

## PROJECT

HaloDAO AMM

### CLIENT

HaloDAO

### DATE

October 2021

### REVIEWERS

Andrei Simion

[@andreiashu](#)

Daniel Luca

[@cleanunicorn](#)

# Table of Contents

---

- [Details](#)
- [Issues Summary](#)
- [Executive summary](#)
- [Scope](#)
- [Recommendations](#)
  - [Increase the number of tests](#)
- [Issues](#)
  - [Add validation checks to the JSON ingest during the deployment process](#)
  - [Whitelisting functionality is not used](#)
  - [depositWithWhitelist allows uncapped deposits](#)
- [Artifacts](#)
  - [Surya](#)
  - [Sūrya's Description Report](#)
  - [Files Description Table](#)
  - [Contracts Description Table](#)
  - [Legend](#)
  - [Tests](#)
- [License](#)

## Details

---

- **Client** HaloDAO
- **Date** October 2021
- **Lead reviewer** Andrei Simion ([@andreiashu](#))
- **Reviewers** Daniel Luca ([@cleanunicorn](#)), Andrei Simion ([@andreiashu](#))
- **Repository:** [HaloDAO AMM](#)
- **Commit hash** `aeb29effd3d379b1ffdae6bf82b39bfae262a6c4`
- **Technologies**
  - Solidity
  - Typescript

## Issues Summary

---

SEVERITY	OPEN	CLOSED
Informational	0	0
Minor	0	3
Medium	0	0
Major	0	0

## Executive summary

---

This report represents the results of the engagement with **HaloDAO** to review **HaloDAO AMM**.

The review is part of a broader engagement with HaloDAO that includes the [HaloDAO Lending Market](#) component.

The full review was conducted over the course of **2 weeks** from **October 18th to October 29th, 2021**. We spent a total of **15 person-days** reviewing the code.

## Scope

---

The initial review focused on the [HaloDAO AMM](#) repository, identified by the commit hash `aeb29effd3d379b1ffdae6bf82b39bfae262a6c4`. A further code change was merged into the repository from commit hash `c22d26a49a44ad6409190572da384cb724435201` (removed the whitelisting functionality from the original DFX Protocol code).

We focused on manually reviewing the codebase, searching for security issues such as, but not limited to, re-entrancy problems, transaction ordering, block timestamp dependency, exception handling, call stack depth limitation, integer overflow/underflow, self-destructible contracts, unsecured balance, use of origin, costly gas patterns, architectural problems, code readability.

### Includes:

- code/contracts/Curve.sol
- code/contracts/Storage.sol
- contracts/assimilators/BaseToUsdAssimilator.sol

## Recommendations

---

We identified a few possible general improvements that are not security issues during the review, which will bring value to the developers and the community reviewing and

using the product.

## Increase the number of tests

A good rule of thumb is to have 100% test coverage. This does not guarantee a lack of security problems, but it means that the desired functionality behaves as intended. The negative tests also bring value because not allowing some actions to happen is also part of the desired behavior.

## Issues

---

### Add validation checks to the JSON ingest during the deployment process

Status **Acknowledged** Severity **Minor**

#### Description

During the deployment of a new Assimilator contract, the `deployAssimilators.ts` script reads configuration data from a JSON file:

[code/scripts/halo/deployAssimilators.ts#L28-L32](#)

```
pairs.forEach(pair => {  
  let data = fs.readFileSync(path.join(__dirname, `./assimilatorConfigs/${NETWORK}/${pair}.json`));  
  let config = JSON.parse(data.toString());  
  assimilatorConfigs.push(config);  
});
```

At the moment there are no sanity checks on the data. For example, in Typescript, the following code prints out 10000000000000000000 and no error is thrown:

```
const obj = JSON.parse(`{ "baseDecimalss": 6 }`); // note the typo in the key  
console.log(parseUnits("1", obj.baseDecimals).toString()); // this prints out 10000000000000000000
```

#### Recommendation

Add a validation step to the JSON config data imported, before deploying a new assimilator.

