniswapV2SpellV1.getPair confirmed - Block: 11462841   Gas used: 105878 (0.88%)

========================================================================
Case 1.

Transaction sent: 0x3aba817d3ca3e44ef03a9aa0dcb5e885f6a69ba60de8a776436a5a1e58bf9fb6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  HomoraBank.execute confirmed - Block: 11462842   Gas used: 755414 (6.30%)

position_id 1
spell lp balance 0
Alice delta A balance -399999999
Alice delta B balance -1000000000000000000
add liquidity gas 755414
bank lp balance 200000000000000000
bank usdt totalDebt 1000000000
bank usdt totalShare 1000000000
bank prev LP balance 200000000000000000
bank cur LP balance 200000000000000000
werc20 prev LP balance 0
werc20 cur LP balance 10041190583866394
========================================================================
Case 2.

Transaction sent: 0xb786ece13c9e83f7f604d21e3fae9b036de8f420e2870b69c175131b42fcef61
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.execute confirmed - Block: 11462843   Gas used: 433750 (3.61%)

spell lp balance 0
spell usdt balance 0
spell weth balance 0
Alice delta A balance 280033941616
Alice delta B balance 0
Alice delta LP balance 1000000000000000
remove liquidity gas 433750
bank delta lp balance 0
bank total lp balance 200000000000000000
bank usdt totalDebt 0
bank usdt totalShare 0
```

```
LP want 1000000000000000
bank delta LP amount 0
LP take amount 10000000000000000
prev werc20 LP balance 10041190583866394
cur werc20 LP balance 41190583866394
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'uniswap_spell_more_add_remove_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462790   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462791   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0xe2affc7545b134ad0230e7711efb90915392878e711f94030c2152c1c8d3c2e8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  SimpleOracle.setETHPx confirmed - Block: 11462792   Gas used: 38249 (0.32%)


Transaction sent: 0x6c91272d1e90416a862a2a1078a868ce3178139d7d96a3c4bcdb7dfd394972fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  ProxyOracle.constructor confirmed - Block: 11462793   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0x4856a201ead1f639457d2a0f785d38c5ef9ec921e6e0e0401f094aa8d6bfc089
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462794   Gas used: 31221 (0.26%)


Transaction sent: 0x7009c041cb8b44c67c5ece3a0bc8a2e10b5bfeddbb04a9b23273d71c3dbf0fb2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  UniswapV2Oracle.constructor confirmed - Block: 11462795   Gas used: 384200 (3.20%)
  UniswapV2Oracle deployed at: 0x6b4BDe1086912A6Cb24ce3dB43b3466e6c72AFd3


Transaction sent: 0x0b05cc58b11a7d91637e88135ec930f8c247b749090198cdc3ac702d45816ad2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  ProxyOracle.constructor confirmed - Block: 11462796   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9


Transaction sent: 0xdcd3f1e318654223e624c7e99290b66229f1c4f4fb5dd0c80e7d27ca11f408a5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462797   Gas used: 31221 (0.26%)


Transaction sent: 0x0f5c1d48ead6c787209c64a72bc64535a15e16943f179bca29ae8dedc4e1ee59
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  ProxyOracle.setOracles confirmed - Block: 11462798   Gas used: 56835 (0.47%)


Transaction sent: 0xb714d7c0888a739ce9a7dc616c8cc9cbedb1565373887681864742a38ce5b1c3
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  HomoraBank.constructor confirmed - Block: 11462799   Gas used: 3700237 (30.84%)
  HomoraBank deployed at: 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472


Transaction sent: 0x1b1e4b5d9674dfbe391cc5a1e7697fc0fdfa085ec073775da35f274c3e4b8212
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.initialize confirmed - Block: 11462800   Gas used: 187114 (1.56%)


Transaction sent: 0xf059664a2c3542e5b464bddf28c34c2aad4d901354969ec8a8041a6258234896
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  ICEtherEx.mint confirmed - Block: 11462801   Gas used: 97948 (0.82%)


Transaction sent: 0xd0638e78933941491cb8323ccf0b2e1f348f56ed95329ec3732b0361cddc8866
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  ICEtherEx.transfer confirmed - Block: 11462802   Gas used: 49998 (0.42%)


Transaction sent: 0xbd77d05b5693ea3fc465627ffb86c413662d6491babdc4d6a2b8be7a2d43f53b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IComptroller.enterMarkets confirmed - Block: 11462803   Gas used: 45842 (0.38%)


Transaction sent: 0xeb781da7538d7b500e87479a6841bda2934bddf04d7ac0c75bfffec190578fd1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  HomoraBank.addBank confirmed - Block: 11462804   Gas used: 60895 (0.51%)


Transaction sent: 0x8c8a642ef8badd2706a5814e81f23a7d9ecad9a69476811113cf0ae097211051
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12

  HomoraBank.addBank confirmed - Block: 11462805   Gas used: 70547 (0.59%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x73c8e1f266c6244046c9849b1372dcc50a16b2dba6c28f460e147e1c3c11ebde
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 649

  IERC20Ex.transfer confirmed - Block: 11462806   Gas used: 41209 (0.34%)

sending from 0xA191e578a6736167326d05c119CE0c90849E84B7 1000000000000 USD Coin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x62fc1b976800994542fb074a8aeb19f2f8ac427609a716f5af0ce0017b0c33fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462807   Gas used: 42381 (0.35%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0x740920a745bcbb15275beb3c69e33b22820bd6828bb4bf9cd27d9a3f100b18cc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 650

  IERC20Ex.transfer confirmed - Block: 11462808   Gas used: 41209 (0.34%)

sending from 0x397FF1542f962076d0BFE58eA045FfA2d347ACa0 1000000000000 USD Coin to 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0x54ed7475e79142cafa1e26f95402149f13fe748cea8066b146120e3e828638d9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462809   Gas used: 42381 (0.35%)

Alice usdt balance 1000000000000
Alice usdc balance 1000000000000

Transaction sent: 0x4f4ffca4e75079fe7bf867ade566c5a0f857c2d1efdc1d78909bf326e80d3a13
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 347

  IERC20Ex.transfer confirmed - Block: 11462810   Gas used: 35936 (0.30%)


Transaction sent: 0x54635050f65027c2b84e20e9554c4261fbf2a867ad47c60e38b0750f41776341
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462811   Gas used: 31297 (0.26%)


