Quantstamp

Arkis

Executive Summary

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

Type	Leveraged Trading Protocol
Timeline	2023-11-13 through 2023-12-15
Language	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Arkis Smart Contracts
Source Code	- https://gitlab.com/primebridge/smart-contracts

Documentation quality	High
Test quality	High
Total Findings	17 Fixed: 13 Acknowledged: 4
High severity findings ⓘ	0

	#76e0adb
Auditors	• Ibrahim Abouzied Auditing Engineer • Julio Aguilar Auditing Engineer • Hytham Farah Auditing Engineer

Medium severity findings	5 Fixed: 3 Acknowledged: 2
Low severity findings	5 Fixed: 5
Undetermined seve	2

rity findings	Acknowledged: 2
Informational findings ⓘ	5 Fixed: 5

Summary of Findings

Arkis is a leveraged trading protocol designed to allow trading across several DeFi platforms. Lenders provide liquidity to the Arkis liquidity pools, which are used to fund leveraged positions. To incentivize repayment, borrowers never receive borrowed funds directly. Instead, loans are provided to *Margin Accounts*.

Margin Accounts are individualized smart contracts that hold the borrowers collateral in escrow, whilst providing them an interface to trade the borrowed funds with Arkis's supported protocols. All positions are held by the Margin Account until the borrower closes their position or the Margin Account is liquidated. The Arkis Insurance Fund is designed to cover potential losses from liquidations.

A notable feature of Arkis is its hybrid architecture. The on-chain features include the liquidity pools, insurance fund, margin accounts, and their related integrations to facilitate trades with DeFi protocols. All functionality relating to initially opening and funding a Margin Account, assessing position health, and performing liquidations is performed/initiated off-chain by the Arkis back-end. **We would like to emphasize that this audit only covers the on-chain features of the protocol and cannot verify the correctness of position health evaluation or timely liquidations.**

Over the course of the audit, we found issues relating to Lenders providing interest-free loans (ARK-1), faulty accounting for Lender rewards (ARK-2 & ARK-3), and the potential to overwrite debt entries (ARK-4). Other smaller issues relating to correctly enforcing the whitelisting mechanisms were also uncovered (ARK-6 & ARK-7). We found the project to be well-tested and well-documented. The Arkis team was available to answer any questions and provide code walkthroughs.

Fix Review Update: All of the listed issues have been adequately addressed by the Arkis team.

ID	DESCRIPTION	SEVERITY	STATUS
ARK-1	**Lenders Provide an Interest-Free Loan if the Protocol Has Insufficient Liquidity**	● Medium ⓘ	Acknowledged
ARK-2	**Users Could Lose Rewards Due to Missing Check in** `RewardsMath`	● Medium ⓘ	Fixed
ARK-3	**Faulty Accounting when Claiming Rewards for Mutiple Epochs**	● Medium ⓘ	Fixed
ARK-4	**Debt Entries Can Be Overwritten**	● Medium ⓘ	Fixed
ARK-5	**Privileged Roles and Ownership**	● Medium ⓘ	Acknowledged
ARK-6	**Compliance May Be Bypassed for Curve**	● Low ⓘ	Fixed

ID	DESCRIPTION	SEVERITY	STATUS
ARK-7	Missing Whitelist Enforcements	● Low ⓘ	Fixed
ARK-8	Liquidity Providers Can Lose Tokens Due to Unsafe Casting	● Low ⓘ	Fixed
ARK-9	Missing Input Validation	● Low ⓘ	Fixed
ARK-10	Trapped Tokens in ConvexFi	● Low ⓘ	Fixed
ARK-11	Fetch Once and Reuse to Improve Gas Consumption	● Informational ⓘ	Fixed
ARK-12	Unlocked Pragma	● Informational ⓘ	Fixed
ARK-13	'Dead' Code	● Informational ⓘ	Fixed
ARK-14	Checks-Effects-Interactions Pattern Violation	● Informational ⓘ	Fixed
ARK-15	Inconsistent Naming Hinders Code Comprehension & Collaboration	● Informational ⓘ	Fixed
ARK-16	`GetOperator()` Function Overloads the	● Undetermined ⓘ	Acknowledged

ID	DESCRIPTION	SEVERITY	STATUS
	Payload Information		
ARK-17	MultiBlock MEV Vulnerability	● Undetermined ⓘ	Acknowledged

Assessment Breakdown

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

> **Disclaimer**
>
> Only features that are contained within the repositories at the commit hashes specified on the front page of the report are within the scope of the audit and fix review. All features added in future revisions of the code are excluded from consideration in this report.