---

### Whitelisting functionality is not used

Status **Fixed** Severity **Minor**

## Description

The original DFX Protocol provides functionality for whitelisted addresses to deposit capital to Curves within a whitelisting period:

[code/contracts/Curve.sol#L466-L473](#)

```
function depositWithWhitelist(  
    uint256 index,  
    address account,  
    uint256 amount,  
    bytes32[] calldata merkleProof,  
    uint256 _deposit,  
    uint256 _deadline  
) external deadline(_deadline) transactable nonReentrant inWhitelistingStage returns (uint256, uint256)
```

During this time not whitelisted deposits are not allowed (notice the presence of `notInWhitelistingStage` modifier):

[code/contracts/Curve.sol#L495-L503](#)

```
function deposit(uint256 _deposit, uint256 _deadline)  
    external  
    deadline(_deadline)  
    transactable  
    nonReentrant  
    notInWhitelistingStage  
    underCap(_deposit)  
    returns (uint256, uint256[] memory)  
{
```

We believe it's worth removing it for several reasons:

- having discussed this with the HaloDAO team there are no plans to use this functionality
- it seems it contains bespoke code that makes sense only for DFX Finance (the 10k max deposit)
- members of the HaloDAO community might get confused about the presence of this code no communications about it through the official channels
- it'll trim down code from contracts, scripts, and tests

## Recommendation

Remove all code that is related to this functionality.

---

`depositWithWhitelist` allows uncapped deposits

## Description

The `depositWithWhitelist` function has not been updated to account for deposit cap limits:

[code/contracts/Curve.sol#L466-L480](#)

```
function depositWithWhitelist(
    uint256 index,
    address account,
    uint256 amount,
    bytes32[] calldata merkleProof,
    uint256 _deposit,
    uint256 _deadline
) external deadline(_deadline) transactable nonReentrant inWhitelistingStage returns (uint256, uint256) {
    require(isWhitelisted(index, account, amount, merkleProof), "Curve/not-whitelisted");
    require(msg.sender == account, "Curve/not-approved-user");

    (uint256 curvesMinted_, uint256[] memory deposits_) =
        Proportionalliquidity.proportionalDeposit(curve, _deposit);

    whitelistedDeposited[msg.sender] = whitelistedDeposited[msg.sender].add(curvesMinted_);
}
```

Discussing with the HaloDAO team we understood that the whitelisting functionality that is present in the DFX Protocol will not be used.

## Recommendation

Since this function will not be used we recommend removing it altogether.

# Artifacts

## Surya




































Sūrya is a utility tool for smart contract systems. It provides a number of visual outputs and information about the structure of smart contracts. It also supports querying the function call graph in multiple ways to aid in the manual inspection and control flow analysis of contracts.

## Sūrya's Description Report













## Files Description Table




File Name	SHA-1 Hash
contracts/Curve.sol	3dbf839b54a7d414e38a35bd15664.
contracts/Storage.sol	a059eb769e3ac2f8db3356da13a6e
contracts/assimilators/BaseToUsdAssimilator.sol	c8d131432a367a9db6050e0eb916a

## Contracts Description Table



Contract	Type	Bases	
L	Function Name	Visibility	Mutability
<b>Curves</b>	Library		
L	add	Private 	
L	sub	Private 	
L	transfer	External 	
L	approve	External 	
L	transferFrom	External 	
L	increaseAllowance	External 	
L	decreaseAllowance	External 	
L	_transfer	Private 	
L	_approve	Private 	
<b>Curve</b>	Implementation	Storage	
L		Public 	
L	setParams	External 	
L	excludeDerivative	External 	
L	viewCurve	External 	
L	setEmergency	External 	
L	setFrozen	External 	
L	transferOwnership	External 	
L	originSwap	External 	
L	viewOriginSwap	External 	
L	targetSwap	External 	
L	viewTargetSwap	External 	



