
Security Review Report NM-0057: SithSwap



NETHERMIND

(Oct 7, 2022)



Contents

- 1 Executive Summary** **3**
- 2 Contracts** **4**
- 3 Summary of Issues** **5**
- 4 Risk Rating Methodology** **6**
- 5 Issues** **7**
 - 5.1 General 7
 - 5.1.1 [Info] Storage variable naming convention may be insecure 7
 - 5.1.2 [Info] Use of 0 and 1 instead of TRUE and FALSE 7
 - 5.2 contracts/cairo/sithswap/amm/factory/factory/SithSwapV1Factory.cairo 7
 - 5.2.1 [Low] External initialization function 7
 - 5.3 contracts/cairo/sithswap/amm/factory/factory/library.cairo 7
 - 5.3.1 [Medium] Lack of argument validation in SithSwapV1Factory.create_pair(...) 7
 - 5.3.2 [Info] Missing check whether _compute_address is correct 8
 - 5.4 contracts/cairo/sithswap/amm/fees/library.cairo 8
 - 5.4.1 [Info] Lower execution cost opportunity in claim_fees_for(...) function 8
 - 5.5 contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo 8
 - 5.5.1 [Low] SithSwapV1Pair.approve(...) function is inconsistent with the ERC20 standard 8
 - 5.5.2 [Low] Unsafe approval change 8
 - 5.5.3 [Info] Imprecise inline documentation for SithSwapV1Pair.approve(...) 8
 - 5.5.4 [Info] Imprecise inline documentation for SithSwapV1Pair.renounceOwnership(...) 9
 - 5.5.5 [Info] Incomplete inline documentation for SithSwapV1Pair.initialize(...) function 9
 - 5.5.6 [Info] Incomplete inline documentation for SithSwapV1Pair.sample(...) function 9
 - 5.5.7 [Info] Inconsistent variable naming 9
 - 5.6 contracts/cairo/sithswap/amm/pair/library.cairo 10
 - 5.6.1 [Medium] set_trade_fee() function does not correctly check the new value 10
 - 5.6.2 [Low] SithSwapV1Pair.set_trade_fee() freeze period is not applied to all cases 10
 - 5.6.3 [Info] Event missing in function set_trade_fee(...) 10
 - 5.6.4 [Info] Misspelled variables 10
 - 5.6.5 [Info] Unchecked conversion from felt to Uint256 11
 - 5.6.6 [Info] Underflow may occur in _get_conditional_observation(...) function 11
 - 5.6.7 [Info] Use of magic numbers for fees 11
 - 5.7 contracts/cairo/sithswap/amm/router/SithSwapV1Router01.cairo 11
 - 5.7.1 [Medium] Assumption of correct Uint256 type arguments 11
 - 5.7.2 [Info] Non-uniform style of accessing namespace-encapsuled functions 12
 - 5.8 contracts/cairo/sithswap/libraries/Initializable.cairo 12
 - 5.8.1 [Info] Function initialize(...) is not emitting an event 12
 - 5.9 contracts/cairo/sithswap/libraries/SafeMath.cairo 12
 - 5.9.1 [Medium] Function felt_add(...) may be insecure 12
 - 5.9.2 [Medium] Function felt_mul(...) does not check for overflow 12
 - 5.9.3 [Medium] Function felt_sub(...) may be insecure 13
 - 5.10 contracts/cairo/sithswap/libraries/SafeOwnable.cairo 13
 - 5.10.1 [Info] Inconsistent function naming format 13
 - 5.11 contracts/cairo/sithswap/libraries/SithMath.cairo 13
 - 5.11.1 [Medium] Missing input validation in SithMath functions 13
 - 5.11.2 [Medium] Functions using is_le(...) may be insecure 13
 - 5.11.3 [Medium] Incorrect check in function sub_lt(...) 14
 - 5.11.4 [Info] Error message misspelling 14
 - 5.11.5 [Info] Function sith_div(...) does incorrect check for the sign 14
 - 5.11.6 [Info] Math operations suboptimal performance 15
 - 5.11.7 [Info] Simplifying conditional branching may save number of steps 15
 - 5.12 contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo 15
 - 5.12.1 [Medium] Constructor argument is not validated 15
 - 5.12.2 [Info] Code duplication 15
 - 5.12.3 [Info] Unsafe conversion from felt to Uint256 type 16
 - 5.12.4 [Info] Non-uniform coding style 16
 - 5.13 contracts/cairo/sithswap/amm/math/L03/library.cairo 16
 - 5.13.1 [Medium] Incorrect computation in _get_y_inner_kconv(...) function 16
 - 5.13.2 [Low] Function calculate_sample(...) may return false result 17
 - 5.13.3 [Info] Commented code in calculate_sample(...) function 17
- 6 Documentation Evaluation** **18**
- 7 Test Suite Evaluation** **19**
 - 7.1 Ape Cairo (math) 19
 - 7.2 Ape Cairo (core - Factory) 24
 - 7.3 Ape Cairo (core - Pair) 25
 - 7.4 Ape Cairo (ext. core - VLP) 32
 - 7.5 Ape Cairo (ext. core - SLP) 33



7.6 Ape Cairo (periphery core)	38
7.7 Ape Cairo (periphery 01)	40
7.8 Ape Cairo (Prostar Cairo)	43
8 About Nethermind	47

1 Executive Summary

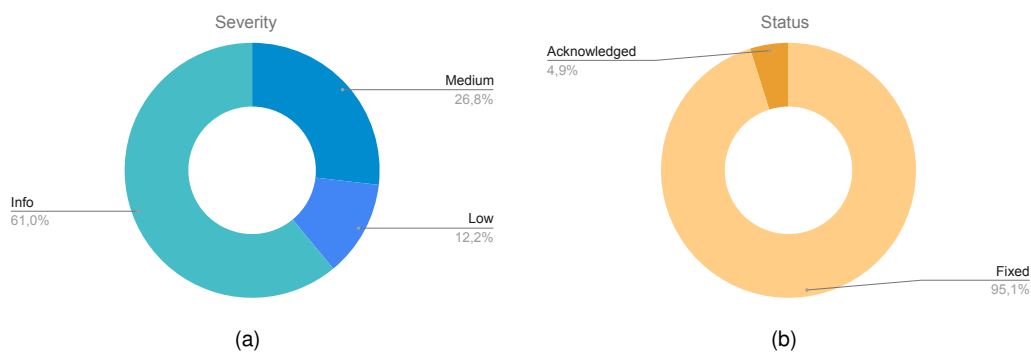
This document presents the security review performed by [Nethermind](#) on the [SithSwap Protocol](#). SithSwap is an AMM protocol featuring instant volatile and stable swaps with low fees and the full security of Ethereum. Contracts are not upgradable and the only privileged action is changing the swap’s fee which is capped by the protocol, demonstrating a high level of decentralization. The reviewed codebase is composed of approximately **6000** lines of code. Development of this project was correctly supported with a considerable test suite using different frameworks like **Protostar**, **Ape**, and also by the use of the static analyzer **Amarna**.

The SithSwap team developed a library supporting the protocol core math operations in a more efficient way than using vanilla **Uint256** operations. This library was manually reviewed, and differential testing techniques were applied in order to find differences between it and the original and simpler implementation.

Overall, the codebase shows very good code quality. The SithSwap team provided documentation and an already tested version of the protocol written in Solidity. Beyond documentation, the team was very responsive and collaborative during the assessment.

During this review, we point out 43 issues, none of which are High or Critical severity. Two of these issues were marked as false positives for a final amount of 41 issues. The distributions of issues can be seen in Figure 1. Most of the **Medium** severity issues are related to not enforcing correct values for **Uint256** at different layers of the protocol. Even though the previously mentioned issues do not represent risk to funds at the current time, the affected functions are part of a library and may be used in following iterations in an unsafe manner.

This document is organized as follows. Section 2 presents the files in the scope of this audit. Section 3 summarizes the findings in a table. Section 4 discusses the risk rating methodology adopted for this audit. Section 5 details each finding. Section 6 discusses the documentation provided for this audit. Section 7 presents the output of the automated test suite. Section 8 concludes the audit report.



Distribution of issues: Critical (0), High (0), Medium (11), Low (5), Undetermined (0), Informational (25).
Distribution of status: Acknowledged (2), Fixed (39).

Summary of the Audit

Audit Type	Security Review
Initial Report	Sep. 26, 2022
Response from Client	Sep. 29, 2022
Final Report	Oct. 7, 2022
Methods	Manual Review, Differential Testing
Repository	SithSwap Protocol
Commit Hashes (Initial Audit)	947ef38a0cf72749473c065431f2f1b4c7bd2b73
Commit Hashes (Math Library V3)	e1e6a925f07fac8d5622db7cc792729f917fc3db
Documentation	Available here
Documentation Quality	High

2 Contracts

Files reviewed in commit 947ef38a0cf72749473c065431f2f1b4c7bd2b73.

	Contract	Lines of Code	Lines of Comments	Comments Ratio	Blank Lines	Total Lines
1	contracts/cairo/sithswap/libraries/utils.cairo	59	7	11.9%	8	74
2	contracts/cairo/sithswap/libraries/Reentrancyguard.cairo	20	2	10.0%	5	27
3	contracts/cairo/sithswap/libraries/SafeERC20.cairo	17	1	5.9%	3	21
4	contracts/cairo/sithswap/libraries/SithMath.cairo	296	53	17.9%	33	382
5	contracts/cairo/sithswap/libraries/SafeMath.cairo	32	8	25.0%	5	45
6	contracts/cairo/sithswap/libraries/ERC20Library.cairo	231	27	11.7%	61	319
7	contracts/cairo/sithswap/libraries/SithStrings.cairo	88	1	1.1%	9	98
8	contracts/cairo/sithswap/libraries/Strings.cairo	123	14	11.4%	36	173
9	contracts/cairo/sithswap/libraries/SafeUint256.cairo	140	20	14.3%	18	178
10	contracts/cairo/sithswap/libraries/Initializable.cairo	22	2	9.1%	5	29
11	contracts/cairo/sithswap/libraries/SafeOwnable.cairo	77	8	10.4%	19	104
12	contracts/cairo/sithswap/libraries/array.cairo	83	42	50.6%	20	145
13	contracts/cairo/sithswap/amm/fees/SithSwapV1Fees.cairo	18	17	94.4%	7	42
14	contracts/cairo/sithswap/amm/fees/library.cairo	39	4	10.3%	12	55
15	contracts/cairo/sithswap/amm/fees/interfaces/ISithSwapV1Fees.cairo	7	1	14.3%	2	10
16	contracts/cairo/sithswap/amm/math/L02/SithSwapV1Library02.cairo	174	9	5.2%	14	197
17	contracts/cairo/sithswap/amm/math/L02/library.cairo	195	4	2.1%	18	217
18	contracts/cairo/sithswap/amm/factory/SithSwapV1Factory.cairo	121	64	52.9%	23	208
19	contracts/cairo/sithswap/amm/factory/library.cairo	133	7	5.3%	28	168
20	.../sithswap/amm/factory/interfaces/ISithSwapV1Factory.cairo	34	4	11.8%	18	56
21	contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo	360	162	45.0%	61	583
22	contracts/cairo/sithswap/amm/pair/library.cairo	1057	9	0.9%	113	1179
23	contracts/cairo/sithswap/amm/pair/interfaces/ISithSwapV1Pair.cairo	122	5	4.1%	57	184
24	contracts/cairo/sithswap/amm/router/SithSwapV1Router01.cairo	174	136	78.2%	23	333
25	contracts/cairo/sithswap/amm/router/SithSwapV1RouterLibrary.cairo	445	8	1.8%	39	492
26	contracts/cairo/sithswap/amm/router/library.cairo	160	3	1.9%	9	172
27	.../sithswap/amm/router/interfaces/ISithSwapV1Router01.cairo	97	4	4.1%	20	121
	Total	4324	622	14.4%	666	5612

Files reviewed in commit e1e6a925f07fac8d5622db7cc792729f917fc3db.

	Contract	Lines of Code	Lines of Comments	Comments Ratio	Blank Lines	Total Lines
1	contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo	161	10	6.2%	35	206
2	contracts/cairo/sithswap/amm/math/L03/library.cairo	236	27	11.4%	18	281
	Total	397	37	9.3%	53	487

3 Summary of Issues

	Finding	Severity	Update
1	Missing input validation in SithMath functions	Medium	Acknowledged
2	Assumption of correct Uint256 type arguments	Medium	Fixed
3	Functions using is_le(...) may be insecure	Medium	Fixed
4	Incorrect check in function sub_lt(...)	Medium	Fixed
5	Incorrect computation in _get_y_inner_kconv(...) function	Medium	Fixed
6	Lack of argument validation in SithSwapV1Factory.create_pair(...)	Medium	Fixed
7	set_trade_fee() function does not correctly check the new value	Medium	Fixed
8	Constructor argument is not validated	Medium	Fixed
9	Function felt_add(...) may be insecure	Medium	Fixed
10	Function felt_mul(...) does not check for overflow	Medium	Fixed
11	Function felt_sub(...) may be insecure	Medium	Fixed
12	External initialization function	Low	Fixed
13	SithSwapV1Pair.approve(...) function is inconsistent with the ERC20 standard	Low	Fixed
14	Unsafe approval change	Low	Fixed
15	SithSwapV1Pair.set_trade_fee() freeze period is not applied to all cases	Low	Fixed
16	Function calculate_sample(...) may return false result	Low	Acknowledged
17	Storage variable naming convention may be insecure	Info	Fixed
18	Code duplication	Info	Fixed
19	Error message misspelling	Info	Fixed
20	Event missing in function set_trade_fee(...)	Info	Fixed
21	Function sith_div(...) does incorrect check for the sign	Info	Fixed
22	Function initialize(...) is not emitting an event	Info	Fixed
23	Imprecise inline documentation for SithSwapV1Pair.approve(...)	Info	Fixed
24	Imprecise inline documentation for SithSwapV1Pair.renounceOwnership(...)	Info	Fixed
25	Incomplete inline documentation for SithSwapV1Pair.initialize(...) function	Info	Fixed
26	Incomplete inline documentation for SithSwapV1Pair.sample(...) function	Info	Fixed
27	Inconsistent variable naming	Info	Fixed
28	Inconsistent function naming format	Info	Fixed
29	Lower execution cost opportunity in claim_fees_for(...) function	Info	Fixed
30	Math operations suboptimal performance	Info	Fixed
31	Misspelled variables	Info	Fixed
32	Missing check whether _compute_address is correct	Info	Fixed
33	Non-uniform style of accessing namespace-encapsuled functions	Info	Fixed
34	Redundant commented code in calculate_sample(...) function	Info	Fixed
35	Simplify conditional branching may save number of steps	Info	Fixed
36	Unchecked conversion from felt to Uint256	Info	Fixed
37	Underflow may occur in _get_conditional_observation(...) function	Info	Fixed
38	Unsafe conversion from felt to Uint256 type	Info	Fixed
39	Use of 0 and 1 instead of TRUE and FALSE	Info	Fixed
40	Use of magic numbers for fees	Info	Fixed
41	Non-uniform coding style	Info	Fixed

4 Risk Rating Methodology

The risk rating methodology used by [Nethermind](#) follows the principles established by the [OWASP Foundation](#). The severity of each finding is determined two factors: **Likelihood** and **Impact**.

Likelihood is a measure of how likely the finding is to be uncovered and exploited by an attacker. This factor will be one of the following values:

- a) **High**: The issue is trivial to exploit and has no specific conditions that need to be met;
- b) **Medium**: The issue is moderately complex and may have some conditions that need to be met;
- c) **Low**: The issue is very complex and requires very specific conditions to be met.

When defining the likelihood of a finding other factors are also considered. These can include but are not limited to: Motive, opportunity, exploit accessibility, ease of discovery and ease of exploit.

Impact is a measure of the damage that may be caused if the finding were to be exploited by an attacker. This factor will be one of the following values:

- a) **High**: The issue can cause significant damage such as loss of funds or the protocol entering an unrecoverable state;
- b) **Medium**: The issue can cause moderate damage such as impacts that only affect a small group of users or only a particular part of the protocol;
- c) **Low**: The issue can cause little to no damage such as bugs that are easily recoverable or cause unexpected interactions that cause minor inconveniences.