Transaction sent: 0x1b3f45d4648f863a05d03697186badb445b50cfcfa7c0be11b88039c2c93aca1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462812   Gas used: 31297 (0.26%)


Transaction sent: 0xf031424618e7628fa47df344f9ee6692f22114f5719267617dc81100fe08d50b
```

```
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462813   Gas used: 34811 (0.29%)


Transaction sent: 0x3c741af7541b8cbf66618f3e8502af81335e3068ae2bcb982014d811ba7c56d4
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462814   Gas used: 34799 (0.29%)


Transaction sent: 0x3fac2569a116673f011934b4a6378dbb1f793bf6d3fb3241d24d10dd31eaf83e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  IERC20Ex.approve confirmed - Block: 11462815   Gas used: 29286 (0.24%)


Transaction sent: 0xd9626aee0dd271272f31af21a196fe96e7bc949c38203f7105be5884330a2a35
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13

  UniswapV2SpellV1.constructor confirmed - Block: 11462816   Gas used: 2407923 (20.07%)
  UniswapV2SpellV1 deployed at: 0xe692Cf21B12e0B2717C4bF647F9768Fa58861c8b


Transaction sent: 0xb95304bfd940a8698c03085ce793a36726c3d6d0cc2ea71131ba04d834db72bd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14

  UniswapV2SpellV1.getPair confirmed - Block: 11462817   Gas used: 114134 (0.95%)

==========================================================================
Case 1.

Transaction sent: 0x56120419c9a8bcaf3ecc79fe7b248ed00f241a1cf757af5775a0af4773b2cc87
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.execute confirmed - Block: 11462818   Gas used: 1121804 (9.35%)

position_id 1
spell lp balance 0
Alice delta A balance -40000000000
Alice delta B balance -49999999998
add liquidity gas 1121804
bank lp balance 0
bank usdt debt 1000000000
bank usdt debt share 1000000000
bank usdc debt 200000000
bank usdc debt share 200000000
bank prev LP balance 0
bank cur LP balance 0
werc20 prev LP balance 0
werc20 cur LP balance 41004339342
prev usdt res 9180679057111
cur usdt res 9221679057111
prev usdc res 9171225238380
cur usdc res 9221425238378
==========================================================================
Case 2.

Transaction sent: 0x156d5c18496a625a312eba0cb7c026bf86b8348637834bd221918f2dae94c236
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  HomoraBank.execute confirmed - Block: 11462819   Gas used: 1106062 (9.22%)

position_id 1
spell lp balance 0
Alice delta A balance -20000000000
Alice delta B balance -29999999998
add liquidity gas 1106062
bank lp balance 0
bank usdt debt 2000000086
bank usdt debt share 1999999914
bank usdc debt 400000015
bank usdc debt share 399999985
bank prev LP balance 0
bank cur LP balance 0
werc20 prev LP balance 41004339342
werc20 cur LP balance 64024394824
prev usdt res 9221679057111
cur usdt res 9242679057111
prev usdc res 9221425238378
cur usdc res 9251625238376
==========================================================================
Case 3.

Transaction sent: 0xd8479c11431984355b1364a736437401183dab17f3412a03df1655d0b53232be
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12

  HomoraBank.execute confirmed - Block: 11462820   Gas used: 631860 (5.27%)

spell lp balance 0
spell usdt balance 0
spell usdc balance 0
Alice delta A balance 33586977139
Alice delta B balance 35221422726
Alice delta LP balance 100000
remove liquidity gas 631860
bank delta lp balance 0
bank total lp balance 0
bank usdt totalDebt 0
bank usdt totalShare 0
bank usdc totalDebt 0
bank usdc totalShare 0
LP want 100000
bank delta LP amount 0
LP take amount 32012197412
prev werc20 LP balance 64024394824
cur werc20 LP balance 32012197412
coll size 64024394824
==========================================================================
Case 4.

Transaction sent: 0x15928dbcbc882937bf588987b6e7e6db229930ead127e5986fc822048f25c20a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13

  HomoraBank.execute confirmed - Block: 11462821   Gas used: 298819 (2.49%)

spell lp balance 0
spell usdt balance 0
spell usdc balance 0
Alice delta A balance 35586977397
Alice delta B balance 35621422772
Alice delta LP balance 100000
remove liquidity gas 298819
bank delta lp balance 0
bank total lp balance 0
bank usdt totalDebt 0
bank usdt totalShare 0
bank usdc totalDebt 0
bank usdc totalShare 0
LP want 100000
bank delta LP amount 0
LP take amount 1157920892373161954235709850086879078532699846656405640394575840079131296399350
prev werc20 LP balance 32012197412
cur werc20 LP balance 0
coll size 32012197412
==========================================================================
Case 5.

Transaction sent: 0xd9d8aaa04e4cfed5ce697edeff7c8f208554c628fac3b474a1a1c2130f6e54cd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14

  HomoraBank.execute confirmed - Block: 11462822   Gas used: 415713 (3.46%)

position_id 1
spell lp balance 0
Alice delta A balance -2000000000
Alice delta B balance -2999999997
Alice delta lp balance 0
add liquidity gas 415713
bank lp balance 0
bank usdt totalDebt 0
bank usdt totalShare 0
bank usdc totalDebt 0
bank usdc totalShare 0
bank prev LP balance 0
bank cur LP balance 0
werc20 prev LP balance 0
werc20 cur LP balance 2246872538
==========================================================================
Case 6.

Transaction sent: 0x6636b464c120a8621218307579512c844f8eae519b9457b2ffbf703bbfb2e1fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 15

  HomoraBank.execute confirmed - Block: 11462823   Gas used: 192057 (1.60%)
```

```
spell lp balance 0
spell usdt balance 0
spell usdc balance 0
Alice delta A balance 2497651514
Alice delta B balance 2500340784
Alice delta LP balance 0
remove liquidity gas 192057
bank delta lp balance 0
bank total lp balance 0
bank usdt totalDebt 0
bank usdt totalShare 0
bank usdc totalDebt 0
bank usdc totalShare 0
LP want 0
bank delta LP amount 0
LP take amount 1157920892373161954235709850086879078532699846656405640394575840079131296399 35
prev werc20 LP balance 2246872538
cur werc20 LP balance 0
coll size 2246872538
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'uniswap_spell_usdc_usdt_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462802   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462803   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0xe2affc7545b134ad0230e7711efb90915392878e711f94030c2152c1c8d3c2e8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  SimpleOracle.setETHPx confirmed - Block: 11462804   Gas used: 38249 (0.32%)