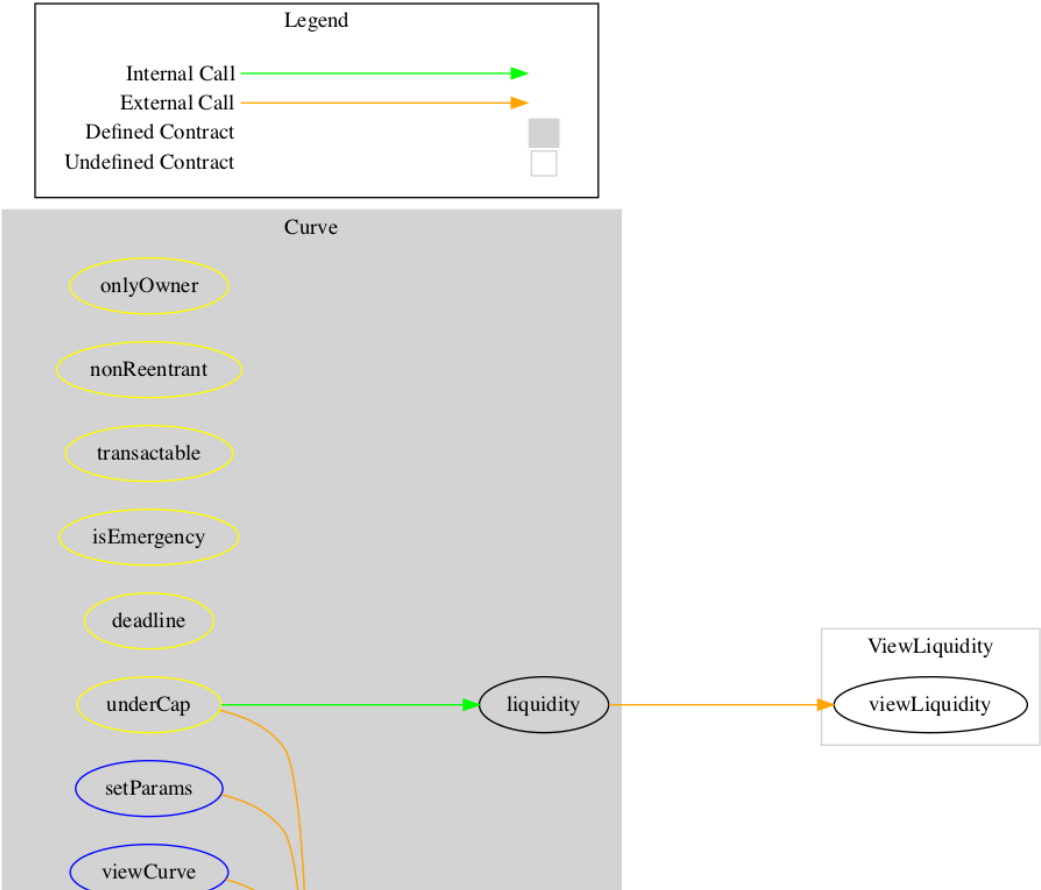
Contract	Type	Bases	
L	deposit	External !	
L	viewDeposit	External !	
L	emergencyWithdraw	External !	
L	withdraw	External !	
L	viewWithdraw	External !	
L	supportsInterface	Public !	
L	transfer	Public !	
L	transferFrom	Public !	
L	approve	Public !	
L	balanceOf	Public !	
L	totalSupply	Public !	
L	allowance	Public !	
L	liquidity	Public !	
L	assimilator	Public !	
L	setCap	Public !	
Storage	Implementation		
BaseToUsdAssimilator	Implementation	IAssimilator	
L		Public !	
L	getRate	Public !	
L	intakeRawAndGetBalance	External !	
L	intakeRaw	External !	
L	intakeNumeraire	External !	
L	intakeNumeraireLPRatio	External !	

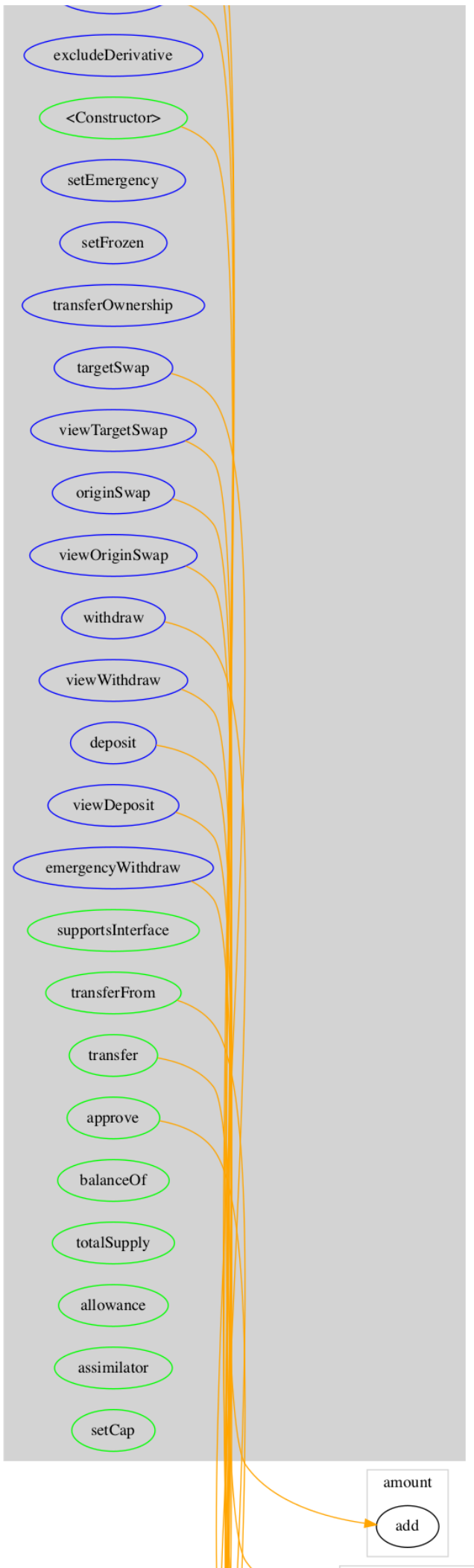
Contract	Type	Bases	
L	outputRawAndGetBalance	External !	
L	outputRaw	External !	
L	outputNumeraire	External !	
L	viewRawAmount	External !	
L	viewRawAmountLPRatio	External !	
L	viewNumeraireAmount	External !	
L	viewNumeraireBalance	External !	
L	viewNumeraireAmountAndBalance	External !	
L	viewNumeraireBalanceLPRatio	External !	