When defining the impact of a finding other factors are also considered. These can include but are not limited: Data/state integrity, loss of availability, financial loss, reputation damage. After defining the likelihood and impact of an issue, the severity can be determined according to the table below.

		Severity Risk		
		Medium	High	Critical
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Info/Best Practices	Low	Medium
	Undetermined	Undetermined	Undetermined	Undetermined
		Low	Medium	High
		Likelihood		

To address issues that do not fit a High/Medium/Low severity, [Nethermind](#) also uses three more finding severities: **Informational**, **Best Practices**, and **Undetermined**.

- a) **Informational** findings do not pose any risk to the application, but they carry some information that the audit team intends to formally pass to the client;
- b) **Best Practice** findings are used when some piece of code does not conform with smart contract development best practices;
- c) **Undetermined** findings are used when we cannot predict the impact or likelihood of the issue.

5 Issues

5.1 General

5.1.1 [Info] Storage variable naming convention may be insecure

File(s): `contracts/cairo/`

Description: Currently some contracts are not following recommended guidelines for storage variable naming. Importing two libraries which contain storage variable named exactly the same in both, may result in storage clashing. It is a good practice to prefix a storage variable name with a unique name (e.g. a namespace that uses this storage variable) to avoid storage clashes.

Recommendation(s): Consider prefixing the name of the storage variable with the name of the namespace that the variable is used by.

Status: Fixed.

Update from the client: Fixed in commit `4c5db4b8288313c00866dbf886448c4669f33325`.

5.1.2 [Info] Use of 0 and 1 instead of TRUE and FALSE

File(s): `contracts/cairo/`

Description: Some expressions are written comparing with 0 or 1 when expecting values that are boolean semantically. For example, checking if a pair is `stable` or not. In other places of the codebase TRUE and FALSE are used, this affects code consistency and readability.

Recommendation(s): Change the code to use TRUE and FALSE on these cases.

Status: Fixed.

Update from the client: Fixed in commit `4fcc6d847d74bd7017d4acafee55485880c4d58`.

5.2 `contracts/cairo/sithswap/amm/factory/factory/SithSwapV1Factory.cairo`

5.2.1 [Low] External initialization function

File(s): `contracts/cairo/sithswap/amm/factory/factory/SithSwapV1Factory.cairo`

Description: Function `SithSwapV1Factory.init(...)` can be called by anyone after contract is deployed. This could allow an attacker to quickly call this function after contract deployment getting ownership of the contract.

Recommendation(s):

- Consider doing contract deployment and initialization in only one transaction;
- Check that contract state is as expected after initialization call;

Status: Fixed.

Update from the client: Fixed in commit `b820cae36b308a423f74b41d4504d6124c38079d`.

5.3 `contracts/cairo/sithswap/amm/factory/factory/library.cairo`

5.3.1 [Medium] Lack of argument validation in `SithSwapV1Factory.create_pair(...)`

File(s): `contracts/cairo/sithswap/amm/factory/library.cairo`

Description: The `stable` input argument in function `SithSwapV1Factory.create_pair(...)` is not validated to ensure it is a boolean. Passing a value outside of the range `[0, 1]` may lead to unexpected behavior. During pair creation, if the argument `stable` is passed a value other than 1 the pair will be marked as volatile. In other parts of the protocol a pair is determined whether it is `stable` or not by checking if `stable` is zero. This means that if a pair is initialized with a value other than 0 or 1 it will be marked as volatile but will behave as a stable pair.

Recommendation(s):

- Consider checking if the `stable` argument is within the range `[0, 1]`;
- Consider making `stable` checks consistent rather than comparing against 0 in some places and 1 in others.

Status: Fixed.

Update from the client: Fixed in commit `3230bc760fd176a2553b7a1ff1bfe7aa42c88dc8`.



5.3.2 [Info] Missing check whether `_compute_address` is correct

File(s): `contracts/cairo/sithswap/amm/factory/library.cairo`

Description: The function `_compute_address` is used in some areas in the protocol to compute the address of a specific pair. Starknet is an evolving ecosystem and in the near future there may be subtle changes in how contract addresses are computed. If this happens, functions relying on `_compute_address` may not work anymore with the newly deployed pairs.

Recommendation(s): Consider adding a check in `create_pair(...)` to ensure that the address returned from `_compute_address` is the same as the address where the pair was deployed.

Status: Fixed.

Update from the client: Fixed in commit `c7d49a368a379e0a8088385ed7d7a63b1ccaa395`.

5.4 `contracts/cairo/sithswap/amm/fees/library.cairo`

5.4.1 [Info] Lower execution cost opportunity in `claim_fees_for(...)` function

File(s): `contracts/cairo/sithswap/amm/fees/library.cairo`

Description: Function `claim_fees_for(...)` transfers claimed amounts of `token0` and `token1` to the recipient address. However, there is no check to ensure that `amount0` and `amount1` are greater than zero. This may lead to sending `0` tokens and making the cost of executing the `claim_fees_for(...)` function higher.

Recommendation(s): Consider transferring tokens in `claim_fees_for(...)` only if amounts are greater than zero.

Status: Fixed.

Update from the client: Fixed in commit `566bed20f134c47291131ee3f900532c730e32d3`.

5.5 `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

5.5.1 [Low] `SithSwapV1Pair.approve(...)` function is inconsistent with the ERC20 standard

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: The `SithSwapV1Pair.approve(...)` function does not return a value. However, the **ERC20** standard states that the `approve(...)` function should return a boolean value indicating success. This could cause failures or unexpected behavior when integrating with other protocols.

Recommendation(s): Consider returning a value in `SithSwapV1Pair.approve(...)` to indicate a successful approval.

Status: Fixed.

Update from the client: Fixed in commit `09d452e66ed30479236bd9fb7198588c5f0ab86b`.

5.5.2 [Low] Unsafe approval change

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: The user is allowed to change allowance for LP tokens. This can only be done by calling `SithSwapV1Pair.approve(...)` function. Due to the ERC20 approval race condition attack vector, it is recommended to increase token allowance with the `increase_allowance(...)` function, and decrease token allowance with the `decrease_allowance(...)` function.

Recommendation(s): Consider implementing `increase_allowance(...)` and `decrease_allowance(...)` functions to increase and decrease token allowance respectively.

Status: Fixed.

Update from the client: Fixed in commit `622486cadfa535cd2d9c4c2936593ece21cadd07`.

5.5.3 [Info] Imprecise inline documentation for `SithSwapV1Pair.approve(...)`

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: Inline documentation of `SithSwapV1Pair.approve(...)` function states that the function "*Increases allowance to spender for amount*". This description is misleading, since the function **sets** the allowance.

Recommendation(s): Consider rephrasing existing description of `SithSwapV1Pair.approve(...)` function.

Status: Fixed.

Update from the client: Fixed in commit `029c9c481c5c0a0ec6a0ef13d58ec1402ef5185f`.



5.5.4 [Info] Imprecise inline documentation for `SithSwapV1Pair.renounceOwnership(...)`

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: Inline documentation provided for the `SithSwapV1Pair.renounceOwnership(...)` function states *"This forever removes Pair ownership altogether, except if a Factory owner still exists"*. The second part of the description does not accurately explain behavior of the function. When ownership of the `Pair` is removed, it cannot be restored regardless of existence of the owner of the `Factory` contract. Imprecise documentation may create false assumptions and lead to confusion.

Recommendation(s): Consider rephrasing the description of the `SithSwapV1Pair.renounceOwnership(...)` function to match its behavior.

Status: Fixed.

Update from the client: Added `Pair.reviveOwner()` function to allow `Factory` owner assign new owner to `Pair` and inline comments updated. Fixed in commit `bb0b3cddbcd5edb5e4b983d713754a2225c7c909`.

Update from Nethermind: The new function `Pair.reviveOwner()` would allow the `Factory` owner to change the owner of any pool at any point in time. This was raised to **SithSwap** team and the pros and cons of different solutions were analyzed, concluding that this was the design that better aligns with the protocol needs.

5.5.5 [Info] Incomplete inline documentation for `SithSwapV1Pair.initialize(...)` function

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: The `SithSwapV1Pair.initialize(...)` function lacks inline documentation for `stable`, `fee` and `fees` input arguments.

Recommendation(s): Consider adding descriptions for missing function arguments.

Status: Fixed.

Update from the client: Fixed in commit `d12d3e452a222c06d3e096459e272cc2b97668fc`.

5.5.6 [Info] Incomplete inline documentation for `SithSwapV1Pair.sample(...)` function

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: The `SithSwapV1Pair.sample(...)` function lacks inline documentation for `window` input argument.

Recommendation(s): Consider adding descriptions for missing function arguments.

Status: Fixed.

Update from the client: Fixed in commit `07e9bf398b22ef60b948a06629fde6285f6c1d28`.

5.5.7 [Info] Inconsistent variable naming

File(s): `contracts/cairo/sithswap/amm/pair/SithSwapV1Pair.cairo`

Description: Function `SithSwapV1Pair.transferOwnership(...)` has an argument named `direct`, which is the flag to specify whether the ownership transfer should happen immediately. However in `SithSwapV1Factory.transferOwnership(...)` and `SafeOwnable.transfer_ownership(...)` functions, this flag is called `atomic`. Providing consistent naming of variables holding the same functionality across the codebase increases readability.

Recommendation(s): Consider renaming the `direct/atomic` variables to be consistent across the contracts.

Status: Fixed.

Update from the client: Fixed in commit `c79a018e03caf3d8a27e54c58ffb44d469c3a688`.

5.6 contracts/cairo/sithswap/amm/pair/library.cairo

5.6.1 [Medium] set_trade_fee() function does not correctly check the new value

File(s): contracts/cairo/sithswap/amm/pair/library.cairo

Description: The set_trade_fee(...) function should only allow fee values lower or equal than 3000. This check is shown in the following code snippet.

```
with_attr error_message("SithSwapV1Pair::set_trade_fee: illegal fee"):
  assert_le(_fee, 3000)
end
```

The assertion done by assert_le will pass for values where $3000 - _fee$ is lower than 2^{128} . For large $_fee$ values this will be true, allowing for fees greater than 3000. If the set fee is large enough, fees computed from swaps can be larger than the actual amounts sent to the pool, which can cause liquidity to be drained to the fees contract. Fees can be changed only once in a period of 31 days, causing the pool to be in an invalid state for this amount of time.

Recommendation(s): Use the assert_le_felt() function for checking if the new value is lower than 3000.

Status: Fixed.

Update from the client: Fixed in commit 073880bc8c79a768e8236ad6b20d92d08cb2af8b.

5.6.2 [Low] SithSwapV1Pair.set_trade_fee() freeze period is not applied to all cases

File(s): contracts/cairo/sithswap/amm/pair/library.cairo

Description: The specification for SithSwapV1Pair.set_trade_fee() states *"Both Factory and Pair owner can set it, but only once every 31 days."* This freeze period is only enforced when the caller is the Factory owner and there exists a Pair owner, making the implementation inconsistent with the specification.

Recommendation(s): Ensure that the fees can only be changed once within the defined time period for all cases, or update the specification to match the existing function logic.

Status: Fixed.

Update from the client: set_trade_fee(...) implementation and specification were updated. Fixed in commit 4913c2ced9b8da691b19ca51a2cbc20e4e0f9ac9.

5.6.3 [Info] Event missing in function set_trade_fee(...)

File(s): contracts/cairo/sithswap/amm/pair/library.cairo

Description: The function set_trade_fee(...) is not emitting an event when the fee is changed. Emitting events is useful for monitoring and debugging purpose. It is a good practice to emit an event after state changes.

Recommendation(s): Consider emitting an event on fee update.

Status: Fixed.

Update from the client: Fixed in commit e1e6a925f07fac8d5622db7cc792729f917fc3db.

5.6.4 [Info] Misspelled variables

File(s): contracts/cairo/sithswap/amm/pair/library.cairo

Description: The function last_observation(...) contains the misspelled variable observation_lenght. Function _get_conditional_observation(...) contains the misspelled variable _observation_lenght.

Recommendation(s): Consider renaming misspelled variables.

Status: Fixed.

Update from the client: Fixed in commit 32f106d39258a67f590f66fd4802aeb654a6a90e.



5.6.5 [Info] Unchecked conversion from felt to Uint256

File(s): `contracts/cairo/sithswap/amm/pair/library.cairo`

Description: The function `_k(...)` converts variables `decimals0` and `decimals1` to `Uint256` type without checking if `decimals0` and `decimals1` are less than 2^{128} . This may lead to invalid `Uint256` numbers if `decimals0` or `decimals1` are greater than 2^{128} .

Recommendation(s): Consider checking if conversion `decimals0` and `decimals1` to `Uint256` results in valid `Uint256` type number.

Status: Fixed.

Update from the client: Fixed in commit `6ca10d50106604da1a60e6cfec521e4ce53af471`.

5.6.6 [Info] Underflow may occur in `_get_conditional_observation(...)` function

File(s): `contracts/cairo/sithswap/amm/pair/library.cairo`

Description: The function `_get_conditional_observation(...)` contains the expression `_observation_lenght - 2`. If `_observation_lenght` is less than 2 this will lead to overflow which may result in unexpected behavior.

Recommendation(s): Consider checking if `_observation_lenght` is greater than 1.

Status: Fixed.

Update from the client: Fixed in commit `3e697e90a12ae50ad600f829e863258ea46f22f4`.

5.6.7 [Info] Use of magic numbers for fees

File(s): `contracts/cairo/sithswap/amm/pair/library.cairo`

Description: It is a good practice to use named constants instead of values in the code. The maximum value for fees and also the value representing a fee of 100% (100000) are used directly in the code rather than using a constant.

Recommendation(s): Consider using a constant for these values.

Status: Fixed.

Update from the client: Fixed in commit `9c6238ebc7735cc74a3617505c9ca42f4c0fc550/`

5.7 `contracts/cairo/sithswap/amm/router/SithSwapV1Router01.cairo`

5.7.1 [Medium] Assumption of correct `Uint256` type arguments

File(s): `contracts/cairo/sithswap/amm/router/SithSwapV1Router01.cairo`

Description: The functions in the `SithSwapV1Router01` contract assume that arguments of `Uint256` type are correct - i.e. that members `low` and `high` are integers within the range $[0, 2^{128})$. However the validity of `Uint256` type arguments are not checked for functions in `SithSwapV1Router01`. This is also not checked in most internally called functions. This may lead to unexpected behavior and break functionalities of the protocol.

Recommendation(s): Consider checking if arguments of `Uint256` type are correct by using the `uint256_check(...)` function.

Status: Fixed.

Update from the client: Fixed in commit `ae6255e8c3f2eec8ee056abd211169cf7c510366`.

5.7.2 [Info] Non-uniform style of accessing namespace-encapsulated functions

File(s): `contracts/cairo/sithswap/amm/router/SithSwapV1RouterLibrary.cairo`

Description: The functions `SithSwapV1Router.add_liquidity(...)`, `SithSwapV1Router.swap(...)` and `SithSwapV1Router.swap_supporting_fee_on_transfer_tokens(...)` are referencing functions through the `SithSwapV1Router` namespace. Below we reproduce simplified example:

```
namespace SithSwapV1Router:
  #...
  func add_liquidity{syscall_ptr : felt*, pedersen_ptr : HashBuiltin*, range_check_ptr}(...) -> (...):
    #...
    let (reserve_a, reserve_b) = SithSwapV1Router.get_reserves(token_a, token_b, stable)
    #...
  end
  #...
end
```

We observed presented style of referencing only in `SithSwapV1RouterLibrary.cairo` file. Using multiple styles could decrease readability.

Recommendation(s): Consider unifying referencing style across the codebase.

Status: Fixed.

Update from the client: Fixed in commit `cefd8428bc7676d58b76ddc9df73e266dbbe45`.

5.8 contracts/cairo/sithswap/libraries/Initializable.cairo

5.8.1 [Info] Function `initialize(...)` is not emitting an event

File(s): `contracts/cairo/sithswap/libraries/Initializable.cairo`

Description: An event should be emitted upon contract initialization. Emitting an event on important state changes is a good practice and may help with post-deployment application monitoring and debugging.