Transaction sent: 0x96bf4ffc65ed5f0054af1734291ec6e23080d14673cc2690c7039fdee7fd33c9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  UniswapV2Oracle.constructor confirmed - Block: 11462805   Gas used: 384200 (3.20%)
  UniswapV2Oracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0x784bc774b5e4520ff23822246bbef6567abf3c007b0e597ef4e786ca10a85297
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  ProxyOracle.constructor confirmed - Block: 11462806   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0xe0aA552A10d7EC8760Fc6c246D391E698a82dDf9


Transaction sent: 0x89bf5f373451fc4dd2adc430f53a98efa4fbda77a828b53cd9778a056e6fb8a3
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462807   Gas used: 31221 (0.26%)


Transaction sent: 0x29ca82fedd8221f3d90332b1f14a83fb0babd3abf5a8e0b8c2b3797218c3f540
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  ProxyOracle.setOracles confirmed - Block: 11462808   Gas used: 56835 (0.47%)


Transaction sent: 0xc952dd93bcbf7235edb30d05f7c024aa1f40b0a159de16d29a7239a5218d7912
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  HomoraBank.constructor confirmed - Block: 11462809   Gas used: 3700237 (30.84%)
  HomoraBank deployed at: 0xcCB53c9429d32594F404d01fbe9E65ED1DCda8D9


Transaction sent: 0xa1fbf66e830af8f00d7a188d393edda0f9faa31f16f62ad53c1ddcf1913fa551
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  HomoraBank.initialize confirmed - Block: 11462810   Gas used: 187114 (1.56%)


Transaction sent: 0xf059664a2c3542e5b464bddf28c34c2aad4d901354969ec8a8041a6258234896
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  ICEtherEx.mint confirmed - Block: 11462811   Gas used: 97948 (0.82%)


Transaction sent: 0x10db4515efbb370de9f69d3db1bda58aa1442246686ad7637bb7e34a21dd7274
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  ICEtherEx.transfer confirmed - Block: 11462812   Gas used: 49998 (0.42%)


Transaction sent: 0x713879ee21e16f5d69227978be959d8e43b315615920db2705a5af45b092e938
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IComptroller.enterMarkets confirmed - Block: 11462813   Gas used: 45842 (0.38%)


Transaction sent: 0x12505f8a8ad53691b1f841847d35767f181a3e75303725aa5c8e6324004850bc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  HomoraBank.addBank confirmed - Block: 11462814   Gas used: 60895 (0.51%)


Transaction sent: 0x16f9eb6f07632ca417b585831d512d03f00f3146f5dfee78cddf5140f6f5b9e7
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.addBank confirmed - Block: 11462815   Gas used: 70547 (0.59%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x73c8e1f266c6244046c9849b1372dcc50a16b2dba6c28f460e147e1c3c11ebde
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 649

  IERC20Ex.transfer confirmed - Block: 11462816   Gas used: 41209 (0.34%)

sending from 0xA191e578a6736167326d05c119CE0c90849E84B7 1000000000000 USD Coin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x62fc1b976800994542fb074a8aeb19f2f8ac427609a716f5af0ce0017b0c33fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462817   Gas used: 42381 (0.35%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0xcCB53c9429d32594F404d01fbe9E65ED1DCda8D9

Transaction sent: 0x41bbbdaa8fa25acd11004789906011ab253c6826294c36b0caf55590df00024e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 650

  IERC20Ex.transfer confirmed - Block: 11462818   Gas used: 41209 (0.34%)

sending from 0x397FF1542f962076d0BFE58eA045FfA2d347ACa0 1000000000000 USD Coin to 0xcCB53c9429d32594F404d01fbe9E65ED1DCda8D9

Transaction sent: 0x33a05509fdc45f125ae80fefc88fc261d294c97c419b9c26309491862e52532f
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462819   Gas used: 42381 (0.35%)

Alice usdt balance 1000000000000
Alice usdc balance 1000000000000

Transaction sent: 0x4f4ffca4e75079fe7bf867ade566c5a0f857c2d1efdc1d78909bf326e80d3a13
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 347

  IERC20Ex.transfer confirmed - Block: 11462820   Gas used: 35936 (0.30%)


Transaction sent: 0xdd784d488ab9d8f170aade72a222e22173ab13c11ce375bc7f40fd41a419b5ff
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462821   Gas used: 31297 (0.26%)


Transaction sent: 0x1b3f45d4648f863a05d03697186badb445b50cfcfa7c0be11b88039c2c93aca1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462822   Gas used: 31297 (0.26%)
```

```
Transaction sent: 0x174e9ae6306e8e4bb09d04b2801b529f19cdd64da41cd12a1bfd6c37f7461892
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462823   Gas used: 34811 (0.29%)


Transaction sent: 0x3c741af7541b8cbf66618f3e8502af81335e3068ae2bcb982014d811ba7c56d4
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462824   Gas used: 34799 (0.29%)


Transaction sent: 0x1f16e1a8f68632e395db94a45bed6adb0e5200c8659747a3fbacd32d26b3e5ff
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  IERC20Ex.approve confirmed - Block: 11462825   Gas used: 29286 (0.24%)


Transaction sent: 0xc1e092f74d05253d60d59ae1f5a548048fc754b7ea6454b2ce07b41e254ca1e5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  UniswapV2SpellV1.constructor confirmed - Block: 11462826   Gas used: 2407923 (20.07%)
  UniswapV2SpellV1 deployed at: 0x7a3d735ee6873f17Dbdcab1d51B604928dc10d92


Transaction sent: 0x7c59d5faa11be5eb189cdaafa7c5c7820478d155275b633a893a650b707d1bf2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12

  UniswapV2SpellV1.getPair confirmed - Block: 11462827   Gas used: 114134 (0.95%)

========================================================================
Case 1.

Transaction sent: 0xa4144db968319354c38968386eb692b736c38b47b3a0329ce5f90b43ba7a8fb9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.execute confirmed - Block: 11462828   Gas used: 1121814 (9.35%)

position_id 1
spell lp balance 0
Alice delta A balance -40000000000
Alice delta B balance -49999999998
add liquidity gas 1121814
bank lp balance 0
bank usdt totalDebt 1000000000
bank usdt totalShare 1000000000
bank usdc totalDebt 200000000
bank usdc totalShare 200000000
bank prev LP balance 0
bank cur LP balance 0
werc20 prev LP balance 0
werc20 cur LP balance 41005887260
========================================================================
Case 2.