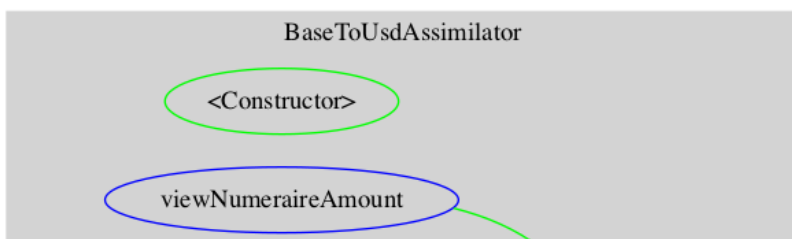
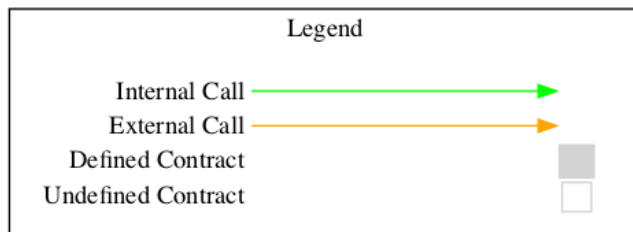
# Legend

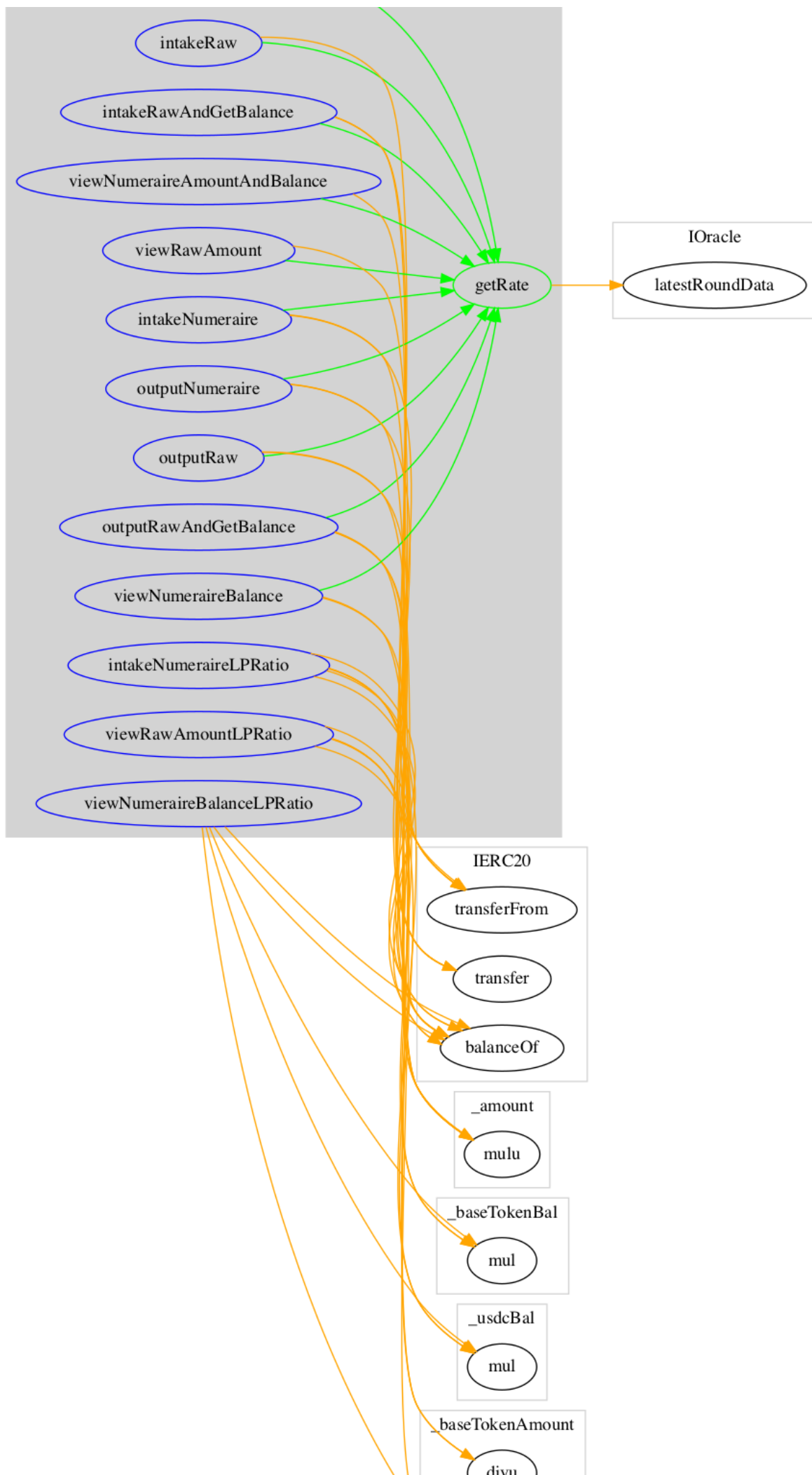
Symbol	Meaning
	Function can modify state
	Function is payable