Recommendation(s): Emit an event for the initializing operation.

Status: Fixed.

Update from the client: Fixed in commit `fa1bd055c732a61d3ffa7aa30f046d569c27bc0b`.

5.9 contracts/cairo/sithswap/libraries/SafeMath.cairo

5.9.1 [Medium] Function `felt_add(...)` may be insecure

File(s): `contracts/cairo/sithswap/libraries/SafeMath.cairo`

Description: The function `felt_add(...)` may revert even if addition is done properly. The function `is_le(...)` is used to check if `a` is less than or equal to the sum of `a` and `b` with the intention of failing on overflow. `is_le(...)` in fact only checks if `b - a` is within the range $[0, 2^{128})$. This could cause failures even when there is no overflow.

An example of arguments that cause failure without overflow in `felt_add(...)` are: `a = 1` and `b = 2128` leading to `c = 2128 + 1`. The function would revert even though `a < c`, since the difference `c - a = 2128` is out of the range $[0, 2^{128})$ and therefore `is_le(...)` would return `FALSE`.

Recommendation(s): Consider replacing `is_le(...)` with `is_le_felt(...)` function which assumes arguments in range $[0, P)$.

Status: Fixed.

Update from the client: Fixed in commit `73eab1b189c05ddd8366491a115bc79b535e3d98`.

5.9.2 [Medium] Function `felt_mul(...)` does not check for overflow

File(s): `contracts/cairo/sithswap/libraries/SafeMath.cairo`

Description: The functions `SafeMath.felt_add(...)` and `SafeMath.felt_sub(...)` check if overflow occurred, however `SafeMath.felt_mul(...)` does not check for this. It may create confusion since developers using `SafeMath` could assume that `felt_mul(...)` would also check for overflow.

Recommendation(s): Consider checking for overflow in function `SafeMath.felt_mul(...)`.

Status: Fixed.

Update from the client: Fixed in commit `e1e6a925f07fac8d5622db7cc792729f917fc3db`.

5.9.3 [Medium] Function `felt_sub(...)` may be insecure

File(s): `contracts/cairo/sithswap/libraries/SafeMath.cairo`

The function `felt_sub(...)` may revert even if subtraction is done properly. The function `is_le(...)` is used to check if `b` is less than or equal to `a` with the intention of failing on overflow. `is_le(...)` in fact only checks if `a - b` is within the range $[0, 2^{128})$. This could cause failures even when there is no overflow.

An example of arguments that cause failure without overflow in `felt_sub(...)` are: `a = 2128 + 1` and `b = 1` leading to `c = 2128`. The function would revert even though `b < a`, since the difference `a - b = 2128` is out of the range $[0, 2^{128})$ and therefore `is_le(...)` would return `FALSE`.

Recommendation(s): Consider replacing `is_le(...)` with `is_le_felt(...)` function which assumes arguments in range $[0, P)$.

Status: Fixed.

Update from the client: Fixed in commit `ce8ffdd498597f389446a20c5583618e0c72225`.

5.10 `contracts/cairo/sithswap/libraries/SafeOwnable.cairo`

5.10.1 [Info] Inconsistent function naming format

File(s): `contracts/cairo/sithswap/libraries/SafeOwnable.cairo`

Description: The function `SafeOwnable.pendingOwner(...)` is formatted in camel case style. Recommended style for function names in Cairo is snake case. Other functions in this contract are formatted in snake case style. It is good practise to keep naming style consistent for readability.

Recommendation(s): Consider reformatting `SafeOwnable.pendingOwner(...)` function name to snake case.

Status: Fixed.

Update from the client: Fixed in commit `89e0a12bfd6e9ced0c587e7cb26a69b3e05a9230`.

5.11 `contracts/cairo/sithswap/libraries/SithMath.cairo`

5.11.1 [Medium] Missing input validation in `SithMath` functions

File(s): `contracts/cairo/sithswap/libraries/SithMath.cairo`

Description: The functions `sith_add(...)`, `sith_sub(...)`, `sith_div(...)`, `sith_div_1e18(...)`, `sith_mul(...)`, `sith_mul_1e18(...)` does not ensure that the arguments `x` and `y` are valid `Uint256` values. These functions can return unexpected results for invalid `Uint256` values.

This does not put funds at risk because arguments received by this function are checked in external functions in the pair contract. However, as functions are part of a library they may be used in following iterations of the code and could potentially cause issues.

Recommendation(s): Consider checking if arguments are valid `Uint256` values with `check_uint256(...)`.

Status: Acknowledged

Update from the client: Input values for these functions should be checked before calling them. A header was added to the library for making it clear to anyone using these functions. The header was added in the commit `2b90e7278f401c1e6ecfd18370787451640d3436`.

5.11.2 [Medium] Functions using `is_le(...)` may be insecure

File(s): `contracts/cairo/sithswap/libraries/SithMath.cairo`

Description: The functions `sith_add(...)`, `sith_small_mul(...)`, `normalize_decimals(...)` and `normalize_decimals_inv(...)` are using the `is_le(...)` function which checks if the difference between the second and first arguments are within the range $[0, 2^{128})$. If this difference is larger than $2^{128} - 1$ then result from `is_le(...)` is `FALSE`, even if first argument is lesser than the second one. We present exmample of such unwanted behavior below:

```
assert is_le(1, 2 ** 128 + 2) = FALSE
```

Recommendation(s): Consider replacing `is_le(...)` with `is_le_felt(...)` function that checks if `a <= b`, where `a` and `b` are in range $[0, P)$.

Status: Fixed.

Update from the client: Fixed in commit `a6033222d35c175b798374d61a98b75c20d7e3c6`.

5.11.3 [Medium] Incorrect check in function sub_lt(...)

File(s): contracts/cairo/sithswap/libraries/SithMath.cairo

Description: The function name sub_lt(...) implies that it subtracts two uint256 values however the function can only return 0 or fail. If the arguments x and y are both equal to each other the call to the function will pass but for any other value it will fail. The function is shown below.

```
func sub_lt{range_check_ptr}(x : Uint256, y : Uint256) -> (res : Uint256):
  let (res : Uint256) = sith_sub(x, y)
  let assert_res_positive = (res.low + 1) * (res.high + 1)
  with_attr error_message("StihMath: lt-substraction equal zero"):
    assert assert_res_positive = 1
  end
  return (res=res)
end
```

Recommendation(s): Assuming that the function sub_lt(...) should fail if $x \leq y$, it should assert that res is not zero.

Status: Fixed.

Update from the client: Fixed in commit e985aa630e885a6ef55ad93c5dd831f165eca2a9.

5.11.4 [Info] Error message misspelling

File(s): contracts/cairo/sithswap/libraries/SithMath.cairo

Description: The error message is misspelled. Below we present an example of misspelling:

```
error_message("StihMath: ...")
```

Recommendation(s): Consider replacing StihMath with SithMath in error messages.

Status: Fixed.

Update from the client: Fixed in commit 71b37d73c36ac81f68f161a5e6cce84a1c33398e.

5.11.5 [Info] Function sith_div(...) does incorrect check for the sign

File(s): contracts/cairo/sithswap/libraries/SithMath.cairo

Description: The function sith_div(...) was introduced to lower cost of execution for the division operation. If the provided argument x (divident) is less than 2^{125} , the function sith_small_div(...) is used, since it is optimized for dividing numbers within the range $[0, 2^{125})$. If x is higher than 2^{125} division is done by uint256_unsigned_div_rem(...) function from the standard library.

Since comparison is done by subtracting 2^{125} from x.low and checking if sign(y_sub_125) is equal to 0, sith_small_div(...) is only used if x is equal to 2^{125} because sign(...) returns 0 only when argument is 0.

```
func sith_div{range_check_ptr}(x : Uint256, y : Uint256) -> (res : Uint256):
  alloc_locals
  # checking if y.low < 2^{125} to call sith_small_div
  local y_sub_125 = y.low - 2 ** 125
  let (local y_sub_125_sign) = sign(y_sub_125)
  if y.high == 0:
    if y_sub_125_sign == 0:
      let (res : Uint256) = sith_small_div(x, y.low)
      return (res=res)
    end
  end
  let (local res : Uint256, _) = uint256_unsigned_div_rem(x, y)
  return (res=res)
end
```

Recommendation(s): Consider changing condition checks for running sith_small_div(...) in sith_div(...) function.

Status: Fixed.

Update from the client: Fixed in commit 401de8f6d26c9c39b3bf4d2ddc2e160c01c4dd3a.



5.11.6 [Info] Math operations suboptimal performance

File(s): `contracts/cairo/sithswap/libraries/SithMath.cairo`

Description: Addition (`sith_add(...)`) and multiplication (`sith_mul(...)`) functions are suboptimal with comparison to the functions from standard `uint256` library. The `sith_div(...)` division function is suboptimal for numbers higher than 2^{128} .

Recommendation(s): Consider usage of functions from standard `uint256` library for addition, multiplication and division operations.

Status: Fixed.

Update from the client: Fixed in commit `71b37d73c36ac81f68f161a5e6cce84a1c33398e`.

5.11.7 [Info] Simplifying conditional branching may save number of steps

File(s): `contracts/cairo/sithswap/libraries/SithMath.cairo`

Description: Functions `sith_add(...)`, `sith_sub(...)`, `sith_mul_1e18(...)`, `sith_mul(...)` and `sith_div(...)` are currently using nested branching to check if numbers are equal 0. We reproduce the described example below:

```
if x.high == 0:
  if y.high == 0:
    local low_add = x.low + y.low
    let (carry) = is_le(2 ** 128, low_add)
    let low = low_add - (2 ** 128 * carry)
    let high = carry
    return (res=Uint256(low, high))
  end
end
```

Nested branching is not a good practice since it reduces code readability. It is also not an optimal solution since every branch increases the number of steps.

Recommendation(s): Consider refactoring nested conditional branches into one branch with multiple conditions. We present example of such comparison below:

```
if a == 0 and b == 0:
  ...
end
```

This solution may be more readable and saves small number of steps.

Status: Fixed.

Update from the client: Fixed in commit `4977b5dcb84d21d2c2c14f3e40e5c2fb4795d056`.

5.12 `contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo`

5.12.1 [Medium] Constructor argument is not validated

File(s): `contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo`

Description: The input argument `_factory` is passed to the constructor, but is never validated. It is not possible to change the provided factory address later in the code. Passing 0 or an incorrect address would put the system in an unusable state where it is not possible to recover and the contract will have to be re-deployed.

Recommendation(s): Consider checking if the passed address is not 0 in order to reduce chances of incorrect deployment.

Status: Fixed.

Update from the client: Fixed in commit `2a34ead431c52d7d3556a4178dc1d8d03f59df70`.

5.12.2 [Info] Code duplication

File(s): `contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo`

Description: The functions `getTradeDiff(...)` and `getTradeDiffByPair(...)` are similar in functionality and therefore partly share the same code. It is a good practice to not duplicate the code.

Recommendation(s): Consider refactoring code so the aforementioned functions do not contain duplicated code.

Status: Fixed.

Update from the client: Fixed in commit `1b867334062633621bbfb7e8bbf88f957c51b9b4`.

5.12.3 [Info] Unsafe conversion from felt to Uint256 type

File(s): contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo

Description: The functions `getTradeDiff(...)`, `getTradeDiffByPair(...)`, `getSample(...)`, `getMinimumValue(...)` and `getAmountOut(...)` convert variables `d0` and `d1` to `Uint256` type without checking if `d0` and `d1` are less than 2^{128} . This may lead to invalid `Uint256` values if `d0` or `d1` are greater or equal to 2^{128} .

Recommendation(s): Consider checking if conversion `d0` and `d1` to `Uint256` results in valid `Uint256` type number with function `uint256_check(...)` or by checking if `d0` and `d1` are less than 2^{128} .

Status: Fixed.

Update from the client: Fixed in commit [6ca10d50106604da1a60e6cfec521e4ce53af471](#).

5.12.4 [Info] Non-uniform coding style

File(s): contracts/cairo/sithswap/amm/math/L03/SithSwapV1Library03.cairo

Description: Contract `SithSwapV1Library03` wraps all the functions in the `SithSwapV1Library03` namespace. This approach is different than the rest of contracts in the project. Keeping a uniform style across the codebase increases readability.

Recommendation(s): Consider unifying style of contracts across the codebase.

Status: Fixed.

Update from the client: Fixed in commit [5fbc54694cab4da0de56324fe2eda803f8074c18](#).

5.13 contracts/cairo/sithswap/amm/math/L03/library.cairo

5.13.1 [Medium] Incorrect computation in `_get_y_inner_kconv(...)` function

File(s): contracts/cairo/sithswap/amm/math/L03/library.cairo

Description: The function `_get_y_inner_kconv(...)` should return `size_flag` equal to `0` when it converges and `size_flag` equal to `1` when it does not converge. When calling this function, if no base condition is met, the function will call itself recursively and will always return `1` for the `size_flag` value.

Value `size_flag` returned by `_get_y_inner_kconv(...)` is checked in `get_y(...)` and if it is other than `0` it will fail. This creates scenarios, in which `get_y(...)` will fail even with convergence over `k`.

Described function is shown below:

```
func _get_y_inner_kconv{range_check_ptr : felt}(
  x0 : Uint256, xy : Uint256, y : Uint256, size : felt
) -> (res : Uint256, size_flag : felt):
  alloc_locals
  if size == 0:
    return (res=y, size_flag=1)
  end
  let (local k : Uint256) = SithSwapV1Library.f(x0, y)
  let (local sign_sub_k_xy) = uint256_le(xy, k)
  let (local new_y : Uint256) = _calculate_new_y(sign_sub_k_xy, x0, xy, y, k)
  local k_dif = k.low - xy.low
  if k_dif == 1 and k.high == xy.high:
    return (res=new_y, size_flag=0)
  end
  if k_dif == 0 and k.high == xy.high:
    return (res=new_y, size_flag=0)
  end
  let (local res, _) = _get_y_inner_kconv(x0, xy, new_y, size - 1)
  return (res=res, size_flag=1)
end
```

Recommendation(s): Consider refactoring `_get_y_inner_kconv(...)` function to return the `size_flag` value returned by the recursive call.

Status: Fixed.

Update from the client: Fixed in commit [bd3da5e573a49f106a069788edbeba65d049535b](#).



5.13.2 [Low] Function calculate_sample(...) may return false result

File(s): contracts/cairo/sithswap/amm/math/L03/library.cairo

Description: The function calculate_sample(...) may incorrectly return 0 under certain conditions. calculate_sample(...) multiplies the reserve amount of the first token by the decimals of the second token, and then the product is divided by the reserve amount of the second token. We reproduce described function below:

```
func calculate_sample{range_check_ptr}{
  order_flag : felt, r0 : Uint256, r1 : Uint256, d0 : Uint256, d1 : Uint256
} -> (res : Uint256):
  alloc_locals
  if order_flag == 1:
    # let (d1_pow) = pow(10, d1)
    let (t1) = SithMath.sith_mul(r0, d1)
    let (res) = SithMath.sith_div(t1, r1)
    return (res=res)
  end
  # let (d0_pow) = pow(10, d0)
  let (t2) = SithMath.sith_mul(r1, d0)
  let (res) = SithMath.sith_div(t2, r0)
  return (res=res)
end
```

When the decimal values for the two tokens differ, a rounding error may occur. In the following example we present values that would lead to incorrect result:

```
r0 = 10      # Reserve amount token 0
d0 = 10      # Decimals token 0
r1 = 10000   # Reserve amount token 1
d1 = 100     # Decimals token 1
order_flag = 1
```

With data above, calculate_sample(...) would perform the computation $r0 * d1 / r1$, which would be evaluated as $10 * 100 / 10000$. The result of the computation in this case would be 0. This result is incorrect since the $r0$ to $r1$ ratio (denominated in $d0$ and $d1$ respectively) is 1:100, not 1:0. This may lead to false result of computation.

Recommendation(s): Consider normalization of the both tokens reserve amounts before computing the ratio.

Status: Acknowledged.

Update from the client: The function in question is only accessed by a UI helper contract, furthermore, the conditions required by the issue are practically impossible to occur under any economically meaningful scenario.