Transaction sent: 0xc8993d36028ecb53267e78c7d144544808db38c57e0672d17678f40f119092b9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  HomoraBank.execute confirmed - Block: 11462829   Gas used: 543560 (4.53%)

spell lp balance 0
spell usdt balance 0
spell usdc balance 0
Alice delta A balance 44625166382
Alice delta B balance 45388972784
Alice delta LP balance 100000
remove liquidity gas 543560
bank delta lp balance 0
bank total lp balance 0
bank usdt totalDebt 0
bank usdt totalShare 0
bank usdc totalDebt 0
bank usdc totalShare 0
LP want 100000
bank delta LP amount 0
LP take amount 1157920892373161954235709850086879078532699846656405640394575840079131296399 35
prev werc20 LP balance 41005887260
cur werc20 LP balance 0
coll size 41005887260
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'wmasterchef_test.py::main'...

Transaction sent: 0x5eed64c1a584d9863e856c23c28935cfe6e14eff4222df98f1a46866d334303c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WMasterChef.constructor confirmed - Block: 11462802   Gas used: 2278156 (18.98%)
  WMasterChef deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0xc65e48704a92e0c8cd54c1f13059d15cb1c2a7b31d0c4ef0cb6031931af1b284
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462803   Gas used: 31297 (0.26%)


Transaction sent: 0xe177b01ee96fabdb91a017f6cf0e9b74f87d3032d630b37ab20f7b764a542a2c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462804   Gas used: 34811 (0.29%)


Transaction sent: 0x920193e89195b5bb23d9a50f555aa71eb2172944255b839a877a785ddf713619
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462805   Gas used: 29264 (0.24%)


Transaction sent: 0x12ee65cc8c5dc1e275dc9da22cd2c8030ec2c47ca273a4841c2d4ac2ec274c6b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462806   Gas used: 29354 (0.24%)


Transaction sent: 0xd64c74e80d8e8b370ba3eb7772ea1f4f73e3c9313e52dfc564f2ebbfcd79d571
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  IERC20Ex.approve confirmed - Block: 11462807   Gas used: 29354 (0.24%)


Transaction sent: 0x1382d2e439f7d55cd659c4c304a5c91ddfe2baf20bc21f03fefaf10de3dea224
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  IERC20Ex.approve confirmed - Block: 11462808   Gas used: 29354 (0.24%)


Transaction sent: 0x3dbfb35dda7cccfeca0e40b3e21516184fe456746912b75fee88934c4203b88e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  IERC20Ex.approve confirmed - Block: 11462809   Gas used: 29354 (0.24%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x73c8e1f266c6244046c9849b1372dcc50a16b2dba6c28f460e147e1c3c11ebde
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 649

  IERC20Ex.transfer confirmed - Block: 11462810   Gas used: 41209 (0.34%)

sending from 0xA191e578a6736167326d05c119CE0c90849E84B7 1000000000000 USD Coin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x62fc1b976800994542fb074a8aeb19f2f8ac427609a716f5af0ce0017b0c33fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462811   Gas used: 42381 (0.35%)

sending from 0xCEfF51756c56CeFFCA006cD410B03FFC46dd3a58 1000000000000 Wrapped Ether to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x6c7b5ce4a751541659b7e794bd08fac622eba555b7f644e69890c60cdce67e29
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462812   Gas used: 36770 (0.31%)

sending from 0x6B4E746fA3c8Fd5eC1861833C883360C11C4c5B3 10000000000 SushiSwap LP Token to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x8a0a74af2b40fb09fcec461d872542ea0cb59df0c3ef5cacb5d0fb539140cdf8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 180

  IERC20Ex.transfer confirmed (ds-math-sub-underflow) - Block: 11462813   Gas used: 23017 (0.19%)

  File "brownie/_cli/run.py", line 49, in main
```

```
    return_value = run(args["<filename>"], method_name=args["<function>"] or "main")
  File "brownie/project/scripts.py", line 66, in run
    return getattr(module, method_name)(*args, **kwargs)
  File "./wmasterchef_test.py", line 51, in main
    setup_transfer(lpusdt, accounts.at(
  File "./wmasterchef_test.py", line 14, in setup_transfer
    asset.transfer(to, amt, {'from': fro})
  File "brownie/network/contract.py", line 1300, in __call__
    return self.transact(*args)
  File "brownie/network/contract.py", line 1174, in transact
    return tx["from"].transfer(
  File "brownie/network/account.py", line 646, in transfer
    receipt._raise_if_reverted(exc)
  File "brownie/network/transaction.py", line 372, in _raise_if_reverted
    raise exc._with_attr(
VirtualMachineError: revert: ds-math-sub-underflow
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'wstaking_rewards_test.py::main'...

Transaction sent: 0x2997df0880c39a5ed1aaddcc3ca112eecc66b0a1bf816ea4f47c8a383f245445
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WStakingRewards.constructor confirmed - Block: 11462815   Gas used: 2042087 (17.02%)
  WStakingRewards deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x5f1be9e83764bee7e005b8827d533bcb357a2b3cc544d634885b647c28eca9f9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462816   Gas used: 29406 (0.25%)


Transaction sent: 0x5daabdc3478e1679ff1560d54dc0a94d18f93ecb3e6eba00616a842d6fd720d0
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462817   Gas used: 34811 (0.29%)


Transaction sent: 0xfaf4030bd936090ffb0531a3aa1120975b042ec1530862709576a7c23fb5d59a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462818   Gas used: 29336 (0.24%)


Transaction sent: 0x011c204f85180ac6d683d9d6dd787d5ac6c3b0a73b4ee29a71ffc57b3a74b3fc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462819   Gas used: 29406 (0.25%)


Transaction sent: 0xada3982d685c3ad1214cd0de45470d389b8281cf99eca1aa0bf727d9ad9ccf14
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  IERC20Ex.approve confirmed - Block: 11462820   Gas used: 34811 (0.29%)


Transaction sent: 0x930afe5898484572c912c886435acf617090b6f9bfd67a85e89862babdb43c28
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  IERC20Ex.approve confirmed - Block: 11462821   Gas used: 29336 (0.24%)

sending from 0xC49F76a596D6200E4f08F8931D15B69DD1f8033E 1000000000000000000 Perpetual to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0xf073823ae334234226c6a7bdab86f6f5d179d2301f09ae1d8781be03a8014eb6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462822   Gas used: 36167 (0.30%)

sending from 0xA191e578a6736167326d05c119CE0c90849E84B7 1000000000000 USD Coin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x62fc1b976800994542fb074a8aeb19f2f8ac427609a716f5af0ce0017b0c33fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462823   Gas used: 42381 (0.35%)

sending from 0x5E4B407eB1253527628bAb875525AaeC0099fFC5 10000000000000000000 Balancer Pool Token to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0xb0af4ac61f6260a911bb3c445297cb0baa2875ec3fb2fb051be6148301a6d2b4
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462824   Gas used: 37029 (0.31%)

============================================================
Case 1.
============================================================
Case 2.