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

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

Methodology

1. Code review that includes the following
   1. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
   2. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.

    3. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
    1. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    2. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Scope

Files Included

- `contracts/*`

Files Excluded

- `helm/*`
- `scripts/*`
- `deployments/*`
- `lib/*`

Findings

ARK-1

Lenders Provide an Interest-Free Loan if the Protocol Has Insufficient Liquidity

● Medium ⓘ Acknowledged

> **Update**
>
> Marked as "Acknowledged" by the client.
>
> The client provided the following explanation:

> We understand this issues and this is the part of the business logic. If a pool does not have liquidity but user decided still to withdraw he will be first in the withdrawal queue by refusing to receive interest.

File(s) affected: `Pool.sol`

Description: When `withdraw()` is called, the pool may lack the liquidity for a Liquidity Provider to withdraw their position. In this case, their position is deleted after tallying their debt in a queue. Positions are repaid as rewards are distributed via `returnAndDistribute()` .

While a perfect liquidation mechanism could guarantee that all positions are eventually repaid, liquidity providers are not guaranteed to receive their withdrawals within any clear time horizon. In the meantime, they no longer accumulate rewards, resulting in providing an interest-free loan to the protocol.

Recommendation: Keep accumulating rewards for liquidity providers until they receive back their liquidity. To help speed the repayment process, consider calling `debt.tryRepay()` on calls to `deposit()` as well.

ARK-2

Users Could Lose Rewards Due to Missing Check in `RewardsMath`

● Medium ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `2710769ea023cee8bac188302d9d0b9f91a79490` .

File(s) affected: `RewardsMath.sol`

Description: The function `RewardsMath.increaseInterest()` updates the state `Staking.TPSS` by adding to it a factor based on the input `_rewardsAmount` , as seen in the following line: `self.TPSS += uint240((_rewardsAmount * TPSS_DENOMINATOR) / (self.tokenVolume))` . Afterwards, a new epoch is started and a few state variables are updated in the subsequent call to `startNewEpoch()` as seen below:

```
function startNewEpoch(Staking storage self, uint256
passingEpochTPSS) private {
    self.linkedListTPSS[passingEpochTPSS] = self.TPSS;
    self.tokenVolume = 0;
    self.epochStartTime[self.TPSS] = block.timestamp;
```

```
        self.numberOfEpochs++;
    }
```

If the value of `_rewardsAmount` is zero, then the “new” TPSS will be the same as the old one which leads to two errors:

1. The linked list will be pointing to itself `self.linkedListTPSS[passingEpochTPSS] = self.TPSS` since `passingEpochTPSS` is equal to `self.TPSS` .
2. The epoch start time of `self.TPSS` will be overwritten with a newer timestamp.

Impact

1. **Users would get zero rewards from the incomplete first epoch**.

The function `calculateUserRewardsForIncompleteFirstEpoch()` calculates the rewards based on the multiplicative factor `userFirstEpochTPSS = nextEpochTPSS - depositEpoch.TPSS` . Any user with `depositEpoch.TPSS` equal to the old `self.TPSS` would get a factor zero and therefore zero rewards.

2. **Users would get the wrong rewards from the complete epochs**.

The function `calculateUserRewardsForTheWholeNumberOfEpochs()` calculates the rewards based on the multiplicative factor `tpsForTheRemainingEpochs = ((lastRewardTime - ufeEndTime) * (self.TPSS - nextTPSSFromUserDepositEpoch)) / numberOfWholeUserEpochs` .

There are three members in this equation: `numberOfWholeUserEpochs` would be the correct since it was updated correctly in `startNewEpoch()` . However:

- `A = (lastRewardTime - ufeEndTime)` where `ufeEndTime = self.epochStartTime[nextTPSSFromUserDepositEpoch]` . The timestamp in `ufeEndTime` would be newer (greater) than what it should be which leads to a difference lower that expected.
- `B = (self.TPSS - nextTPSSFromUserDepositEpoch)` . If we assume the value of `self.TPSS` cannot be increased to compensate for that repeated update, then the current value of `self.TPSS` and `nextTPSSFromUserDepositEpoch` could more or less compensate each other resulting in the expected value of `B` . However, if the error of updating `TPSS` with the same old value happens multiple times, factor `B` would be lower than expected. On the other hand, if the value of `self.TPSS` can indeed by increased to compensate for that repeated updated, then the value of `B` could be greater than expected and this could compensate to some extent the lower value from `A` . However, it would still result in the wrong values.