5.13.3 [Info] Commented code in calculate_sample(...) function

File(s): contracts/cairo/sithswap/amm/math/L03/library.cairo

Description: The function contain lines of commented code. It is a good practise to remove commented code.

```
func calculate_sample{range_check_ptr}{
  order_flag : felt, r0 : Uint256, r1 : Uint256, d0 : Uint256, d1 : Uint256
} -> (res : Uint256):
  alloc_locals
  if order_flag == 1:
    # let (d1_pow) = pow(10, d1)
    let (t1) = SithMath.sith_mul(r0, d1)
    let (res) = SithMath.sith_div(t1, r1)
    return (res=res)
  end
  # let (d0_pow) = pow(10, d0)
  let (t2) = SithMath.sith_mul(r1, d0)
  let (res) = SithMath.sith_div(t2, r0)
  return (res=res)
end
```

Recommendation(s): Consider removing commented parts of the code.

Status: Fixed.

Update from the client: Fixed in commit [5e549079804ad63dd47db1c6475b9b10132ea23f](https://github.com/NethermindEth/sithswap/commit/5e549079804ad63dd47db1c6475b9b10132ea23f).

6 Documentation Evaluation

Technical documentation is designed to explain the software product in a way that developers, users and the whole community can easily follow the purpose and the underlying functionality of each file/function/line. Documentation can appear not only in the form of a README.md, but also using **code as documentation**, diagrams, websites, research papers, videos and other sources as well. Specifically, code as documentation is a software engineering practice where the code is written in such a way that it serves as its own explanatory documentation. It can be achieved by using meaningful names for variables, functions and methods following an intuitive design that can be easily understood by readers.

The documentation is sufficient for the purpose of this audit. The team provided an high level documentation for the protocol which is publicly accessible. The team also provided multiple files explaining the purpose of most of the externally accessible functions together with a diagram explaining expected interactions between different contracts in the protocol.

Documentation was provided for the SithSwapV1Library03 library explaining its structure, approach and motivation. All the questions that were unanswered by this document were quickly addressed by the SithSwap team through communication channels.

Beyond these files, the code contains comments in a **NatSpec** format for the functions that will be accessible for the users. These comments describe the function purpose, arguments and return values.

Alongside the documentation, a reference implementation written in Solidity was provided to assist the audit team in verifying that the Cairo contracts function as intended. During the assessment, the SithSwap team created new documentation about different tests done for checking performance of the new math library or fixing found issues.

7 Test Suite Evaluation

The protocol presents an extensive test suite using multiple frameworks like **Ape**, and **Protostar**. The CI pipeline tests run on every commit pushed to **master** and **03** branches.

Below, we present output of the different test suites.

7.1 Ape Cairo (math)

```

===== test session starts =====
platform linux -- Python 3.9.13, pytest-6.2.5, py-1.11.0, pluggy-0.13.1 --
↳ /home/runner/.cache/pypoetry/virtualenvs/sithswap-C2YYCxA-py3.9/bin/python
cachedir: .pytest_cache
SithSwap: welcome to the dark side of the Force
rootdir: /home/runner/work/core-amm/core-amm, configfile: setup.cfg
plugins: eth-ape-0.3.5, ordering-0.6, typeguard-2.13.3, asyncio-0.19.0, web3-5.30.0
asyncio: mode=auto
collecting ... collected 40 items
INFO: Starting 'starknet-devnet' process.

tests/cairo/test_SithSwapV1Library.py::test_k[175379405890453581290311239239-3333333333334849839438483-0-10000000000000000-10000000000000000]
WARNING: The connected provider does not support snapshotting. Tests will not be completely isolated.
SUCCESS: Contract 'cairo.sithswap.amm.factory.SithSwapV1Factory' deployed to:
↳ 0x02B83B23905401a1d1C3344BFACE17c61A4C33460Dd9cfd9ff5c013ED728a8ee
SUCCESS: Contract 'cairo.sithswap.mocks.math.SithSwapV1Library02Mock' deployed to:
↳ 0x06bF4181Bba833eee7970383Db20c1705bDd131dF81E2625B994Ceb832e5A611
SUCCESS: Contract 'cairo.sithswap.mocks.math.SithSwapV1Library03Mock' deployed to:
↳ 0x022187b74eEe0130a1aAa55672a32B7ad19cbC1A02FB9686dda691F75EeB6AF7

LOG: [02] `k`: (312195842913757207366000367921663185093, 1717979173957424)
LOG: [02] steps: 32900000000000
LOG: [03] `k`: (312195842913757207366000367921663185093, 1717979173957424)
LOG: [03] steps: 34400000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_k[175379405890453581290311239239-3333333333334849839438483-1-10000000000000000-10000000000000000]

LOG: [02] `k`: (99013587949947838045883114639493647809, 52841493519022963104)
LOG: [02] steps: 37760000000000
LOG: [03] `k`: (99013587949947838045883114639493647808, 52841493519022963104)
LOG: [03] steps: 28840000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_k[175379405890453581290311239239-97-0-10000000000000000-10000000000000000]

LOG: [02] `k`: (17011802371373997385160190206183, 0)
LOG: [02] steps: 32900000000000
LOG: [03] `k`: (17011802371373997385160190206183, 0)
LOG: [03] steps: 34400000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_k[175379405890453581290311239239-97-1-10000000000000000-10000000000000000]

LOG: [02] `k`: (523247928761766648430216292352317547, 0)
LOG: [02] steps: 37760000000000
LOG: [03] `k`: (523247928761766648430216292352317547, 0)
LOG: [03] steps: 25100000000000
PASSED
    
```



```
tests/cairo/test_SithSwapV1Library.py::test_d[33333333333333333333333333333333-29]
LOG: [02] `d`: (60115566451855299017576580328109442237, 108842069520582)
LOG: [02] steps: 259100000000000
LOG: [03] `d`: (60115566451855299017576580328109442237, 108842069520582)
LOG: [03] steps: 183800000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_d[7777777777777777777777777777777755555555555-33333333334849839438483]
LOG: [02] `d`: (53660195373243829851521656801686257633, 1382697401688)
LOG: [02] steps: 280800000000000
LOG: [03] `d`: (53660195373243829851521656801686257633, 1382697401688)
LOG: [03] steps: 220200000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_d[300000000000000000-1000000000000000]
LOG: [02] `d`: (360000000000000000, 0)
LOG: [02] steps: 280800000000000
LOG: [03] `d`: (360000000000000000, 0)
LOG: [03] steps: 237500000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_d[79570000000000000000-79790000000000000000]
LOG: [02] `d`: (202352216760400000000000000000, 0)
LOG: [02] steps: 280800000000000
LOG: [03] `d`: (202352216760400000000000000000, 0)
LOG: [03] steps: 223500000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_d[1111111111000000000000000001-1111111111000000000000000001]
LOG: [02] `d`: (11994552949891529374254802912408504396, 16124751)
LOG: [02] steps: 280800000000000
LOG: [03] `d`: (11994552949891529374254802912408504396, 16124751)
LOG: [03] steps: 238500000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_d[33333333333333000000000000000001-3333333333000000000000000001]
LOG: [02] `d`: (89130642838695495809360963117957167788, 108874722141105)
LOG: [02] steps: 280800000000000
LOG: [03] `d`: (89130642838695495809360963117957167788, 108874722141105)
LOG: [03] steps: 234100000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[1-17537940589045358129031123-3333333333334849839438483]
LOG: [02] `_get_y`: (259812194696352991420803655, 0)
LOG: [03] `_get_y`: (259812194696352991420803655, 0)
LOG: [02] steps: 18238300000000000
LOG: [03] steps: 12174200000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[1-3333333333334849839438483-175379405890453581290311239239]
LOG: [02] `_get_y`: (149380158218594810550442073, 0)
LOG: [03] `_get_y`: (149380158218594810550442073, 0)
LOG: [02] steps: 16843600000000000
LOG: [03] steps: 11251900000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[175379405890453581290311239239-1-3333333333334849839438483]
LOG: [02] `_get_y`: (1, 0)
LOG: [03] `_get_y`: (1, 0)
LOG: [02] steps: 22493000000000000
LOG: [03] steps: 16374000000000000
PASSED
```

```
tests/cairo/test_SithSwapV1Library.py::test_get_y[175379405890453581290311239239-3333333333334849839438483-1]
LOG: [02] `get_y`: (1, 0)
LOG: [03] `get_y`: (1, 0)
LOG: [02] steps: 710100000000000
LOG: [03] steps: 463900000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[17537940589045358129031123-17537940589045358129031123
-17537940589045358129031123]
LOG: [02] `get_y`: (3252, 0)
LOG: [03] `get_y`: (3252, 0)
LOG: [02] steps: 526670000000000
LOG: [03] steps: 373410000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[175379405890453581290311239239-3333333333334849839438483
-17537940589045358129031123]
LOG: [02] `get_y`: (1, 0)
LOG: [03] `get_y`: (1, 0)
LOG: [02] steps: 224900000000000
LOG: [03] steps: 161900000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[11111111100000000000000001-3333333333333300000000000000003
-55555555500000000000000007]
LOG: [02] `get_y`: (2430000008, 0)
LOG: [03] `get_y`: (2430000008, 0)
LOG: [02] steps: 12283100000000000
LOG: [03] steps: 9053100000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[5555555555000000000000000001-333333333333330000000000000003
-11111111100000000000000007]
LOG: [02] `get_y`: (2, 0)
LOG: [03] `get_y`: (2, 0)
LOG: [02] steps: 295400000000000
LOG: [03] steps: 206450000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_y[5555555555000000000000000001-333333333333330000000000000003
-11111111100000000000000007]
LOG: [02] `get_y`: (2, 0)
LOG: [03] `get_y`: (2, 0)
LOG: [02] steps: 379090000000000
LOG: [03] steps: 291490000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[1-1-1-1000000000000000-1000000000000000-0]
LOG: [02] `get_amount_out`: (0, 0)
LOG: [03] `get_amount_out`: (0, 0)
LOG: [02] steps: 76500000000000
LOG: [03] steps: 73700000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[1-1000000000000000-1000000000000000-1000000000000000
-1000000000000000-1]
LOG: [02] `get_amount_out`: (0, 0)
LOG: [03] `get_amount_out`: (0, 0)
LOG: [02] steps: 140480000000000
LOG: [03] steps: 108100000000000
PASSED
```



tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[13000000300000000000000000-77777777555555500000000000000000-9999933333333333333333000000000000000000-100000000000000000-100000000000000000-0]

LOG: [02] `get_amount_out`: (167141740496954542651089623347378, 0)
LOG: [03] _get_amount_out: (167141740496954542651089623347378, 0)
LOG: [02] steps: 76200000000000
LOG: [03] steps: 69500000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[13000000300000000000000000-77775555000000000000000000-999993333300000000000000000-100000000000000000-100000000000000000-1]

LOG: [02] `get_amount_out`: (9965159225630548860207798153, 0)
LOG: [03] _get_amount_out: (9965159225630548860207798153, 0)
LOG: [02] steps: 60603000000000000
LOG: [03] steps: 46392000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[1000000000000000000000003-555555555000000000000000-3333333333333333333333000000000000000000-100000000000000000-100000000000000000-0]

LOG: [02] `get_amount_out`: (589390962729802642704302830994262, 0)
LOG: [03] _get_amount_out: (589390962729802642704302830994262, 0)
LOG: [02] steps: 765000000000000
LOG: [03] steps: 737000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[5000000000000000000000003-555555500000000000000000-7777777700000000000000000-100000000000000000-100000000000000000-1]

LOG: [02] `get_amount_out`: (1498580241904320373574033179, 0)
LOG: [03] _get_amount_out: (1498580241904320373574033179, 0)
LOG: [02] steps: 60603000000000000
LOG: [03] steps: 45207000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[1000000000000-555555333333330000-555555333333333000000000000000-100000-1000000000000000000-0]

LOG: [02] `get_amount_out`: (99999820003173993802970925815133, 0)
LOG: [03] _get_amount_out: (99999820003173993802970925815133, 0)
LOG: [02] steps: 762000000000000
LOG: [03] steps: 695000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[1000000000000000-5555553333333300000000000000-55555533333333333300000000000000-100000-1000000000000000000-0]

LOG: [02] `get_amount_out`: (100000000000004199400167, 0)
LOG: [03] _get_amount_out: (100000000000004199400167, 0)
LOG: [02] steps: 762000000000000
LOG: [03] steps: 695000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[30000000000000003-1155555550000000-55555533330000000000000000-100000000-100000000000000000-0]

LOG: [02] `get_amount_out`: (1405810627986214194957583167, 0)
LOG: [03] _get_amount_out: (1405810627986214194957583167, 0)
LOG: [02] steps: 765000000000000
LOG: [03] steps: 737000000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[3000000000000003-1155555550000000-555533330000000000000000-100000000-100000000000000000-1]

LOG: [02] `get_amount_out`: (229659993954020691912420783, 0)
LOG: [03] _get_amount_out: (229659993954020691912420783, 0)
LOG: [02] steps: 52901000000000000
LOG: [03] steps: 39887000000000000
PASSED


```

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[33333333333330000000000000000003-115555555555550000
000000000000-555553333777777777700000000-1000000000000000-100000000-0]

LOG: [02] `_get_amount_out`: (155762616947026086739179666, 0)
LOG: [03] `_get_amount_out`: (155762616947026086739179666, 0)
LOG: [02] steps: 76500000000000
LOG: [03] steps: 66700000000000
PASSED

tests/cairo/test_SithSwapV1Library.py::test_get_amount_out[3333333000000000000000003-1155555500000000000000000-55555
7777700000000-100000000000000000-100000000-1]

LOG: [02] `_get_amount_out`: (52476746809459997, 0)
LOG: [03] `_get_amount_out`: (52476746809459997, 0)
LOG: [02] steps: 4520200000000000
LOG: [03] steps: 3301800000000000
PASSED
INFO: Stopping 'starknet-devnet' process.

===== 40 passed in 443.14s (0:07:23) =====

```

7.2 Ape Cairo (core - Factory)

```

===== test session starts =====
platform linux -- Python 3.9.13, pytest-6.2.5, py-1.11.0, pluggy-0.13.1 --
↳ /home/runner/.cache/pypoetry/virtualenvs/sithswap-C2YYCzxA-py3.9/bin/python
cachedir: .pytest_cache
SithSwap: welcome to the dark side of the Force
rootdir: /home/runner/work/core-amm/core-amm, configfile: setup.cfg
plugins: eth-ape-0.3.5, ordering-0.6, typeguard-2.13.3, asyncio-0.19.0, web3-5.30.0
asyncio: mode=auto
collecting ... collected 1 item
INFO: Starting 'starknet-devnet' process.

tests/cairo/test_SithSwapV1Factory.py::test_factory
WARNING: The connected provider does not support snapshotting. Tests will not be completely isolated.
SUCCESS: Contract 'cairo.sithswap.amm.factory.SithSwapV1Factory' deployed to:
↳ 0x04B185474DccF279364C857F6F84c9dDFBC42EDd359a5B803e8a67D97e6786Ee
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0083A8212751e0570aCaDc3f036Afaf8d2004179F693c47612a7b2c26A2a72A6
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0239C9A21b22c4ff89C575FD8f1769f7Ae731aA48395f420446C900beB2C8C26
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x056CF9DEF9e782A35308f801D53350004692aBeb3F3BB95DA48de95A0B9bC1d6
LOG: pair_code_hash: 3352931706048919474844077695034476280974373978651495137909581957287310792635
LOG: fees_code_hash: 2089195524015445278712589678407412562190959021678001175009865006858454927751
LOG: V pair creation fee: 5946500000000000
LOG: pair address: 53576290847541242211170904032626472154579245651396369759778292672084924713
LOG: S pair creation fee: 5946600000000000
LOG: last_pair: 53576290847541242211170904032626472154579245651396369759778292672084924713
LOG: CREATE2 pair address: 53576290847541242211170904032626472154579245651396369759778292672084924713
LOG: CREATE2 fees address: 79711105545058944584323825373594923350991674303618664312515296549566776996
LOG: pair: 0x001e52B7134F321EE46dF255C60d83EE4FE19F7Fb755F83C73E29cCF3D055929
LOG: metadata: [1, 0, 232617352691330520716693378237376202847033496614773113407657791740967547558,
↳ 1006727601243700892941852200205990445460895297133611583085895965642792406054, 1000000000000000000,
↳ 100000000000000000]
LOG: pair_owner: 0x689b5912b28116e838e391ad6faa2b6b739006691aa78373d96db4ae310cfe3
LOG: factory_address: 0x04B185474DccF279364C857F6F84c9dDFBC42EDd359a5B803e8a67D97e6786Ee
factory_owner: 295718826920018441125599937111091253445605066208535325081986593780030033891
PASSED
INFO: Stopping 'starknet-devnet' process.

===== 1 passed in 191.97s (0:03:11) =====