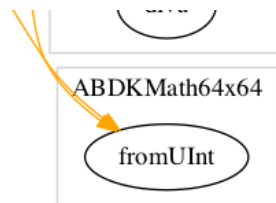
# Graphs











## Describe

```
$ npx surya describe ./code/contracts/Curve.sol

+ [Lib] Curves
  - [Prv] add
  - [Prv] sub
  - [Ext] transfer #
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Ext] increaseAllowance #
  - [Ext] decreaseAllowance #
  - [Prv] _transfer #
  - [Prv] _approve #

+ Curve (Storage)
  - [Pub] <Constructor> #
  - [Ext] setParams #
    - modifiers: onlyOwner
  - [Ext] excludeDerivative #
    - modifiers: onlyOwner
  - [Ext] viewCurve
  - [Ext] setEmergency #
    - modifiers: onlyOwner
  - [Ext] setFrozen #
    - modifiers: onlyOwner
  - [Ext] transferOwnership #
    - modifiers: onlyOwner
  - [Ext] originSwap #
    - modifiers: deadline,transactable,nonReentrant
  - [Ext] viewOriginSwap
    - modifiers: transactable
  - [Ext] targetSwap #
    - modifiers: deadline,transactable,nonReentrant
  - [Ext] viewTargetSwap
    - modifiers: transactable
  - [Ext] deposit #
    - modifiers: deadline,transactable,nonReentrant,underCap
  - [Ext] viewDeposit
    - modifiers: transactable,underCap
  - [Ext] emergencyWithdraw #
    - modifiers: isEmergency,deadline,nonReentrant
  - [Ext] withdraw #
    - modifiers: deadline,nonReentrant
  - [Ext] viewWithdraw
    - modifiers: transactable
```

- [Pub] supportsInterface
- [Pub] transfer #
  - modifiers: nonReentrant
- [Pub] transferFrom #
  - modifiers: nonReentrant
- [Pub] approve #
  - modifiers: nonReentrant
- [Pub] balanceOf
- [Pub] totalSupply
- [Pub] allowance
- [Pub] liquidity
- [Pub] assimilator
- [Pub] setCap #
  - modifiers: onlyOwner

(\$) = payable function

# = non-constant function

```
$ npx surya describe ./code/contracts/assimilators/BaseToUsdAssimilator.sol
```

```
+ BaseToUsdAssimilator (IAssimilator)
  - [Pub] <Constructor> #
  - [Pub] getRate
  - [Ext] intakeRawAndGetBalance #
  - [Ext] intakeRaw #
  - [Ext] intakeNumeraire #
  - [Ext] intakeNumeraireLPRatio #
  - [Ext] outputRawAndGetBalance #
  - [Ext] outputRaw #
  - [Ext] outputNumeraire #
  - [Ext] viewRawAmount
  - [Ext] viewRawAmountLPRatio
  - [Ext] viewNumeraireAmount
  - [Ext] viewNumeraireBalance
  - [Ext] viewNumeraireAmountAndBalance
  - [Ext] viewNumeraireBalanceLPRatio
```

(\$) = payable function

# = non-constant function

## Tests

Most of the tests that come with the original DFX Protocol code are integration tests, not unit tests. This means that the global state of the blockchain affects the results of the tests.