Transaction sent: 0xa06c741a09980cc8cee3ea0bcff7afd16cc0ae8d0fd740861009e0e0114f3203
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  WStakingRewards.mint confirmed - Block: 11462825   Gas used: 87933 (0.73%)

alice bpt balance 0

Transaction sent: 0x4096a90282d7d2edab9a3b360f56e4f4aca5c7816e5443be056850ef83260ee6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12

  WStakingRewards.burn confirmed - Block: 11462826   Gas used: 119417 (1.00%)

alice bpt balance 100000000000000000000
alice perp balance 59026056321849511400
perp gained 58026056321849511400
perp calculated reward 58026056321849511400

Transaction sent: 0x329bb4b6d60009550d8b4588406a7fdc537db9e073714f141da32ddbbbe53e42
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13

  IStakingRewards.stake confirmed - Block: 11462827   Gas used: 54007 (0.45%)


Transaction sent: 0xd5200a4eacfe1751b6907045d635621a8f638c426c142c15f9ba70cddaec229a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14

  IStakingRewards.withdraw confirmed - Block: 11462828   Gas used: 75525 (0.63%)


Transaction sent: 0x9d3c128e19ea7ab07a400649e072281998c79ced022f53045ca67832b294e909
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 15

  IStakingRewards.getReward confirmed - Block: 11462829   Gas used: 59297 (0.49%)

perp gained from directly staking 58014455750813555900
============================================================
Case 3.

Transaction sent: 0xbe331880953e913d5161fcdbd473f357ad6a3f78b5d6f8454461c118c5d258b7
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 16

  WStakingRewards.mint confirmed - Block: 11462830   Gas used: 79443 (0.66%)

alice bpt balance 0

Transaction sent: 0xcd190acafdcff05c2f23b99f8d4f653059e163a8e675268bd9fa78f786959219
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 17

  WStakingRewards.burn confirmed - Block: 11462831   Gas used: 120761 (1.01%)

alice bpt balance 100000000000000000000
alice perp balance 175054967823476623200
perp gained 58014455750813555900
perp calculated reward 58014455750813555900

Transaction sent: 0x37e2a19140c7bf9689b71eb7b3e7d3adaac650bc73f0698bc0f77a0e741fe64f
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 18

  IStakingRewards.stake confirmed - Block: 11462832   Gas used: 54007 (0.45%)


Transaction sent: 0x97498fbd0fb0339369a902e87869562e8239593d6e4213beca49912b76374c8b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 19

  IStakingRewards.withdraw confirmed - Block: 11462833   Gas used: 75525 (0.63%)


Transaction sent: 0xac4f27f612d29ce10df84128d55aa67cc2e9d558bed8e01d1a35a70be525cbf2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 20

  IStakingRewards.getReward confirmed - Block: 11462834   Gas used: 59297 (0.49%)
```

```
perp gained from directly staking 58002855179777600400
============================================================
Case 4.

Transaction sent: 0x0f20fccf8a9129723762afb4afe68808479a7f6161b237827df94ff407b3bbc8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 21

  WStakingRewards.mint confirmed - Block: 11462835   Gas used: 79443 (0.66%)

alice bpt balance 0

Transaction sent: 0xe23e39fb539e0b915d1ce16755bf5ee570a93684862cb5cf57b4e6217b836fb9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 22

  WStakingRewards.burn confirmed (ERC1155: burn amount exceeds balance) - Block: 11462836   Gas used: 29765 (0.25%)


Transaction sent: 0xca67800d04879784c150ffe5d3d3080dd1438c88b65797a9273ed5210486d753
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 23

  WStakingRewards.burn confirmed - Block: 11462837   Gas used: 164507 (1.37%)


Transaction sent: 0xf426174500f165f528f3c6c9513778f06c0bff173f2cc73276bb8de3ba28c464
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 24

  WStakingRewards.burn confirmed - Block: 11462838   Gas used: 120761 (1.01%)

perp gained 88339490609184182450
perp calc reward 88339490609184182450

Transaction sent: 0xbebc728f9afc482f9bb201c41597f7d36fb268a1f5699624e77f4e9fa66ea245
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 25

  IStakingRewards.stake confirmed - Block: 11462839   Gas used: 54007 (0.45%)


Transaction sent: 0xf1fad9812cb99d317cf2d50e3888dca3f717550562abadc863ca2d49d02fcd7a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 26

  IStakingRewards.withdraw confirmed - Block: 11462840   Gas used: 90525 (0.75%)


Transaction sent: 0x6d47450e0110ee159a02545972c890adc51be87310a827aa0e6e55963871ac7a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 27

  IStakingRewards.withdraw confirmed - Block: 11462841   Gas used: 75525 (0.63%)


Transaction sent: 0x8a2a165e39dfea6279eb49919578492d46e2519e7ff3c5dc346dc1f95631ff03
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 28

  IStakingRewards.getReward confirmed - Block: 11462842   Gas used: 59297 (0.49%)

perp gained from wstaking 88339490609184182450
perp gained from directly staking 88327890038148226950
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'balancer_oracle_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462812   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462813   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0xa6c2d6fe503336bda9ca0ab5489199ebceb9d4f1b5dba1bbce92aadd7b3a4dde
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  SimpleOracle.setETHPx confirmed - Block: 11462814   Gas used: 37997 (0.32%)


Transaction sent: 0x0ab53c8bb9c4498f168c792ae872939fcbe77d2c9439898d56b788990f11c9d6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  Balancer2TokensOracle.constructor confirmed - Block: 11462815   Gas used: 933311 (7.78%)
  Balancer2TokensOracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0x784bc774b5e4520ff23822246bbef6567abf3c007b0e597ef4e786ca10a85297
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  ProxyOracle.constructor confirmed - Block: 11462816   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0xe0aA552A10d7EC8760Fc6c246D391E698a82dDf9