```

7.3 Ape Cairo (core - Pair)

```

===== test session starts =====
platform linux -- Python 3.9.13, pytest-6.2.5, py-1.11.0, pluggy-0.13.1 --
  /home/runner/.cache/pypoetry/virtualenvs/sithswap-C2YYCxA-py3.9/bin/python
cachedir: .pytest_cache
SithSwap: welcome to the dark side of the Force
rootdir: /home/runner/work/core-amm/core-amm, configfile: setup.cfg
plugins: eth-ape-0.3.5, ordering-0.6, typeguard-2.13.3, asyncio-0.19.0, web3-5.30.0
asyncio: mode=auto
collecting ... collected 22 items
INFO: Starting 'starknet-devnet' process.

tests/cairo/test_SithSwapV1Pair.py::test_pair[1-0-1000-1-4-2-1-2]
WARNING: The connected provider does not support snapshotting. Tests will not be completely isolated.
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
  ↪ 0x05C120c30b1E7BCE301f2b7B31527FE9D84132AdBE27d7B364d1A0b30f148032
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
  ↪ 0x01b125Bb85DD8C3aF06c89e0ae0d29Fc92e5C20720Ca50456a92E44b3D56f2bC
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
  ↪ 0x0688B12caaE1a1d052dA0aD17EB839992d674aFDA97D7873Aa3c7eA36b3fe080
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
  ↪ 0x067Af6e027e91038a67236BF1B5669952994d311dFACbbC1a3257d30282941b
SUCCESS: Contract 'cairo.sithswap.amm.fees.SithSwapV1Fees' deployed to:
  ↪ 0x056b36c6a25a181B6F5fa51A8Be87e6A24e6DAc1F26a2bc9E39Be30D0ebaC584
LOG: pair contract at: 0x067Af6e027e91038a67236BF1B5669952994d311dFACbbC1a3257d30282941b
pid 1
stable 0
token0 0x01b125Bb85DD8C3aF06c89e0ae0d29Fc92e5C20720Ca50456a92E44b3D56f2bC
_token0 0x1b125bb85dd8c3af06c89e0ae0d29fc92e5c20720ca50456a92e44b3d56f2bc
token1 0x05C120c30b1E7BCE301f2b7B31527FE9D84132AdBE27d7B364d1A0b30f148032
_token1 0x5c120c30b1e7bce301f2b7b31527fe9d84132adbe27d7b364d1a0b30f148032
dec0 1000000000000000000
dec1 1000000000000000000
LOG: ADD LIQUIDITY
LOG: Token Amounts: 1000000000000000000 / 400000000000000000
LOG: Deployer Balances: (1000000000000000000000, 0) / (10000000000000000000000, 0)
expected LP: 1999999999999999000
LOG: burn_amount: 1999999999999999000
LOG: deployer_lp_amount: 1999999999999999000
LOG: pair_token0_bal: 500
LOG: pair_token1_bal: 2000
LOG: reserve0: 500
LOG: reserve1: 2000
LOG: SWAP T-0
LOG: swap_amount0: 1000000000000000000
LOG: Deployer T-0 Balance: 999999999999999999999999999999500
LOG: reserve0: 10000000000000000501
LOG: reserve1: 4000000000000002001
LOG: pair_balance0: 10100000000000000501
LOG: trade_fee0: 100000000000000000
LOG: pair_balance1: 4000000000000002001
LOG: token1 total supply: 10000000000000000000000000000000
LOG: SWAP T-1
LOG: decimals1 18
LOG: swap_amount1 1000000000000000000
LOG: Deployer T-1 Balance: 999999603921180314882659648
LOG: reserve0: 10099000000000000501
LOG: reserve1: 396078819685117340352
LOG: reserve0: 10099000000000000501
LOG: reserve1: 396078819685117340352
LOG: pair_balance0: 10099000000000000501
LOG: token0_out 251795394257564731
LOG: pair_balance1: 397078819685117340352
LOG: new_trade_fee1: 100000000000000000
LOG: token1 total supply: 10000000000000000000000000000000
LOG: trade fee1: 100000000000000000
PASSED