The test run below was run with the `BLOCK_NO=12640151` environment variable. The rest of the env vars were taken from the `.env.example` file provided in the repository.

The failed tests are related to a bug that the HaloDAO team asked to investigate: providing subsequent liquidity to a Curve sometimes failed with `Error: Transaction reverted without a reason string`. We narrowed down the issue to an invariant check in DFX CurveMath `enforceLiquidityInvariant` function. The HaloDAO team took it from there and is further investigating the case.

```
$ yarn run test
yarn run v1.22.15
$ hardhat test
Creating Typechain artifacts in directory typechain for target ethers-v5
Successfully generated Typechain artifacts!
```

#### Deployment

##### Core Contracts

- ✓ Curves
- ✓ Orchestrator
- ✓ ProportionallLiquidity
- ✓ Swaps
- ✓ ViewLiquidity
- ✓ CurveFactory
- ✓ Router

##### Assimilators

- ✓ CadcToUsdAssimilator
- ✓ UsdcToUsdAssimilator
- ✓ EursToUsdAssimilator
- ✓ XsgdToUsdAssimilator

##### Curve/Pair Contract

- ✓ CADC:USDC (384ms)

#### Curve Contract

##### Curve/Caps

- ✓ Should still deposit if under cap (910ms)
- ✓ Should still view deposit if under cap (9894ms)
- ✓ Should still deposit if under cap not set (7646ms)
- ✓ Should still view deposit if cap not set (9262ms)
- ✓ Should not be able to deposit if over cap (8376ms)
- ✓ Should not be able to view deposit if over cap (10101ms)

##### Curve/Pair Creation

- ✓ CADC:USDC (3861ms)
- ✓ EURS:USDC (3562ms)
- ✓ XSGD:USDC (3232ms)
- ✓ No duplicate pairs for CADC:USDC (3893ms)
- ✓ No duplicate pairs for EURS:USDC (3231ms)
- ✓ No duplicate pairs for XSGD:USDC (3502ms)

##### Set Dimensions

- ✓ CADC:USDC (3661ms)
- ✓ EURS:USDC (3365ms)
- ✓ XSGD:USDC (3974ms)

##### Emergency Withdraw



✓ CADC:USDC (8146ms)

1) EURS:USDC

✓ XSGD:USDC (7481ms)

#### Freeze and Unfreeze Curve

✓ CADC:USDC (10103ms)

2) EURS:USDC

✓ XSGD:USDC (9828ms)

#### Curve

##### Invariant Checking

✓ CADC (10793ms)

✓ XSGD (11062ms)

3) EURS

##### Swaps

✓ CADC/USDC 50/50 - 1 (CADC -> USDC) (8141ms)

✓ CADC/USDC 50/50 - 1 (USDC -> CADC) (8071ms)

✓ CADC/USDC 50/50 - 100 (CADC -> USDC) (7980ms)

✓ CADC/USDC 50/50 - 100 (USDC -> CADC) (7824ms)

✓ CADC/USDC 50/50 - 10000 (CADC -> USDC) (7674ms)

✓ CADC/USDC 50/50 - 10000 (USDC -> CADC) (7958ms)

✓ XSGD/USDC 50/50 - 1 (XSGD -> USDC) (8207ms)

✓ XSGD/USDC 50/50 - 1 (USDC -> XSGD) (7800ms)

✓ XSGD/USDC 50/50 - 100 (XSGD -> USDC) (7946ms)

✓ XSGD/USDC 50/50 - 100 (USDC -> XSGD) (7358ms)

✓ XSGD/USDC 50/50 - 10000 (XSGD -> USDC) (7892ms)

✓ XSGD/USDC 50/50 - 10000 (USDC -> XSGD) (9357ms)

4) EURS/USDC 50/50 - 1 (EURS -> USDC)

5) EURS/USDC 50/50 - 1 (USDC -> EURS)

6) EURS/USDC 50/50 - 100 (EURS -> USDC)

7) EURS/USDC 50/50 - 100 (USDC -> EURS)