Transaction sent: 0x89bf5f373451fc4dd2adc430f53a98efa4fbda77a828b53cd9778a056e6fb8a3
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462817   Gas used: 31221 (0.26%)


Transaction sent: 0x2cfef28569d370eff83c598ea21c583ded4d4578abee64899fd9548692b686f2
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  ProxyOracle.setOracles confirmed - Block: 11462818   Gas used: 52647 (0.44%)

======================================================================
Case 1.
lp price 44085420470675066087425155254830405 00
dai price 888757122066144197139861067 6149
weth price 51922968585348276285304963292200 96
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...
  File "brownie/_cli/run.py", line 49, in main
    return_value = run(args["<filename>"], method_name=args["<function>"] or "main")
  File "brownie/project/scripts.py", line 52, in run
    module = _import_from_path(script)
  File "brownie/project/scripts.py", line 110, in _import_from_path
    _import_cache[import_str] = importlib.import_module(import_str)
  File "/usr/local/Cellar/python@3.9/3.9.1/Frameworks/Python.framework/Versions/3.9/lib/python3.9/importlib/__init__.py", line 127, in import_module
    return _bootstrap._gcd_import(name[level:], package, level)
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "./borrow_test.py", line 2, in <module>
    from brownie import (
ImportError: cannot import name 'UniswapV2LPKP3ROracle' from 'brownie' (/usr/local/lib/python3.9/site-packages/brownie/__init__.py)
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'curve_add_remove_3_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462799   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462800   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0xc0dceaccc2bb98034d6ef65f4c5d0f3a0fb74c3558e7b66b538d2e128ab198b1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2
```

```
  SimpleOracle.setETHPx confirmed - Block: 11462801   Gas used: 53027 (0.44%)


Transaction sent: 0x6c91272d1e90416a862a2a1078a868ce3178139d7d96a3c4bcdb7dfd394972fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  ProxyOracle.constructor confirmed - Block: 11462802   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0x4856a201ead1f639457d2a0f785d38c5ef9ec921e6e0e0401f094aa8d6bfc089
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462803   Gas used: 31221 (0.26%)


Transaction sent: 0xeac269c842c6355ce8127069232f3aa92fa3b01d17faf3019aab875cd6a0b53c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  ProxyOracle.setOracles confirmed - Block: 11462804   Gas used: 67905 (0.57%)


Transaction sent: 0x1c56bdb95d468f1652ece74aa9816a08f3ecf2ab59782782dc2ab1d5a4228a01
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  HomoraBank.constructor confirmed - Block: 11462805   Gas used: 3700237 (30.84%)
  HomoraBank deployed at: 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9


Transaction sent: 0x1b9045adf7152c1d2d7716ba9db28df314ea08235e02adb41456421a7c3d2619
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  HomoraBank.initialize confirmed - Block: 11462806   Gas used: 187114 (1.56%)


Transaction sent: 0xf059664a2c3542e5b464bddf28c34c2aad4d901354969ec8a8041a6258234896
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  ICEtherEx.mint confirmed - Block: 11462807   Gas used: 97948 (0.82%)


Transaction sent: 0x95fb1db3be7666681c51bc192c7f4bd598238b875bc0d60a7b20e536bbbeed08
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  ICEtherEx.transfer confirmed - Block: 11462808   Gas used: 49998 (0.42%)


Transaction sent: 0xc86ffe3bf18cae644ad6f2642b672839b9d3f8cff84c8e06c5c8b640c8916ece
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IComptroller.enterMarkets confirmed - Block: 11462809   Gas used: 45842 (0.38%)


Transaction sent: 0x38e790bfeb8b48be5916cf4475baf942a4b4b97a97c0f84b3521643fd029cd9a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  HomoraBank.addBank confirmed - Block: 11462810   Gas used: 56904 (0.47%)


Transaction sent: 0x9f6c5cf53a82a9261c7798dd1e7b657129f95b99c684866877783444b7060886
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  HomoraBank.addBank confirmed - Block: 11462811   Gas used: 70547 (0.59%)


Transaction sent: 0x47d045a1e386b790f8171825748551ade6c2af8a0ab46fe1a9800509a95bc14d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  HomoraBank.addBank confirmed - Block: 11462812   Gas used: 60895 (0.51%)

sending from 0xC3D03e4F041Fd4cD388c549Ee2A29a9E5075882f 1000000000000000000000000 Dai Stablecoin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x519df73fc6f245671a894a760250da72c3f1844c06a9bb396c99217056857343
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462813   Gas used: 37018 (0.31%)

sending from 0xA191e578a6736167326d05c119CE0c90849E84B7 1000000000000 USD Coin to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x62fc1b976800994542fb074a8aeb19f2f8ac427609a716f5af0ce0017b0c33fd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462814   Gas used: 42381 (0.35%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0x33A4622B82D4c04a53e170c638B944ce27cffce3

Transaction sent: 0x73c8e1f266c6244046c9849b1372dcc50a16b2dba6c28f460e147e1c3c11ebde
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 649

  IERC20Ex.transfer confirmed - Block: 11462815   Gas used: 41209 (0.34%)

sending from 0xC3D03e4F041Fd4cD388c549Ee2A29a9E5075882f 1000000000000000000000000 Dai Stablecoin to 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9

Transaction sent: 0x60b3f8136ccc6cd260dfaa294422c6835071f09804131cdbb724893fddefe2d4
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  IERC20Ex.transfer confirmed - Block: 11462816   Gas used: 37018 (0.31%)

sending from 0x397FF1542f962076d0BFE58eA045FfA2d347ACa0 1000000000000 USD Coin to 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9

Transaction sent: 0xc3f16599cb192baa06c09be4d25a09beebdb43664debb89a9eabf9bbde29175d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462817   Gas used: 42381 (0.35%)

sending from 0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 1000000000000 Tether USD to 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9

Transaction sent: 0x6bbe213db6009930967f6de0d3c87c48c525b8ec403e2c785164a4d2068ede10
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 650

  IERC20Ex.transfer confirmed - Block: 11462818   Gas used: 41209 (0.34%)

Alice dai balance 1000000000000000000000000
Alice usdc balance 1000000000000
Alice usdt balance 1000000000000

Transaction sent: 0xc60a1b3f418e109a46af50da30ada6293f1477e4cdc7d7d76161c2b5e9a0691d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  IERC20Ex.transfer confirmed - Block: 11462819   Gas used: 35614 (0.30%)