```



```
tests/cairo/test_SithSwapV1Pair.py::test_name_and_symbol
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x033E9987eEd05d25d886D9326bfe98b5BebeD0216542CD7ED7cD5Cd8EEAbc2E4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0036097F130c9d533f5446022789a9a8fe7DeACA03e8400f21DF191c98D1c7a9
LOG: symbol0 = '', symbol1 = ''
LOG: stable = 1, pid = 3625009
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x04E57fc9f41E7b0910e5f37F835FD73D45a74345989599986b3149d4F719dd4
LOG: stable = 0, pid = 8810934
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x05186fcb24e0071AFaFB5485992FFa8A371688A255F0Be79CA88E9FA7E82C665
LOG: symbol0 = '', symbol1 = ''
LOG: stable = 1, pid = 2093034
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x01A360d754e17D4bAbFD0C37cFF12CB9Aa75471c7535d3ff8AdB5c13b62aDFc8
LOG: stable = 0, pid = 3842877
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07fbb7E177d489cD07bb2B978eC020Bc5f024626D059ee2d3b94cd1e1f4d71F5
LOG: symbol0 = '', symbol1 = ''
LOG: stable = 1, pid = 4679693
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x01358A3984c6ADe7296cBa3F4ed463844B5b22f48Ec61d8E5a481dD478a6eae
LOG: stable = 0, pid = 4296348
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x033fb67Ca0eda12002dF9F80B40a5AAcCd4392cb435F1aBB0f49Eb01a39a837
LOG: symbol0 = 'SSSSSSSSSS', symbol1 = 'SSSSSSSSSS'
LOG: stable = 1, pid = 7659698
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07B7d0318eBEde78B83640330c954b6Dc63e226f72121e4b00Cec2bb80Aa4dA5
LOG: stable = 0, pid = 4182489
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0255A5eBc58d9A44D5144c3a98be364BC31d50a7a2234c79295644dF70Eb1255
LOG: symbol0 = 'SYMBOL with 24 character', symbol1 = ''
LOG: stable = 1, pid = 9927435
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x050B3e17600ebfe112932d1442b81777Bf7d4cA72198C3362347FD5e67e5510
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_initialize_revert
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05835f1e4e6FE7967B55fb5919470475D07C19B7D96580C82898fBC1feBab004
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01642f83E18d35c83a00291dBb0aF033B13F29bB2511D7E1A0a3aF3BF911B61
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x03Cc24F9601D3EFB1bBDe96637d340BFA03C3F0A72bDB551A8362e692Cfe34bc
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_raw_pair_ownership
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0632bAE4BC2916cB16caEB17206F6b2d4A0066CCEa25C8E944132ec59eae129b
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04065da6123a42676a71b394959bc2Af7C62f340c0Bc7E22D661Df57b1E418fd
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x008Bed2FB74525dc329279fC9bbB74e908248Ab72BC5f598eBD9ad2668BbD124
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_factory_pair_ownership
SUCCESS: Contract 'cairo.sithswap.amm.factory.SithSwapV1Factory' deployed to:
↳ 0x022ED72457a63130a249a01B2f48099b19c0dA88346002130d6263df51d21f14
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04d05178a3c77Aeb5A946f0a72516322be71c4490E758B0D9114AC9C43923738
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07E7B394FCf8a287eECd26CfaC48691b5a75C0d89C985548e350eD8d75239950
LOG: Pair created: Arguments(pid=1 token0=2177317877702624505273049649121446483369315991217316682959491264930510944056
↳ token1=3575571041355833708217273971872973683755041875975401923011372645690879744336 stable=0 fee=307
↳ fees=1045568970102940113652135638643153037927174049741617453250073929451083017054
↳ pair=3135781077296899234763469442732410337579313501099689062689494681380304790644)
deployer 2957188269200184411255999937111091253445605066208535325081986593780030033891
pair 3135781077296899234763469442732410337579313501099689062689494681380304790644
factory 987385517399515304082448724157081951997182783915017413542556698594614845204
pair.owner() 2957188269200184411255999937111091253445605066208535325081986593780030033891
pair.pendingOwner() 0
PASSED
```



```
tests/cairo/test_SithSwapV1Pair.py::test_volatile_stable_swap[1000000000000000000-1000000000000000000-500000000000000000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02fa450d66a72ce2953b64f5cb129d069a55cadc60a6b1d09aed87a863d0707
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05Ea252672F8D0Fa305e8a7AD7DaA5fd5Ee4c54E066848718f3DdBfA11396195
LOG: Pair created: Arguments(pid=2 token0=1346813706439678180917393727438173555179544289580171009177054992299741480711
↳ token1=2675262857275236823917645272414965280665738836874418196470364108053070569877 stable=0 fee=975
↳ fees=876612305263430244562615401930649236855674683634718692535270565634260845709
↳ pair=1262798733103352357749441224498444770585427376920882489084516610043443385518)
LOG: Pair created: Arguments(pid=3 token0=1346813706439678180917393727438173555179544289580171009177054992299741480711
↳ token1=2675262857275236823917645272414965280665738836874418196470364108053070569877 stable=1 fee=975
↳ fees=579233392680206698933938593237924112454518070261356757472476202274547148780
↳ pair=2148789402966402637965249575310557879362947403373376320338088656065863126392)
LOG: volatile Reserve0 : (1000000000000000000, 0)
LOG: volatile Reserve1 : (1000000000000000000, 0)
LOG: stable Reserve0 : (1000000000000000000, 0)
LOG: stable Reserve1 : (1000000000000000000, 0)
LOG: expected_output_amount_stable : 4950949547557643084
LOG: expected_output_amount_volatile : 4717666535653458153
LOG: volatile Reserve0 after swap : (10495125000000000000, 0)
LOG: volatile Reserve1 after swap : (95282333464346541847, 0)
LOG: stable Reserve0 after swap : (10495125000000000000, 0)
LOG: stable Reserve1 after swap : (95049050452442356916, 0)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_skim_sync
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01c095faC0123C0AD672dc9Dc8bD6d8de07c67ba5897D59fCb3438fB98e7E0D0
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x052Bd12BAB739b9a3706C84F0883263bD8E9957Db52389637962a33e28305176
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x01aef63DD3b3b854052Ba0bE04A3f812ccA179745D61A4BB126F350E7a406CC5
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[1-5-10-1]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03a94c9A8822e56c5429CdaC02e1e250E567fCeb4c756926fbBD7AfCd6c298D5
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06D1e6525fcC639ecF5fCAE1503663418150d41191eae204532E7c43094F3B6A
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03a35737C1dcB078734214f0904adc921168800A31b93d0dFfCD73fd0C0052fa
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07f464CeE0f979a6FeFA2c1fBa8e2E224607Ac5eB7aa42AF1C75f2f4Ce23168a
LOG: Pair created: Arguments(pid=4 token0=1656064398588316065329731528919649287552253620428325098345876136403522459861
↳ token1=3084737750502417715815997701015094377541114771671703249146998305860522818410 stable=1 fee=1000
↳ fees=59132603475485344281862828611700746552855073825529237144238628002224123542
↳ pair=284675851365187228438622497961776976929167124315805325472317525485253551347)
LOG: Pair created: Arguments(pid=5 token0=1645536572453971903035067871116242244251790819638863394831606296504396960506
↳ token1=1656064398588316065329731528919649287552253620428325098345876136403522459861 stable=1 fee=1000
↳ fees=57618666855125989843135783339836819810833869952360378366200504436662481009
↳ pair=2108147394888780438711573152143680370331555419947847265582938474185960824968)
LOG: Pair created: Arguments(pid=6 token0=3084737750502417715815997701015094377541114771671703249146998305860522818410
↳ token1=35979963759650644646464645682660508862807240775099611735435426564686269847178 stable=1 fee=1000
↳ fees=3526291280064367015824738369835270719747055937610104670519523698538791371429
↳ pair=120649969013720336713854823569118866550684431215900267120867315658337128609)
PASSED
```

```
tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[1-3-5-100]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x050b24176db8809f65E9aaBd743c109b5d60Bb5064aBA01f76a1045a8E676e1D
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x063691b3432311246ca22A79f67DFA4aC86226F79d4934DE753536D71D696c02
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00133e4800D1Aed9d77Ba13029D28735Cb2d8a706A8F1Ea74596369F7bd0643a
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04bbb9A2224c0d7f5F1cbc20F7DB3449c353d9580344190A45BBC7d3cb482927
LOG: Pair created: Arguments(pid=7 token0=2281248655131091664390343549052985618091652104978093795068313800429319712285
↳ token1=2810292419118718389007135953843573629100225938301543572201263578421289118722 stable=1 fee=1000
↳ fees=2981085112482264041685411863161550462500572606073299157003616827022313286463
↳ pair=3111757240544120184791802268517734182003489665039431799686125004154689081933)
LOG: Pair created: Arguments(pid=8 token0=33999943706708939817405510014320658639641580110674836576432041803845231674
↳ token1=2281248655131091664390343549052985618091652104978093795068313800429319712285 stable=1 fee=1000
↳ fees=2495384326918274444796888477132468399003118012033236072051594480822831356558
↳ pair=1109026167386599381185329717214530469073428924527239357255785019085317114584)
LOG: Pair created: Arguments(pid=9 token0=2140932989644043948868383939449365442944235036233928383634461372574098532647
↳ token1=2810292419118718389007135953843573629100225938301543572201263578421289118722 stable=1 fee=1000
↳ fees=2927283477187544733265675795834377090433629799735972862963672233763709003459
↳ pair=108364323206964244636057107650512173402297929703643412541636238341566422183)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[5-6-10-100]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06b0b82E7E0984C51384A61E3f72840F6Ce3ACC809a6C133be7B6F12ed7738c2
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01be6eEe54501859ac781C9c74c3e99E8dC055B2c999a9E3C8f8F33217821227
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06AC0223577A66358BE25714AE0477a17e5FBc7cc7C02b77A8f5d23D5008387
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x011FbF695Cd579Fa751c79b0895a00f6c25d60B91Cb04173159636101763C355
LOG: Pair created: Arguments(pid=10 token0=788779408335794875572316257599221581103632225656168028983560115616808571431
↳ token1=3026113349659214613294570051274454795717993384716459711380249609989887834306 stable=1 fee=1000
↳ fees=179442625138314212292335240101317342213377925411140202167603360580564939753
↳ pair=150514342755197929678323904270573707966510573595426669317178228210755988393)
LOG: Pair created: Arguments(pid=11 token0=3017789542944828874287867396821369056769643055466230658647369334351793783687
↳ token1=3026113349659214613294570051274454795717993384716459711380249609989887834306 stable=1 fee=1000
↳ fees=445642858406588526738280900830224086269531316953930213655167752682034076060
↳ pair=197385095587559310432499791129582413921560258007679726101015852612645459187)
LOG: Pair created: Arguments(pid=12 token0=5084061817114583313925948492746843122469726275771209868074975943550174479189
↳ token1=788779408335794875572316257599221581103632225656168028983560115616808571431 stable=1 fee=1000
↳ fees=165012807747667093530682133643256101760998390796946791488828663700158414922
↳ pair=924091894969900536588097088546221004971509719860308406597104194681023985152)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[5-6-1-10000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01F79097219a180e2df91D6BC6E1F65f8b624382E04d81F28696bfa526bC3a1
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05Efd754Cc0c822b9Fde2bf667A4a13a8027d2274898D8A9DCfb22f32c8D1Df7
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00F3BB3f5850b891A4B156333D42FA3906b1Fe79fdDA6fe8B83BC52b8D7FFE84
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x079924fd0920656C446b1650c356bE8426301C9B2629A02881DdD81Ee7a3Dc36
LOG: Pair created: Arguments(pid=13 token0=889721999548108109187055944421285604754857399324878891803887287187066831777
↳ token1=2685326852987298998343776602956445352837564506743650824147502356326523936247 stable=1 fee=1000
↳ fees=1629893274628033001551046444305110040900080883657475288786877019577260412317
↳ pair=2814031319678217819726511664774964110651187645689088297030117339797939569452)
LOG: Pair created: Arguments(pid=14 token0=430636171085325606804904274047316106913444043171650705901490452738642804356
↳ token1=889721999548108109187055944421285604754857399324878891803887287187066831777 stable=1 fee=1000
↳ fees=2327763350368104608682637043587879505671845548614307552678395501930739642969
↳ pair=1045051632287030905395054223754392709727762161484571314095685413835278669206)
LOG: Pair created: Arguments(pid=15 token0=2685326852987298998343776602956445352837564506743650824147502356326523936247
↳ token1=3436772847582701795150369098763645031003355575693595704647674550442275363894 stable=1 fee=1000
↳ fees=299268484786007069269528913317975989999847567052410500494270113915886696683
↳ pair=2550076950622893756512345827463050103717652990911719364093774098581464898475)
PASSED
```

```

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[3-3-5-10000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05274F9E5906295F7164ABc2894E9b40F28429c9958903894F2388F8084F5f2f
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x039439606777780D6F2AA6Ac221F46db9FeE6620776EB3cdAaD78130C9a70dd
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0741918E1338FD4DC240087a96dB7fB8529977d4a81ddFE0A414eB241e0c23d
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x024CA384620e4222A77f31cD5cd63490F11DF5e59F7EB0074B3659c49C83Aa0
LOG: Pair created: Arguments(pid=16 token0=1618827909929958991304097126334837598741992298409128107676939464633581465821
↳ token1=2331020785450987493963109510122136878266173251738737078769181552752876019503 stable=1 fee=1000
↳ fees=575808404299282588343655801631268133329389133507473775105901873980942448110
↳ pair=1400435142044886385250965680370493199557104528763171033533549294276346108238)
LOG: Pair created: Arguments(pid=17 token0=2331020785450987493963109510122136878266173251738737078769181552752876019503
↳ token1=3282039582850548716106326235691494420321679271124272593024293091277059179069 stable=1 fee=1000
↳ fees=3318340843650657949268578769504071629941370393502387393614375266384111766395
↳ pair=1944405330869609233427329610427377565575023484645639156654207789609818310792)
LOG: Pair created: Arguments(pid=18 token0=1040034627783647033419718204020783197303141560163264077887668458451825605280
↳ token1=1618827909929958991304097126334837598741992298409128107676939464633581465821 stable=1 fee=1000
↳ fees=13435969934325311297125281988730771694841581289642037579708430758510562439830
↳ pair=1232782110535825733902118238962848160267583968327719573975284970873469898794)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[2-5-1-10000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0461992046C15038E31A422d86A60E33F294eC822e3B64877c1fc21f0D81dd66
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0683F92D9532ddA572E95959A4DA8118Df83dCB99f4578C43C6aDFc8e24BDF35
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x078D9f2A127ebD100756A380909e5909689097cbfe3B32A00E48b33049be1609
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07E5e0Fbd18A82a953862Ad98D9134D6876E679702cBdE157889A5372FC492A1
LOG: Pair created: Arguments(pid=19 token0=1981692396977306062362355476335389508472820215616019852315779027156238196070
↳ token1=2947053820735973987005944679855113855987050169691764961944418298392497348405 stable=1 fee=1000
↳ fees=2572423292678240598035665324934484965759414787062335415326308518187458621055
↳ pair=1453381931367415290261329957342942811641582755510268511639218110917158654854)
LOG: Pair created: Arguments(pid=20 token0=1981692396977306062362355476335389508472820215616019852315779027156238196070
↳ token1=3416413888151275084547165474919464644687997721204386496900178966144373102089 stable=1 fee=1000
↳ fees=3383271925435320315898551104966179500500476447603163724438626339741366542971
↳ pair=381147526488477488477800626967777926493509263923978775302060544656046330306)
LOG: Pair created: Arguments(pid=21 token0=2947053820735973987005944679855113855987050169691764961944418298392497348405
↳ token1=3572350698112658101966803433583776997463767010874460564472696310346807546529 stable=1 fee=1000
↳ fees=2252088306244681117414555903221569731172560064155251515258431081830222635092
↳ pair=2558165937876897818627860127219362012478954223950985407874465285030215311124)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[1-5-5-10000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01524C592D59CF2Be327eDc5d31dAc86dEc854E0ABBaFE6382EB31D05Cb468b0
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x011a1b153C315546e478890f61b152666B8372c004C0a42153F33D87b70DD8c7
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0748769C7EdFA9061cd145c248F46Da15b7b5E781B42dc0399222CF1e5d0D5C4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x031EB43278c7eab8847bABCe4230Ef7bDf1f8F8AE11fbd788e77411560Ec98a3
LOG: Pair created: Arguments(pid=22 token0=498437791916779702001774518658588163201311560124536493159631064945954511047
↳ token1=597721244828701875799796014173742034041562884198001973652472336729813313712 stable=1 fee=1000
↳ fees=1781732172933801064419987851150577391971838075157118465885910088711831913438
↳ pair=1685767840730413019093072679232265161767810054655790471267906917699726150403)
LOG: Pair created: Arguments(pid=23 token0=597721244828701875799796014173742034041562884198001973652472336729813313712
↳ token1=3294221553928866992577547078318581176741737788319670599760118370834507158980 stable=1 fee=1000
↳ fees=574376677993119440183241268590487467325292553042541799499543819086588707443
↳ pair=23290222460711564904852233202629804021616043391989433197846092405129976379471)
LOG: Pair created: Arguments(pid=24 token0=498437791916779702001774518658588163201311560124536493159631064945954511047
↳ token1=1411187632752622387712343636141985160836009364042796392767867831652755216547 stable=1 fee=1000
↳ fees=582104040605499239441184146221586066196820348968726022344076306635719672656
↳ pair=877321343677119225308730357830761761208838935692695726319025519123804232077)
PASSED
    
```



```
tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[5-5-1-100000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05389b6d21203a1b94431fb7bc3ebc41220521a49a7c6e3780c266be2a4cE795
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02b82963668f00424bb9dff955dd4ea76a52ec5a49bfDCA1C2E4e1C5831b0E1
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04aa42dc7881a661c447a45dCb480AD4A638d73857a000a93A80A17b65b87D1f
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x044f996d2749845d63ab2d94c322DeE5BBABFc0d422C71572047733a3a4ABA0A
LOG: Pair created: Arguments(pid=25 token0=1230011208538626605387924765263618115601674833209993410604005471452035920097
↳ token1=2361580391350423758174724785955016811797899499031578302017765960984650639253 stable=1 fee=1000
↳ fees=2742688742900831496545235532194784277323582462810027225381441962148203960425
↳ pair=2846386265947334928095400641318642326902874464148742521557270053663488492832)
LOG: Pair created: Arguments(pid=26 token0=2110076854483355727480637321903654809491487275178520265312615760402474106143
↳ token1=2361580391350423758174724785955016811797899499031578302017765960984650639253 stable=1 fee=1000
↳ fees=2239862993380278958556823448145545586440371895338683529335672447054913341296
↳ pair=938563106546342967363702911018190594450951438594476121047038178940731737979)
LOG: Pair created: Arguments(pid=27 token0=1230011208538626605387924765263618115601674833209993410604005471452035920097
↳ token1=194989122241322612649060668557653319449867946303225574692319015779724605962 stable=1 fee=1000
↳ fees=1702015165425428045479889454473871163486478552655691198897621390147363796705
↳ pair=756530865448023841532343550153440143097414224798365647585633821682035317155)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_usdc_pairs[2-3-9-100000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03a86Ba178D45643060DF7F1e356E69C2DC0e6a5098992b551266fB12c465d3A
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0269f1b117830e7296295408155644920073aB04cAc2A929f5637667FE436D6e
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03dF955Cf44f5AF7Ad62e123BbdF297d2A2deA453DcB7AF020C30A883789Fe3b
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01DE0E243A6b37Bd0F3387c26B97624E822B4208E48Bd9b15f20880f63c55c08
LOG: Pair created: Arguments(pid=28 token0=1091812734224495941922159999907651438311484013381520802372929248832342158702
↳ token1=1654511692767913093219195280759132884687760024649385143400314275706301734202 stable=1 fee=1000
↳ fees=1478292203603923959659214105348799445126384015760627269957080791195570159477
↳ pair=3161960014741424407481309043509761291636646348153457498353725306829497690944)
LOG: Pair created: Arguments(pid=29 token0=1654511692767913093219195280759132884687760024649385143400314275706301734202
↳ token1=1751976307444988103734814461508615822284320610969104197241418137276636593723 stable=1 fee=1000
↳ fees=327574753472604172166090909684481200859074983600310104594547781184792241846
↳ pair=2769243119740638995985283338352381681303425909987640332430037682656897776873)
LOG: Pair created: Arguments(pid=30 token0=844650498123222526878928775590905399458388721478679238105697453645914004488
↳ token1=1091812734224495941922159999907651438311484013381520802372929248832342158702 stable=1 fee=1000
↳ fees=416944532941759514160581957816538976582519456143834437857090980563545359362
↳ pair=620625501144562390396542055628483650475430674268393620753336837076006167968)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_swap_gas[500000000000000000-100000000000000000-100000000000000000-1662497915624478906]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00691c0319B400086E50a60095469BdACfa859b42f61ad0e4418e84C2C87E898
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00DC57718D0d76C79DE1D644C53c29Fa89BAFD72117cbe576AaCad08f9Ed6501
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0470D2Dc540f54af7769C6A70370F38a4DF9707A9907A672ec60d98318cDE24
PASSED
```

```
tests/cairo/test_SithSwapV1Pair.py::test_get_amount_out_end_of_program_reached
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07e21f5bc892e5b799cb0a5259d0f3457EB055a66EC9685e5f2e6f0331FB7B
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x069aAa3fc9632893761Ac314176ECF268c2d78FDeFaE7FCCA66be4D9b56f357a
LOG: Pair created: Arguments(pid=31 token0=2987146556039626009655278459986274336671046207458139829285831648550054737274
↳ token1=3565713805337565186631136876301751651178936341741522459048698537799167638395 stable=1 fee=1000
↳ fees=2680953065912004406865249272887008939549147080936649261861366076931054636753
↳ pair=2776229452233634045925264930440005457106469710475034812194337418291196269524)
XPASS

tests/cairo/test_SithSwapV1Pair.py::test_trade_fee_revert
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0708Ed3041dBb9A05a54cCfb20815aCc4ADD5d27EE39FaD56C668e4196Eb15Cb
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x061d44006111eE8A5377E1d4477F232008A5C33E3f14E2927FFe6dCE4dF4a6D
LOG: Pair created: Arguments(pid=32 token0=2765584985352422239895278017081955441302273358842078737421847894349227969133
↳ token1=3181961731498409803157202296656308221453814194496013525592548762756322104779 stable=0 fee=307
↳ fees=1578084195430024000897065345231479335215746012485646065885361378560465759880
↳ pair=2761469113037428470453826616130688007548595398266260863120205516615980982783)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_trade_fee[1000000000000000000-100000000000000000-100000000000000000
-996006981039903216-500]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0657BE0334614a1A91c9541D2602188C4D4BCa4fE1AC3e64C87A1AA0d1Cc5FB2
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02b090c5FF47C25f32B32E25624f174236e925FA1b6191c5872D4C7f9945dF8b
LOG: Pair created: Arguments(pid=33 token0=1216589970035114113537682447658978329565323286605916621350870177201187577739
↳ token1=2868904204337309707959830172241454969961970869128243632474023678928680148914 stable=0 fee=975
↳ fees=256239059345683271658796600067974613140119873351852464939952417301214122093
↳ pair=2748556619774448995852572239183267449597766521727736329014138695276812346145)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_claim_fees[5000000000000000-1000000000000000-1000000000000000-0
-1662497915624478906]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04B8Bed97d69EB2A8D890BCB810Da56A602345855D3315b1c6Fb31c8845b56fd
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03bA9395d94F283C877C2C88c448CB95481b63Ed9F18A72d0FC054EB50388417
LOG: Pair created: Arguments(pid=34 token0=1686590696428940933298509816749668834436255341985019452656585567974677054487
↳ token1=2135668449574214099693511518327534597562002031362589830133728636449479939837 stable=0 fee=307
↳ fees=2342579489251035196796703653401397582905694408652784336139415792584570055293
↳ pair=1802376386152733973480121158080292515495088266663388535652893916097945757585)
PASSED

tests/cairo/test_SithSwapV1Pair.py::test_oracle_functions
SUCCESS: Contract 'cairo.sithswap.mocks.math.SithSwapV1Library02Mock' deployed to:
↳ 0x0011CC2E93c4A6E9d715E21f3063E827d7CA19e541e0cfB6e49c3387B455ab2d
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0770C93a5f5760a457EBb70A798DccF48Ae2f29556048394599EfA799Fa20eD4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03B324f68D72Af1e0F1e808317fFDBade4fbed122B8426aD1f74D54105ff1CED
LOG: Pair created: Arguments(pid=35 token0=1673459280256705947460855395033114529283264429958607466143521951694941265133
↳ token1=336546563607126809187239415711034731784311000775045283061694522398096051924 stable=0 fee=307
↳ fees=727017791626065954706556966816721256855895282058458820699511876695328135248
↳ pair=2149456793663304744552882542254844033724129850770072561268905532785734016751)
LOG: timeElapsed 30
PASSED
INFO: Stopping 'starknet-devnet' process.

===== 21 passed, 1 xpassed in 7826.23s (2:10:26) =====
```


7.4 Ape Cairo (ext. core - VLP)

```

===== test session starts =====
platform linux -- Python 3.9.13, pytest-6.2.5, py-1.11.0, pluggy-0.13.1 --
  /home/runner/.cache/pypoetry/virtualenvs/sithswap-C2YYCxA-py3.9/bin/python
cachedir: .pytest_cache
SithSwap: welcome to the dark side of the Force
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07567ABA96969F3b86EADe3EE682a793e882B9E93494A022622d73962282d980
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_get_input_price[500000000000000000-100000000000000000-20000000000000000000-2851015155847869602]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0779660e57074D41CF70FCD8012e50a5D34057A9600ba5dc1826bBECd413EA74
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0263458f302F3A2aB1Af328054C322cc2641c9b78a12c608A1d0feb7FF0A72d6
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x02D61BA06F616A5cB049dA9CDd49dC7280D9b1E5F17A610EaC9eD36bd8e4dc6
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_get_input_price[1000000000000000000-500000000000000000-20000000000000000000-831248957812239453]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00B4AbBb14fd3AC2E399eCaC8f230893602e3742fED3e05E3B03d5AF1c81Db94
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04F4147e5BeA7e4Dbe175f101138aDea75dAaBB1253838e67F34f3D4ADF53295
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x007edc01221f40EE80F5B4Ca397306b31C937f557183A2A032fcc970B9f8a023
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_get_input_price[1000000000000000000-100000000000000000-1000000000000000000-906610893880149131]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0674fafAa510aaf01858E5a0398F2e08E0b22EDBebbb232827De8d07b5AaCd30
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0759D1EeE7aa44D2457c7c4943e55dE925906E376962d5314f97C3caeAa86cB7
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x03E343aa1d91162c36B8b888d70BA6eF850aE7C3F3835dC01124BDCAea32bBEC
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_get_input_price[1000000000000000000-1000000000000000000-1000000000000000000-987158034397061298]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0290F409E36fC1B3942F575A735E1BAC10F47CC30D4e9D77Fa3Ae76DA134A48e
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07832f372A75335718585525B2CD2Fb1dd3adb522B20f184f3eA5216ca4DeB2A
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x071F20db6cd944E4276810E471f6620721EeE6316c06fDc75aB8179669D53A0B
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_get_input_price[1000000000000000000-1000000000000000000-1000000000000000000-996006981039903216]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05fCEe1d90a6C7E12E9ec4F183CDF7D48a9D2CedB027291947D5Ff4FF26dCcF1
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01Ac6f923AF306ae11cdB7Dcc1041117799563d4fb4E8F166E260DA1C877521b
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x000515F9a7064dDA0432032b156DD5897061996bc288b15B25975f15e12D158
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_token0[500000000000000000-100000000000000000-100000000000000000-0-1662497915624478906]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00e96adcF8D1D7c3254e085c007E9C63f80CB4F9E5BDF1E23D0daFf85A7e7294
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0406abF5D307A7414b53Cbc1BcAeC89dB28d1BD28190337b96833660b5b9699c
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07C490a0239A183813911e009B95f3fdE7d78C2a9511356f162B92bBC6C0AEF9
PASSED
    
```

```
tests/cairo/test_SithSwapV1Pair_VLP.py::test_swap_token1[500000000000000000-100000000000000000-0-100000000000000000-453305446940074565]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x068C0557d21D9F4b205e8b60cfa6fe11Ff0402dF09589D888E76c5b60d1a69b
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x015dAAF1CD9C984143A706d95cd60323fD9731b3d0cf43191120FF427FBCa5E0
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0541ADcCC5Bb7306D8AF589Af577983261Be0De9D92B8f77f16FA5CaDd05a560
PASSED

tests/cairo/test_SithSwapV1Pair_VLP.py::test_burn[300000000000000000-300000000000000000-300000000000000000]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x013435a59098Aea273105f806F4659beF976E827111fE0161231bAE6f94b41c5
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04Dd1c53F5E1b2Dbe291C38ED45A0cf226E59CCc8B59386E03C23Ca3B1C7c9b1
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x02595f1E2DA45fCa8Ff363d044D10E97725F23a71F77a085760f82E8Ac05770f
PASSED
INFO: Stopping 'starknet-devnet' process.

===== 24 passed in 4649.78s (1:17:29) =====
```