8) EURS/USDC 50/50 - 10000 (EURS -> USDC)

9) EURS/USDC 50/50 - 10000 (USDC -> EURS)

##### Pool Ratio changes between operations

###### viewDeposit

✓ CADC/USDC 50/50 - 1 (10320ms)

✓ CADC/USDC 50/50 - 100 (10341ms)

✓ CADC/USDC 50/50 - 10000 (10097ms)

✓ XSGD/USDC 50/50 - 1 (10549ms)

✓ XSGD/USDC 50/50 - 100 (9725ms)

✓ XSGD/USDC 50/50 - 10000 (10093ms)

10) EURS/USDC 50/50 - 1

11) EURS/USDC 50/50 - 100

12) EURS/USDC 50/50 - 10000

###### viewWithdraw

✓ CADC/USDC 50/50 - 1 (10659ms)

✓ CADC/USDC 50/50 - 100 (11605ms)

✓ CADC/USDC 50/50 - 10000 (10149ms)

✓ XSGD/USDC 50/50 - 1 (11188ms)

✓ XSGD/USDC 50/50 - 100 (10029ms)

✓ XSGD/USDC 50/50 - 10000 (10040ms)

13) EURS/USDC 50/50 - 1

14) EURS/USDC 50/50 - 100

15) EURS/USDC 50/50 - 10000

#### Add and remove liquidity

- ✓ CADC/USDC 50/50 - 1 (12022ms)
- ✓ CADC/USDC 50/50 - 100 (13635ms)
- ✓ CADC/USDC 50/50 - 10000 (13345ms)
- ✓ XSGD/USDC 50/50 - 1 (14248ms)
- ✓ XSGD/USDC 50/50 - 100 (14465ms)
- ✓ XSGD/USDC 50/50 - 10000 (13287ms)

16) EURS/USDC 50/50 - 1

17) EURS/USDC 50/50 - 100

18) EURS/USDC 50/50 - 10000

#### Oracle updates between operations

##### viewDeposit

- ✓ CADC/USDC 50/50 - 1 (14915ms)
- ✓ CADC/USDC 50/50 - 100 (13690ms)
- ✓ CADC/USDC 50/50 - 10000 (13967ms)
- ✓ XSGD/USDC 50/50 - 1 (13644ms)
- ✓ XSGD/USDC 50/50 - 100 (14334ms)
- ✓ XSGD/USDC 50/50 - 10000 (13430ms)

19) EURS/USDC 50/50 - 1

20) EURS/USDC 50/50 - 100

21) EURS/USDC 50/50 - 10000

##### viewWithdraw

- ✓ CADC/USDC 50/50 - 1 (14184ms)
- ✓ CADC/USDC 50/50 - 100 (14460ms)
- ✓ CADC/USDC 50/50 - 10000 (14417ms)
- ✓ XSGD/USDC 50/50 - 1 (14542ms)
- ✓ XSGD/USDC 50/50 - 100 (14394ms)
- ✓ XSGD/USDC 50/50 - 10000 (14981ms)

22) EURS/USDC 50/50 - 1

23) EURS/USDC 50/50 - 100

24) EURS/USDC 50/50 - 10000

#### Add and remove liquidity

- ✓ CADC/USDC 50/50 - 1 (22223ms)
- ✓ CADC/USDC 50/50 - 100 (21662ms)
- ✓ CADC/USDC 50/50 - 10000 (19519ms)
- ✓ XSGD/USDC 50/50 - 1 (18651ms)
- ✓ XSGD/USDC 50/50 - 100 (19556ms)
- ✓ XSGD/USDC 50/50 - 10000 (20296ms)

25) EURS/USDC 50/50 - 1

26) EURS/USDC 50/50 - 100

27) EURS/USDC 50/50 - 10000

#### Factory

- ✓ No duplicate pairs (3139ms)

#### Zap

- ✓ CADC (42195ms)
- ✓ XSGD (41097ms)

28) EURS

#### Router

29) "before each" hook for "CADC -> USDC targetSwap"

84 passing (30m)

29 failing

#### 1) Curve Contract

Emergency Withdraw

EURS:USDC:

Error: Transaction reverted without a reason string

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at runMicrotasks (<anonymous>)

at processTicksAndRejections (node:internal/process/task\_queues:96:5)

at EthModule.\_estimateGasAction (node\_modules/hardhat/src/internal/hardhat-network/provider/modules/

at HardhatNetworkProvider.request (node\_modules/hardhat/src/internal/hardhat-network/provider/provid

at EthersProviderWrapper.send (node\_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