Transaction sent: 0x9131309117ffb6d759f1fee1e19fe0bc243bb954cc1d066d390dd35c9e4e4759
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  IERC20Ex.approve confirmed - Block: 11462820   Gas used: 29358 (0.24%)


Transaction sent: 0xf06282757c9c23b075e011c8b822a98da3047b2dc460d0e9b5c8ade45e511a49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  IERC20Ex.approve confirmed - Block: 11462821   Gas used: 29358 (0.24%)


Transaction sent: 0x34647ad76a25e69eabd81747934073600a901c714a0713061b4cfc89ace02a3f
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  IERC20Ex.approve confirmed - Block: 11462822   Gas used: 34811 (0.29%)


Transaction sent: 0x3c741af7541b8cbf66618f3e8502af81335e3068ae2bcb982014d811ba7c56d4
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  IERC20Ex.approve confirmed - Block: 11462823   Gas used: 34799 (0.29%)


Transaction sent: 0xfb55913a30ed5094b9b908b7c3289f4ebc5d01aadeee67805bbee59a9084c94e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9

  IERC20Ex.approve confirmed - Block: 11462824   Gas used: 31297 (0.26%)


Transaction sent: 0xce01efca01df2adea5656612086e7237b96269af40daa8687d4e9fa0af5909c7
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10

  IERC20Ex.approve confirmed - Block: 11462825   Gas used: 31297 (0.26%)


Transaction sent: 0xd962902115ec254d9c127400431a4d760c2457c37bcfd0e7f586612d30529237
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11

  IERC20Ex.approve confirmed - Block: 11462826   Gas used: 30227 (0.25%)


Transaction sent: 0xf44137d3ea653ee7e6e8343d19767984af2fc6f488c4f025763aacec78479607
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11
```

```
  CurveSpellV1.constructor confirmed - Block: 11462827   Gas used: 1939026 (16.16%)
  CurveSpellV1 deployed at: 0x7a3d735ee6873f17Dbdcab1d51B604928dc10d92

  File "brownie/_cli/run.py", line 49, in main
    return_value = run(args["<filename>"], method_name=args["<function>"] or "main")
  File "brownie/project/scripts.py", line 66, in run
    return getattr(module, method_name)(*args, **kwargs)
  File "./curve_add_remove_3_test.py", line 123, in main
    curve_spell.registerPool(lp)
  File "brownie/network/contract.py", line 506, in __getattribute__
    raise AttributeError(f"Contract '{self._name}' object has no attribute '{name}'")
AttributeError: Contract 'CurveSpellV1' object has no attribute 'registerPool'
Terminating local RPC client...


Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'curve_oracle_test.py::main'...

Transaction sent: 0x88f8c681dc12efe65e26d2efa59c0b2f7f2cb938e48bcfb6e963ac754b6aea49
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  WERC20.constructor confirmed - Block: 11462789   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x52aad4031537dd7b6490479adc95fd671f57089422cc77b7abc5813a4fdbf67d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.constructor confirmed - Block: 11462790   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6


Transaction sent: 0xc6020efa8586575a8ce413b2df5051cd7080be92694911b46f6208075ebaa916
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  SimpleOracle.setETHPx confirmed - Block: 11462791   Gas used: 45638 (0.38%)


Transaction sent: 0x07e6a316d37297bcb393a35194994c8ac5e9972279beb8cf68443883ad8f149a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3

  CurveOracle.constructor confirmed - Block: 11462792   Gas used: 634007 (5.28%)
  CurveOracle deployed at: 0x6951b5Bd815043E3F842c1b026b0Fa888Cc2DD85


Transaction sent: 0xb55804b35fc55f95c3e14afcfa0f1b57a096d6eb2d778d1e2d1d47d83f13a614
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4

  CurveOracle.registerPool confirmed - Block: 11462793   Gas used: 82471 (0.69%)


Transaction sent: 0xfa623d356f63193a57df8afb7f765dfc04187b910c77b048e3247dec516f4540
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5

  ProxyOracle.constructor confirmed - Block: 11462794   Gas used: 1215346 (10.13%)
  ProxyOracle deployed at: 0x6b4BDe1086912A6Cb24ce3dB43b3466e6c72AFd3


Transaction sent: 0x1792b5063748ab347a5617960c5dae86589c870e2619f262d5396cf1ddebce87
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6

  ProxyOracle.setWhitelistERC1155 confirmed - Block: 11462795   Gas used: 31221 (0.26%)


Transaction sent: 0x741b3b5295e24b32758ffa23f42b31efd6515f5b7af32ccd909706ede9510130
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7

  ProxyOracle.setOracles confirmed - Block: 11462796   Gas used: 67905 (0.57%)

========================================================================
Case 1.
pool virtual price 1005389840520077229
lp price 905080967411977493873883 5983448
dai price 906055358918898655209510 6856227
usdt price 900228877331592045813282032967307 3223442669
usdc price 901153548795379500662588321917127962 5142296
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.
Attached to local RPC client listening at '127.0.0.1:8545'...
  File "brownie/_cli/run.py", line 49, in main
    return_value = run(args["<filename>"], method_name=args["<function>"] or "main")
  File "brownie/project/scripts.py", line 52, in run
    module = _import_from_path(script)
  File "brownie/project/scripts.py", line 110, in _import_from_path
    _import_cache[import_str] = importlib.import_module(import_str)
  File "/usr/local/Cellar/python@3.9/3.9.1/Frameworks/Python.framework/Versions/3.9/lib/python3.9/importlib/__init__.py", line 127, in import_module
    return _bootstrap._gcd_import(name[level:], package, level)
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "<frozen, line line, in in
  File "./deploy_to_mainnet.py", line 1, in <module>
    from brownie import accounts, ERC20KP3ROracle, UniswapV2LPKP3ROracle
ImportError: cannot import name 'UniswapV2LPKP3ROracle' from 'brownie' (/usr/local/lib/python3.9/site-packages/brownie/__init__.py)


Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.

Launching 'ganache-cli --port 8545 --gasLimit 12000000 --accounts 10 --hardfork istanbul --mnemonic brownie --fork https://mainnet.infura.io/v3/ID'...

Running 'uniswap_lp_oracle_test.py::main'...