7.5 Ape Cairo (ext. core - SLP)

```
===== test session starts =====
platform linux -- Python 3.9.13, pytest-6.2.5, py-1.11.0, pluggy-0.13.1 --
↳ /home/runner/.cache/pypoetry/virtualenvs/sithswap-C2YYCzxA-py3.9/bin/python
cachedir: .pytest_cache
SithSwap: welcome to the dark side of the Force
rootdir: /home/runner/work/core-amm/core-amm, configfile: setup.cfg
plugins: eth-ape-0.3.5, ordering-0.6, typeguard-2.13.3, asyncio-0.19.0, web3-5.30.0
asyncio: mode=auto
collecting ... collected 32 items
INFO: Starting 'starknet-devnet' process.

tests/cairo/test_SithSwapV1Pair_SLP.py::test_init_raw_pair
WARNING: The connected provider does not support snapshotting. Tests will not be completely isolated.
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07C7935cd208b309e2626baE0D54DFe94d5cB950eA6073D12806466D035cC772
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x041E204b3b0B1D616c4832ebe8dc8057A2386Bf6e21999186891941a8B4f69DA
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x031a6B892c853b92A2d5E5AF86e78CB292e0C78F84F9eAcDf4424491E8f6E137
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x016FA8eE6726A1B0dd1be51Fd601D6648ecC3F08E452781BFa664243e0E9f98f
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_mint
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07C2eC43e540F74B1F90f7b77B2c00C1ac8FA0bb6bEcDeECcf80B524FD6016Ec
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0354d5D9B29a6f45ABe181C498a940Bf534947DdB613Ae137E8f385aEbc73Af2
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x03457c468794Efc0375457Ac106CeBcb18370D059f44678ea6694e6D84A2094
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[10000000000000000-50000000000000000-100000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x00377180423849Ce7F68C97a26F6bA866d72F008311D3d337c6a6Ae80368b5b4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0357c473aDcE650BC7B3B55E59AAfE3BB96172012B9Df9263C808cc13ea9F1e
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06A574e4F177cf14F0ed8DF7e76B40B06F4C0C3f3322139A92ae1f5796A8B961
PASSED
```

```
tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[10000000000000000-10000000000000000-50000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0430a477055c6559423fE48dbFBE8c02bEfb392816d7993E2dac2B9c151510A4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x036FFc689611edFe09956464516272e142d5e70c8959167cd519F5dC5ca9495F
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04bFA4692EcF0D66F2f84c6d01a9e45eb9C0C7FF7A2886CE7CeFaeCF28f68F3C
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[20000000000000000-10000000000000000-20000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0784B5BD8bE9d0AeEE97dC9619F0F78EcF6E7B5B9A69aFD0dB8A0eB43fAf585
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04585b015703c5f3112FE4628498e27f28BE12F5143A03207AefC5B863Ba731F
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05dA0035F09f037c84885887Ec3018bEbdd562864bF5C1b06dB2389C39E849F5
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[20000000000000000-10000000000000000-50000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x062487461C72ca2C2F0043cbe004870374DCba4E031FD8a50849e315B11ef7ac
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0692661C670B9bBbc000695b1f69B70081338b7B2ef70b6AD359b30e8f9495cD
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02080CE144530E13a0a9a53523b6D221Eb0E304aA4bfC5F7B9f36C00c1344b2D
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[10000000000000000-10000000000000000-100000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x02CC2a19c9A8226bCCfC060546BDDb66c9cFfED913B72C12bAe4110e70bb008
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05FE61f07cE3c9fB420728dB9c4B07D4409600c1CfBe8B3618E01a6f151Dcfb
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05404992CC635901432CAc5186ca847a5ae978ff41420dCCdB51DA1F15FBbdf
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[10000000000000000-10000000000000000-1000000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0252fA9FB1e126e952D493796d2dfB11CE602b76A6F139B783aea2254b21aDA3
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x061860b82b5a23481159e93Dd7150Fe1F95279Eef33F0648e6FDfC52007efC95
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x067e146BdE57f2E4bcA5C55c7528797A02c83F8146c7B50F550448F2fc080C3d
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_get_input_price[10000000000000000-10000000000000000-1000000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x076BD390E0B39096AacB185fd72ff6347A50E0Bd5cafca4f1e91244C3B625217
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03d9dC98866684376eec1595114FC07A40cF6D0936e772a6F45374238cdc7Dab
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03B427996Cc15bbc87dBdd9c9Ac1640A5E9d702Cb82FBc4d642992e1f15711A1
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_token0
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05B23F03d8846Fecd154eFe98fe8D5C96740d45E07D35E52373Bea5e1fa099b5
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x059E0778B7829608E09222ed55c9964f7fd69018E00b0b6986dCe7A20c32fd9B
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07C2ce6EAC8F862C207B1AbD9bC63a15F4451eb97d81B47F5bd4d570b5458768
PASSED
```

```
tests/cairo/test_SithSwapV1Pair_SLP.py::test_swap_token1
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x064ca69D5B0F9203042f7a64c5743778839EA5E3d6d8519d4836dd775e1CcDB2
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x039Dc19c33D5900166C22A475E1e5edE6e97d0Caf0080aD4A01292e6D9d9BEfC
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x07c484C53Cc4316E06F4217838a67c3c3D90786802dfF71B398E9561C3a8d738
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_burn
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05F91c160A52868593108b4a0174430C8E389Eb724FE3BECE6D2f24Bd163718f
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07c0c94B51f89f45539dAb08D49B2573d265e73765056648bB853Dc5c089b624
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x02F7730fDe392ae7bB1EE7c77DB6FEc33E0942493C6B292d1B14345d8EBc2D7b
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[200000000000000000-300000000000000000-800000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x011b94A26912A630df3888f0A268C1570a09Ff79EB11d5e69d66335Dd4Dc83f1
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x016b8F73df2887aA87a82a65533cf03ba60c8591905663f9F34B2b50Dcf03144
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0355ad812751D637E3d496eE6A40945DfDA3A56C82EAcBbd1253ff5C44307402
2099681471282907328
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[1000000000000000000-900000000000000000-300000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x05EF07BC44E6bDf2d693560d4D8eAA2021BBd2cB1a9Db096eabE9c40d15662
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01E32a6e9C79F11F837d978F92447889A9185Db1114d11758e573650C0B5E53a
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x052D0c79494DC98848Ffe30724ad1997193f43e1E4852A5Fc75E293281c0584f
686883535830154678
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[1000000000000000000987546-89999999999999999993454-300000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x05cc25590A0c7e48bFE866A4EaabaE06024837d7b24fb3E05cF78e7359Bb26A5
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x076B759080C8B62C7293838b9242A0483B03A8973E9d48cB3d5c50335F2030d6
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x044846848e6b2513403d2599C992564F7be089027E0f87d6A99dc5886f7EF9fd
686883535844457023
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[2000000000000000000-400000000000000000-1000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x059e2E331B5EC81131EAB473b277AfdB0BA7C3886bFc4936A15DcDd722c09004
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x078020caf5B1D5b9bD9710860a94956e09d24A22798440C4C9C2a6d2f307a0d
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x007f7aa2682BA0dC462C1244Cdcbf5fF0670aaC5cceD6d8EddA4b1649279E7d5
2098827671173281886
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[2000000000000000000-4992144444477457756-1000000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x02F2E6B09A83A851351f03dc6b3e4996Db873C821aC75E505CB83c3ab4592f2e
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03eEe8d2c8Ac996fEa5C39Ea4BD72654091Ab551F0C80ca29900bC2F692A439
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x050aE203bb98b879f901d92c44249D8Cbf96202F07C2c8058342e55D856AB60F
2027305731949847588
PASSED
```

```
tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[200000000000000000-49999999999998889-100000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x0313B60539eBEF857C6783198fF319301515aD6Eeb3705860fAee770f2f47062
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06d60ad211Dab5C2D2D28D7cdF89C3Bb6a3B86A8Ef87813B271b8E6Ae1dB9094
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05e5703207B1Ba9Ac9c1Ed07d71A8F32f923797FCA7326b59270c15775aB96dA
2026939621136211061
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[19999999999988843544-500000000000000000-100000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x04185743266556319956300Bec4EA52959a28fe91A760AFcF990837eCA29c3e6
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x03A5897cDF72B4B1368Bdfc253EF18A12EB16aec876aB40e98f1FA20b8bfcf32
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06F8b3CefDD1218EE5534372Ce03452F22eEf08e8B18271f20DE2996461369Ec
2026939621125156401
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[200000000000000000-500000000000000000-100000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x043D6685A412e29b408Fe50EBb7F3b3B541d50F9aEF827382A03eAb97c43A70a
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00bE9B6D4346BcA89b59Ca08404fe05f3533270AA305f4f99d4e0551C0Da29C3
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0571a5073eE729b7C829620917545b2f17799491381d83637016D3a111ee0B7A
2026939621136210545
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[200000000001156456-500000000000000000-100000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x002BF38f9fa1b3C2c79fdC86f2301218CF75052e62e152254b9e08de66B8DB62
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x074eCaDe35f6C73620BDC1813Ac4eC3f38Ccb503149e6fc6f367783bC8cEA992
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x072932F415586e1B52E5054a80F1f714d799E7d9B621a0F562eb6b0bfA4Ca532
2026939621147264689
PASSED

tests/cairo/test_SithSwapV1Pair_SLP.py::test_relative_low_liquidity_stable_swap[200000000000007575-500000000000000000-100000000000000000]
SUCCESS: Contract 'cairo.sithswap.amm.pair.SithSwapV1Pair' deployed to:
↳ 0x060f73A3D4F3452c48B94EEe360465d315E2f6535D5BdcF4c44ACb231E3222c
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01791d8c14E233175C6d0F384Da9A0DB11955050e61154Fcf0e04A2e9E951784
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0776122BA97a9fBf50599166AEe2245eb8c0D7FECab143A83c4F05804Ca82141
2026939621136218051
PASSED
```



```

tests/cairo/test_SithSwapV1Router.py::test_pair_for
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x003abbb887cfA0692AB9FF5c241b51FFC3c7bcA183D38Bcf0326bff861c3E960
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x040A6562F7bC1e310Adc90C30ab8217253540012EC825Ad82db1E121D58d2353
LOG: Pair created: Arguments(pid=1 token0=103772731256754888588812068710439077999727187426490923627715595052897266016
↳ token1=1827619609526171896807720267576228522627530347755387783085002458525095240531 stable=0 fee=307
↳ fees=70441792731347769216727529428679773907357016484220550527059860907331823628
↳ pair=1452721059341890234056015374264718567860172073935705366591480868090735968981)
PASSED

tests/cairo/test_SithSwapV1Router.py::test_get_amount_out
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05A29D7b270c796b39efe7638c5665b7940182C4e851740A0b18de06064dC532
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x041d935b1bb342a08b4B3c99EC4C42FA33694680B9d183A8eba3C502013e4f0d
LOG: Pair created: Arguments(pid=2 token0=1861506972196938892290029587907218542705991059321716085550126699566010879757
↳ token1=2548880361772627382621986078590019573777897038655667308693437638383307179314 stable=1 fee=975
↳ fees=3351590816159585251467376351451924237285535798445802325569780034860018763927
↳ pair=2852262024936104494548898000372543957128969741446679310580008785883225541411)
LOG: Pair created: Arguments(pid=3 token0=1861506972196938892290029587907218542705991059321716085550126699566010879757
↳ token1=2548880361772627382621986078590019573777897038655667308693437638383307179314 stable=0 fee=975
↳ fees=1290178015301256008224782134955882440435842123274539522953532840783898086058
↳ pair=19628643361458490857629267196559036698909044051543264760749495452517709718)
PASSED

tests/cairo/test_SithSwapV1Router.py::test_get_amounts_out
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x010C9a39Bc6CB476A751094D5dde3E7F0070aC7035373d0664F018311FAe528
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x037026A6349Db409220Ffe87f11862c02c3c729AdEFD679f64CB37B90fE36916
LOG: Pair created: Arguments(pid=4 token0=474579438858402225123041859087033270872840501144058607375806327220642440488
↳ token1=1555092164258417525280353038439286423924280183916600092826700122205492308246 stable=0 fee=307
↳ fees=9929406112196242051678762425247715910267633561144329171207686925673324286
↳ pair=3052050796144547367228415020133811889562257730258907951324225244006066072967)
PASSED

tests/cairo/test_SithSwapV1Router.py::test_get_amounts_out_multiple
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0019A16B568D7053996505C977bf37f38Ca9cAD1e2d0CdCCfe750c0067F4eBd6
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04F8a26233Fb9335B34Fad1C0aa831282BCA978CF64bd551D8Bd63c3ad07223
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x05d93e0aCeAF2248B78Bfe19b582720ff4bDa7062C5867ff49bFa687042ce66d
LOG: Pair created: Arguments(pid=5 token0=45285251610627895090934202904261971558795566304350427420377179399386360790
↳ token1=2248550196855477162370137670306120325922607046919973619851693737781599695395 stable=0 fee=1000
↳ fees=1270853212766330537441831525812943147611671633331125125881130855613454839532
↳ pair=3547811482821691619964861065208182684301707698861932139259189416092940576465)
LOG: Pair created: Arguments(pid=6 token0=45285251610627895090934202904261971558795566304350427420377179399386360790
↳ token1=2645398255612587028298383806694376178688299800411602302422813640431569266285 stable=1 fee=1000
↳ fees=2537468903414596048406903645256779415504210098472116878910087251540439915806
↳ pair=2587322476177420871642234588404282538376390212525757445933340165469188040792)
LOG: Pair created: Arguments(pid=7 token0=2248550196855477162370137670306120325922607046919973619851693737781599695395
↳ token1=2645398255612587028298383806694376178688299800411602302422813640431569266285 stable=1 fee=2999
↳ fees=1069060278726375490327944116422278114097257500226128171122099484335054981508
↳ pair=237443285939377605867371555696337478546292875455335334764857836242757448031)
PASSED

tests/cairo/test_SithSwapV1Router.py::test_get_trade_diff
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x017aef9202B6f0e6d7679d704a897Fb9937d101e3ccEf4B5CeEB104A3B862c4
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x029b15eD9977f5D79df793fC435B95A43ec2b686F97F6955D33255A18b39F85E
LOG: Pair created: Arguments(pid=8 token0=669521644301127681746220357794318289913024189067480882032904594496471720644
↳ token1=1178638334549954503513840970720454065885736409698893872046686534578160138334 stable=0 fee=307
↳ fees=2126718480331861674215242549837560200703439339432891479869681684714284815293
↳ pair=1164006241074636013245618806383229209496200965012441003737833928107246660678)
PASSED