#### 2) Curve Contract

Freeze and Unfreeze Curve

EURS:USDC:

Error: Transaction reverted without a reason string

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at runMicrotasks (<anonymous>)

at processTicksAndRejections (node:internal/process/task\_queues:96:5)

at EthModule.\_estimateGasAction (node\_modules/hardhat/src/internal/hardhat-network/provider/modules/

at HardhatNetworkProvider.request (node\_modules/hardhat/src/internal/hardhat-network/provider/provid

at EthersProviderWrapper.send (node\_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

#### 3) Curve

Invariant Checking

EURS:

Error: Transaction reverted without a reason string

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at runMicrotasks (<anonymous>)

at processTicksAndRejections (node:internal/process/task\_queues:96:5)

at EthModule.\_estimateGasAction (node\_modules/hardhat/src/internal/hardhat-network/provider/modules/

at HardhatNetworkProvider.request (node\_modules/hardhat/src/internal/hardhat-network/provider/provid

at EthersProviderWrapper.send (node\_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

#### 4) Curve

Swaps

EURS/USDC 50/50 - 1 (EURS -> USDC):

Error: Transaction reverted without a reason string

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

at processTicksAndRejections (node:internal/process/task\_queues:96:5)

at EthModule.\_estimateGasAction (node\_modules/hardhat/src/internal/hardhat-network/provider/modules/

at HardhatNetworkProvider.request (node\_modules/hardhat/src/internal/hardhat-network/provider/provid

at EthersProviderWrapper.send (node\_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

5) Curve

Swaps

EURS/USDC 50/50 - 1 (USDC -> EURS):

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

6) Curve

Swaps

EURS/USDC 50/50 - 100 (EURS -> USDC):

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

7) Curve

Swaps

EURS/USDC 50/50 - 100 (USDC -> EURS):

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

8) Curve

Swaps

EURS/USDC 50/50 - 10000 (EURS -> USDC):

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

9) Curve

Swaps

EURS/USDC 50/50 - 10000 (USDC -> EURS):

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
```

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 10) Curve

Pool Ratio changes between operations

viewDeposit

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 11) Curve

Pool Ratio changes between operations

viewDeposit

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 12) Curve

Pool Ratio changes between operations

viewDeposit

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 13) Curve

Pool Ratio changes between operations

viewWithdraw

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
```

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 14) Curve

Pool Ratio changes between operations

viewWithdraw

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 15) Curve

Pool Ratio changes between operations

viewWithdraw

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 16) Curve

Pool Ratio changes between operations

Add and remove liquidity

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

#### 17) Curve

Pool Ratio changes between operations

Add and remove liquidity

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
```

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

#### 18) Curve

Pool Ratio changes between operations

Add and remove liquidity

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

#### 19) Curve

Oracle updates between operations

viewDeposit

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

#### 20) Curve

Oracle updates between operations

viewDeposit

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

#### 21) Curve

Oracle updates between operations

viewDeposit

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)

```

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

## 22) Curve

Oracle updates between operations

viewWithdraw

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

## 23) Curve

Oracle updates between operations

viewWithdraw

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

## 24) Curve

Oracle updates between operations

viewWithdraw

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

## 25) Curve

Oracle updates between operations

Add and remove liquidity

EURS/USDC 50/50 - 1:

Error: Transaction reverted without a reason string

```
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
```



```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

## 26) Curve

Oracle updates between operations

Add and remove liquidity

EURS/USDC 50/50 - 100:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

## 27) Curve

Oracle updates between operations

Add and remove liquidity

EURS/USDC 50/50 - 10000:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

## 28) Zap

EURS:

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w

```

## 29) Router

"before each" hook for "CAD -> USDC targetSwap":

Error: Transaction reverted without a reason string

```

at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at <UnrecognizedContract>.<unknown> (0xdb25f211ab05b1c97d595516f45794528a807ad8)
at runMicrotasks (<anonymous>)
at processTicksAndRejections (node:internal/process/task_queues:96:5)
at EthModule._estimateGasAction (node_modules/hardhat/src/internal/hardhat-network/provider/modules/
at HardhatNetworkProvider.request (node_modules/hardhat/src/internal/hardhat-network/provider/provid

```

```
at EthersProviderWrapper.send (node_modules/@nomiclabs/hardhat-ethers/src/internal/ethers-provider-w
```

## License

---

This report falls under the terms described in the included [LICENSE](#).