Transaction sent: 0xa3a3186b87d2a448ced3e26b4d2d08adab86acc35d4649f9fe3bd5384494be46
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0

  SimpleOracle.constructor confirmed - Block: 11462816   Gas used: 417736 (3.48%)
  SimpleOracle deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87


Transaction sent: 0x232a7b8a9588220df89d28fd30f0f562cfacc1d703a1603e7ce5a3795716cb58
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1

  SimpleOracle.setETHPx confirmed - Block: 11462817   Gas used: 52883 (0.44%)


Transaction sent: 0xc400577b05a8936ecd2b7de2fc0eb81f190db571d57e8a14f812040b24845423
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2

  UniswapV2Oracle.constructor confirmed - Block: 11462818   Gas used: 384200 (3.20%)
  UniswapV2Oracle deployed at: 0xE7eD6747FaC5360f88a2EFC03E00d25789F69291

ETH-USDT LP: 557583789230142006987198599724271565867
ETH-USDC LP: 557881771032412266177437577876328971538
USDT-USDC LP: 200351462186537582287859020230099906763397 83
Terminating local RPC client...

Brownie v1.12.2 - Python development framework for Ethereum

HomoraVReauditProject is the active project.
Attached to local RPC client listening at '127.0.0.1:8545'...

Running 'uniswap_spell_add_remove_test.py::main'...

Transaction sent: 0x893bab04abb988fa2039621d6746fa29aef509a0de0f04ef4fb8f1230180dead
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8

  WERC20.constructor confirmed - Block: 11462820   Gas used: 1855697 (15.46%)
  WERC20 deployed at: 0x420b1099B9eF5baba6D92029594eF45E19A04A4A

  File "brownie/_cli/run.py", line 49, in main
    return_value = run(args["<filename>"], method_name=args["<function>"] or "main")
  File "brownie/project/scripts.py", line 66, in run
    return getattr(module, method_name)(*args, **kwargs)
  File "./uniswap_spell_add_remove_test.py", line 43, in main
    simple_oracle = SimpleOracle.deploy({'from': admin})
  File "brownie/network/contract.py", line 283, in __call__
    return tx["from"].deploy(
  File "brownie/network/account.py", line 469, in deploy
    exc = VirtualMachineError(e)
  File "brownie/exceptions.py", line 104, in __init__
    raise ValueError(exc["message"]) from None
ValueError: the tx doesn't have the correct nonce. account has nonce of: 10 tx has nonce of: 9
```

Code Coverage

No coverage report could be generated in the current form of the project.

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

```
435cb22aad93529fa885391f1362971211c09abdbba7c62fb80ed55aee3a1591 ./contracts/Governable.sol
b7d6b9cf372c56ce761d1f3206a716bce37d977c57f67e803faa08cf5c53966c ./contracts/HomoraBank.sol
69570cabe65c83083661acde35f23c54fbcd7b04dbd710abba7fd759d9050175 ./contracts/wrapper/WERC20.sol
f53dc2c4cba4080018d5ce85e5cb2864b44e447d2128fee31a62151005d35ac6 ./contracts/wrapper/WMasterChef.sol
68d99de4af9cf04ae720ae995b8cb18e777e9a0a8631b709c07efc537b68613f ./contracts/utils/ERC1155NaiveReceiver.sol
f4eb56a7939f11dbddefa48dc348305675df1a6702104a3c0aa4cf429adf9b61 ./contracts/utils/HomoraMath.sol
8f1ca27770f8b08541bce7f389a2d971f69b925a32e6f76f62ff8642e150c27a ./contracts/spell/BasicSpell.sol
66b9909f4f38c3c95ee21ad51051b8a13c93374604fa4942dd6098ac40f77e22 ./contracts/spell/HouseHoldSpell.sol
a4e0bd99d8843c4f40730c1148eed9bfa582fc90c56c423acd15511f6a906c6b ./contracts/spell/UniswapV2SpellV1.sol
9bcbccb3d4d2b4bae4eafb966a8649782bc7d716918b6f3ac6da77147f3fdd97 ./contracts/oracle/BaseKP3ROracle.sol
7d48946a3931712c3f387b1aa109e01c37fa661b3a1e5e7b3c39c1bb845af7e3 ./contracts/oracle/ERC20KP3ROracle.sol
9d562cb77fcdc3c4d6e76da5bd81c0ef7353e06fa9db75953079070f34a37344 ./contracts/oracle/ProxyOracle.sol
ecf2a015ea51de1779539e2dc1369ccea07bc8d9b05ecb2ea4742ef1df133de8 ./contracts/oracle/SimpleOracle.sol
f11f704f6076dc314c03d3485a35e80ef81549f0a9472ce72733eb091575ce1d ./contracts/oracle/UniswapV2LPKP3ROracle.sol
```

Tests

```
193126384ab0fed5e3fc7845027c82c15929e954d152126b7952ac3f922f9371 ./scripts/borrow_test.py
d4d3b9955cc7324ff23a167617a7430ca046406d96abb5fca4fdaea85640aba7 ./scripts/deploy_to_mainnet.py
f6f97488ccd4ecba2eda64c507cd1aeeb77468019c8cfc0c381e9960f204fc0d ./scripts/uniswap_spell_add_remove_test.py
f6824c31fa8fb3a2a127e042a0b6c8da0a291266d9ccbac3a8f100e00a924ebe ./scripts/uniswap_spell_more_add_remove_test.py
2a311ca6e8b8eb41698fe4a82771af095e9c44756a4ecc5f26e4e37c7467fac3 ./scripts/uniswap_spell_usdc_usdt_test.py
```

Changelog

- 2020-12-11 - Initial report
- 2021-01-13 - reaudit report

About Quantstamp

Quantstamp is a Y Combinator-backed company that helps to secure blockchain platforms at scale using computer-aided reasoning tools, with a mission to help boost the adoption of this exponentially growing technology.

With over 1000 Google scholar citations and numerous published papers, Quantstamp's team has decades of combined experience in formal verification, static analysis, and software verification. Quantstamp has also developed a protocol to help smart contract developers and projects worldwide to perform cost-effective smart contract security scans.

To date, Quantstamp has protected $5B in digital asset risk from hackers and assisted dozens of blockchain projects globally through its white glove security assessment services. As an evangelist of the blockchain ecosystem, Quantstamp assists core infrastructure projects and leading community initiatives such as the Ethereum Community Fund to expedite the adoption of blockchain technology.

Quantstamp's collaborations with leading academic institutions such as the National University of Singapore and MIT (Massachusetts Institute of Technology) reflect our commitment to research, development, and enabling world-class blockchain security.