```




```
tests/cairo/test_SithSwapV1Router01.py::test_addliquidity_revert[10000000000000000-10000000000000000-0-100000000000000000-SithSwapV1Router::add_liquidity: insufficient desired B amount]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x017B02dFf8489827D063949cDcAA7E2F96AA7b361db88069c519Aeb73D7A927f
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0401c8864b11Cf57F8EBDF1Fd3484a1df31aB262907C0769F0d5FA88bEe8dED5
LOG: Pair created: Arguments(pid=3 token0=669654879259119936965660968271404069002138662977880442861024283584196416127
↳ token1=1812402211205803906663050407595789478827574144942854980113883188276343922389 stable=0 fee=307
↳ fees=3291126793320544296921523612230542031741017088690331865308301164891391169336
↳ pair=321714203955524703225954985162422161253990595406899163521391614431853345411)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_addliquidity_revert[10000000000000000-10000000000000000-0-1427247692705959881058285969449495136382746624-SithSwapV1Router::add_liquidity: insufficient desired B amount]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0069BB3529f6CdbA1A342DfCe242e74C2A3629fABaFbB509ec96c39E75550617
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x00AbeF7b23301F56165726cCc4B569c7A27603cE777F47AA34006123aC9fe31f
LOG: Pair created: Arguments(pid=4 token0=186811001665086628187016317009352250906247077828976422568567721999841166871
↳ token1=303783685233153343177898693852578028547928137597394504077106652614850765599 stable=0 fee=307
↳ fees=999435209929867370114498254000669157874306992719454227685284592073115757120
↳ pair=219484086210741855068723503361104184491273684599992319997997769001744137216)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_addliquidity_revert[10000000000000000-30000000000000000-10000000000000000000-SithSwapV1Router::add_liquidity: insufficient optimal B amount]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01f3F887962Ad40D85F267eE9EC855d11f8aC02ADbEeD6de4301293165fF9110
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x06969FeeE57550b21EB2CA0dCF1Bd1Cc089889EB3a0F21Ea1c40314e50Bf2064
LOG: Pair created: Arguments(pid=5 token0=883371973825680209505246078104452996263911494697026514949715630239921443088
↳ token1=2980007969517577934693525961654065975384784847196511654858088674035719151716 stable=0 fee=307
↳ fees=283947686747265908209912461915303338765411379938615514503543210898150128505
↳ pair=2388219848638430009906308222437529948160719381588091265467332092285269294743)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_addliquidity_revert[20000000000000000-30000000000000000-2000000000000000000-100000000000000000-SithSwapV1Router::add_liquidity: insufficient optimal A amount]
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x073768EC3149e4a4B1d3123382994DBa8222553d0FAa7Db4770393550D5A6
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x004daA48461bB15e68dac10eCA11cfe7De50C12F5dcbf3E7937EA7A4749A489A
LOG: Pair created: Arguments(pid=6 token0=137222469366302617281186272577119116558942544593591689713470312366378469530
↳ token1=3264090678003855688531484626289756887713235596628849172834148658272361567654 stable=0 fee=307
↳ fees=1929229217073338726917345216189487918748412540708885260903436017289156334754
↳ pair=962353840184017316411308035284820083983587868969483347966545216851295998386)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_add_liquidity
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x051cAFc0e878d3B42a1BE58b9E3eFA2eE6114E626f8226D4b3EfbB99dA5a7284
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04f4d4c53e68261d37c8730F2E8081960d73605a56422D4604a726FeA1DeBc89
LOG: Pair created: Arguments(pid=7 token0=2241830566046210807100921367816967958482580293670419590282172090991039659145
↳ token1=2312248967132732143343658273858068906593689171114936516291606037783151014532 stable=0 fee=307
↳ fees=2739905963042350901991337635489499965593316189628346723905943189611129693316
↳ pair=867696202419169232983170291777636674014380139316135625542125966358100090039)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_remove_liquidity
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x003A8F9BC419E820f35b20B1148932590387288F19673e433a1D0B9c333234B
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x04f6d9987A45322b298C407119D10799F773f8bD6bD1f79982851302DBdcB945
LOG: Pair created: Arguments(pid=8 token0=103469949618869108778651021168041957347268957673458676648279095500363473739
↳ token1=2245397562014260212824015631196633349152784943898138338021355651079866202437 stable=0 fee=307
↳ fees=3124778401223670410057229341984995073190617747926316292254141644634893150324
↳ pair=3365045638909929280028299276593462360032368515124216985908976600024684829717)
PASSED
```

```

tests/cairo/test_SithSwapV1Router01.py::test_swap_exact_tokens_for_tokens_simple
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x055639b214c2959c5b5bb68ff12E7aA10238812bECC67FA32b8438F81984284D
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02827aD954d0044335413E45873C882429840c54a02A2bdB48291AeDdB45084A
LOG: Pair created: Arguments(pid=9 token0=1135163687882263546826684462479017210941603368534073563689459561049234933834
↳ token1=2413911291085840028807502987648835634065141940297877379789386473827018745933 stable=0 fee=307
↳ fees=160353205028918756087329320143135390992002001471263205913148050791394317095
↳ pair=2573643575176110380768453453773077869521501889848078686606389971322854537654)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_swap_exact_tokens_for_tokens
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x07595801178fB558A0c81E55eaAaCF4965149D054c5cf8529aEAE2Aa875D462
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0127b196e49a86d0044C50a33eb22bd8317CD324F914aA5626D8E022e016E99F
LOG: Pair created: Arguments(pid=10 token0=522445561279776440941803818004605235461242905510508616359590843814044428703
↳ token1=3324046711967906069124484782184686278082667749273761694415770840812485989474 stable=0 fee=307
↳ fees=2053813187816970834155576243284601610733255343486623729217023985386522261942
↳ pair=1253480110511062180723107977973410458105575226336896665417019758876127166125)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_swap_exact_tokens_for_tokens_stable
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x01148fb950ce4Ad6DCA445aC98cb8A20Ce0F7D2884C4780D7A2Ee50Be12fef
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x02323B0386cc6e5e7c10F99a7A5cf6063c8DbC266D9a5b1379ddfBeed3E6A20
LOG: Pair created: Arguments(pid=11 token0=488643522249874023188938890496235259221219238675476969833471912886552047599
↳ token1=993375348515697810225764407312641893986531268441906939887593944627508308512 stable=1 fee=975
↳ fees=3267886983997371700947113308395846098779906659008666964758188026027889939631
↳ pair=1970996578611820395837661227946623046228341861752988917980132289919426445852)
PASSED

tests/cairo/test_SithSwapV1Router01.py::test_swap_exact_tokens_for_tokens_multiple
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x024c83361d7916C2F4434ce8f2Fd21E2940A76463604A241D6873aD12F1F4870
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x002b56eC75Cc8A7da798e38266E5Eb42B078FD9B571D77d43d4889E084381f37
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20Mock' deployed to:
↳ 0x0695321f53227dB99D38c2b61A5610de83cad5CEf823e94b5A00a37C36B51687
LOG: Pair created: Arguments(pid=12 token0=76574348924389366050661652948781618035185263330436900795473459645511114551
↳ token1=1039811661802109123416825747339812394931514117221465048107952839076607903856 stable=0 fee=1000
↳ fees=347272521093952467363577072106235044737545452175758563341224231216259560256
↳ pair=597821399536149121969373424886767853458232567377815585686991938594880611193)
LOG: Pair created: Arguments(pid=13 token0=1039811661802109123416825747339812394931514117221465048107952839076607903856
↳ token1=2977483235982372834808957212037407751759671706407336131432316899240608863879 stable=1 fee=1000
↳ fees=1276195985203000657380325727926099266695470972975701746803840225767715687444
↳ pair=228282011126323288242085187950014415850297921316827274796429119180639093532)
LOG: Pair created: Arguments(pid=14 token0=76574348924389366050661652948781618035185263330436900795473459645511114551
↳ token1=2977483235982372834808957212037407751759671706407336131432316899240608863879 stable=1 fee=2999
↳ fees=3048441548847729364721982460955741393612865657615085521436681072165876932363
↳ pair=2185334711721194586722841990328935438068602977438134043829512452697287047652)
PASSED
    
```



```

tests/cairo/test_SithSwapV1Router01.py::test_swap_exact_tokens_for_tokens_supporting_fee_on_transfer_tokens
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20FeesMock' deployed to:
↳ 0x07cA348183DE352b8af26c51328b40B92A81E72bE2d5C7A7d0087c2B03236d1B
SUCCESS: Contract 'cairo.sithswap.mocks.tokens.ERC20FeesMock' deployed to:
↳ 0x03366b7DbECf98dAF15E63a770FeA0Dc3ca6C9e14aDf69579cA0dD1bbF2FBaCB
LOG: Pair created: Arguments(pid=15 token0=1453090164195007809849187465863872200780467406301926549038009689385338911435
↳ token1=3523455429698572677489583752264838833702232534976894701872685672252932582683 stable=0 fee=307
↳ fees=1734605426014087419415650938656495137815919855751088054431494206744413426682
↳ pair=725409669255976099621107001987994662777891467175603220850234314658684567524)
transfer_logs
[Arguments(from_=2957188269200184411255999937111091253445605066208535325081986593780030033891
↳ to=1453090164195007809849187465863872200780467406301926549038009689385338911435 value=(1000000000000000, 0)),
↳ Arguments(from_=2957188269200184411255999937111091253445605066208535325081986593780030033891
↳ to=725409669255976099621107001987994662777891467175603220850234314658684567524 value=(9000000000000000, 0)),
↳ Arguments(from_=725409669255976099621107001987994662777891467175603220850234314658684567524
↳ to=3523455429698572677489583752264838833702232534976894701872685672252932582683 value=(163179541926701361, 0)),
↳ Arguments(from_=725409669255976099621107001987994662777891467175603220850234314658684567524
↳ to=2957188269200184411255999937111091253445605066208535325081986593780030033891 value=(1468615877340312250, 0)),
↳ Arguments(from_=725409669255976099621107001987994662777891467175603220850234314658684567524
↳ to=1453090164195007809849187465863872200780467406301926549038009689385338911435 value=(276300000000000, 0)),
↳ Arguments(from_=725409669255976099621107001987994662777891467175603220850234314658684567524
↳ to=1734605426014087419415650938656495137815919855751088054431494206744413426682 value=(248670000000000, 0))]
PASSED
INFO: Stopping 'starknet-devnet' process.

===== 14 passed in 2172.91s (0:36:12) =====

```

7.8 Ape Cairo (Prostar Cairo)

```

08:22:46 [INFO] Collected 7 suites, and 36 test cases (71.356 s)
Collecting tests

[PASS] tests/proto/test_math_libs.cairo test_sith_math_directional (steps=6997, memory_holes=88)
      range_check_builtin=273 bitwise_builtin=26

[captured stdout]:
[setup]:
owner_address: 3171724132921051860405373901922296539481540746429872579351200954976901555062
sithmathcaller_address: 797148299375822784048620297590535626380362556723830344201351971134496730325

[test]:
TESTING: SITH_MUL

> Setup: n= 12 step= 5 base= 2** 39 ( 549755813888 )

> X if fixed: 1180591620717411303424 - 0

> Y takes the following Uint256 values:

549755813888 - 0
17592186044416 - 0
562949953421312 - 0
18014398509481984 - 0
576460752303423488 - 0
18446744073709551616 - 0
590295810358705651712 - 0
18889465931478580854784 - 0
604462909807314587353088 - 0
19342813113834066795298816 - 0
618970019642690137449562112 - 0
19807040628566084398385987584 - 0
633825300114114700748351602688 - 0

```

```
> Directional testing:

-----> Testing # 0
  x: 1180591620717411303424 - 0
  y: 549755813888 - 0
  res: 649037107316853453566312041152512 - 0
-----> Testing # 1
  x: 1180591620717411303424 - 0
  y: 17592186044416 - 0
  res: 20769187434139310514121985316880384 - 0
-----> Testing # 2
  x: 1180591620717411303424 - 0
  y: 562949953421312 - 0
  res: 664613997892457936451903530140172288 - 0
-----> Testing # 3
  x: 1180591620717411303424 - 0
  y: 18014398509481984 - 0
  res: 21267647932558653966460912964485513216 - 0
-----> Testing # 4
  x: 1180591620717411303424 - 0
  y: 576460752303423488 - 0
  res: 0 - 2
-----> Testing # 5
  x: 1180591620717411303424 - 0
  y: 18446744073709551616 - 0
  res: 0 - 64
-----> Testing # 6
  x: 1180591620717411303424 - 0
  y: 590295810358705651712 - 0
  res: 0 - 2048
-----> Testing # 7
  x: 1180591620717411303424 - 0
  y: 18889465931478580854784 - 0
  res: 0 - 65536
-----> Testing # 8
  x: 1180591620717411303424 - 0
  y: 604462909807314587353088 - 0
  res: 0 - 2097152
-----> Testing # 9
  x: 1180591620717411303424 - 0
  y: 19342813113834066795298816 - 0
  res: 0 - 67108864
-----> Testing # 10
  x: 1180591620717411303424 - 0
  y: 618970019642690137449562112 - 0
  res: 0 - 2147483648
-----> Testing # 11
  x: 1180591620717411303424 - 0
  y: 19807040628566084398385987584 - 0
  res: 0 - 68719476736
-----> Testing # 12
  x: 1180591620717411303424 - 0
  y: 633825300114114700748351602688 - 0
  res: 0 - 2199023255552
```

```
[PASS] tests/proto/test_arb_swap.cairo test_flash_loan (steps=20547, memory_holes=674)
      pedersen_builtin=69 range_check_builtin=918 bitwise_builtin=4
```

```
[captured stdout]:
```

```
[test]:
```

```
pid: 1
```

```
stable: 0
```

```
token0: 1609548864969440717869750621959983950421014985795233706561846804322204663998
```

```
token1: 203070218281227428892405745003485829426818515794062964961503841408105890559
```

```
decimals0: 100000000000000000
```

```
decimals1: 100000000000000000
```

```
pair: 27415733988529077058079482690322476634677122642994918945736636307213272677
```

```
is_pair: 1
```

```
starting_callee_balance token0: 0
```

```
starting_callee_balance token1: 0
```


8 About Nethermind

Founded in 2017 by a small team of world-class technologists, Nethermind builds Ethereum solutions for developers and enterprises. Boosted by a grant from the Ethereum Foundation in August 2018, our team has worked tirelessly to deliver the fastest Ethereum client in the market. Our flagship Ethereum client is all about performance and flexibility. Built on .NET core, a widespread, enterprise-friendly platform, Nethermind makes integration with existing infrastructures simple, without losing sight of stability, reliability, data integrity, and security

Nethermind is made up of several engineering teams across various disciplines, all collaborating to realize the Ethereum roadmap, by conducting research and building high-quality tools. Teams focus on specific areas of the Ethereum problem space. Each consists of specialists and experienced developers working alongside interns, learning the ropes in the Nethermind Internship Program.

Our mission is to gather passionate talent from around the world, and to tackle some of the blockchain's most complex problems. Nethermind provides software solutions and services for developers and enterprises building the Ethereum ecosystem. We offer security reviews to projects built on EVM compatible chains and StarkNet. We have expertise in multiple areas of the Ethereum ecosystem, including protocol design, smart contracts (written in Solidity and Cairo), MEV, etc. We develop some of the most used tools on Starknet and one of the most used Ethereum clients. Learn more about us at <https://nethermind.io>.

Disclaimer

This report is based on the scope of materials and documentation provided by you to Nethermind in order that Nethermind could conduct the security review outlined in **1. Executive Summary** and **2. Audited Files**. The results set out in this report may not be complete nor inclusive of all vulnerabilities. Nethermind has provided the review and this report on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. This report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on this report in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, Nethermind disclaims any liability in connection with this report, its content, and any related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. Nethermind does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and Nethermind will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.