Any user with `depositEpoch.TPSS` equal to the old `self.TPSS` could get a different reward amount which could potentially reduce the amount of available tokens for other users.

Exploit Scenario:

1. User `u1` makes a deposit at `t_0`. Resulting state:

   ```
       numberOfEpochs = 4
       TPSS = 9
       timeWhenVolumeWasLastUpdated = t_0
       linkedListTPSS[TPSS = 9] = 0
       epochStartTime[TPSS = 9] = startOfEpoch4
       users[u1].depositEpoch.TPSS = 9
       users[u1].depositEpoch.epochNum = 4
       users[u1].depositEpoch.timeWhenUserVolumeWasLastUpdated
   = t_0
   ```

2. Two epochs go by but there is no update for the user. Resulting state:

   ```
       numberOfEpochs = 6
       TPSS = 11
       timeWhenVolumeWasLastUpdated = t_2
       linkedListTPSS[TPSS = 9] = 10
       linkedListTPSS[TPSS = 10] = 11
       linkedListTPSS[TPSS = 11] = 0
       epochStartTime[TPSS = 9] = startOfEpoch4
       epochStartTime[TPSS = 10] = t_1
       epochStartTime[TPSS = 11] = t_2
       users[u1] => unchanged
   ```

3. A new epoch goes by but the error is introduced. Resulting state:

   ```
       numberOfEpochs = 7
       TPSS = 11 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< ERROR:
   stayed the same
       timeWhenVolumeWasLastUpdated = t_3
       linkedListTPSS[TPSS = 9] = 10
       linkedListTPSS[TPSS = 10] = 11
       linkedListTPSS[TPSS = 11] = 0 -> 11 <<<<<< overwritten
   to itself
       epochStartTime[TPSS = 9] = startOfEpoch4
       epochStartTime[TPSS = 10] = t_1
       epochStartTime[TPSS = 11] = t_2 -> t_3 <<< overwritten
   to newer ts
       users[u1] => unchanged
   ```

4. In the same epoch 7, user `u1` claims or makes a new deposit. The difference `(self.TPSS - nextTPSSFromUserDepositEpoch)` in `calculateUserRewardsForTheWholeNumberOfEpochs()` would be lower than expected since `self.TPSS` did not increase, leading to less rewards for the users. Resulting state for the user:

```
    users[u1].depositEpoch.TPSS = 11
    users[u1].depositEpoch.epochNum = 7
    users[u1].depositEpoch.timeWhenUserVolumeWasLastUpdated
= t_3
```

5. If the same user `u1` claims or deposits one or more epochs later, the rewards from the incomplete epoch would be zero as mentioned in impact number 1 (description above). As for impact number 2, the rewards would actually be greater than expected which would leave other users with less available tokens:
    - `(lastRewardTime - ufeEndTime) => (t_5 - t_3)` ⇒ would still be correct.
    - `(self.TPSS - nextTPSSFromUserDepositEpoch) => (13 - 11)` ⇒ would be greater than expected since `nextTPSSFromUserDepositEpoch` would be lower than expected.

Recommendation: Validate that `_rewardsAmount` is greater than zero.

ARK-3

Faulty Accounting when Claiming Rewards for Mutiple Epochs

● Medium ⓘ Fixed

> **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `fc1aef13ebdb852f69425438ae183c8077b77a5c` .

File(s) affected: `RewardsMath.sol`

Description: Liquidity Providers accumulate rewards across epochs. Rewards are recalculated and distributed when they interact with the Pool. If it has been several epochs since the user last interacted with the pool, the function `calculateUserRewardsForTheWholeNumberOfEpochs()` calculates the rewards for elapsed epochs by applying the average TPS of the epochs across the elapsed time.

However, the calculation assumes that each epoch is identical in length. Rewards should be distributed in proportion with the length of the epoch.

Exploit Scenario:

1. LP stakes into the protocol.
2. Epoch 1 elapses with a TPS of 10, and lasts for 10 seconds.
3. Epoch 2 elapses with a TPS of 100, and lasts for 1 year.

4. LP claims rewards. Given that the average TPS of the epochs is 55, the user is rewarded according to 55 TPS * (1 year + 10 seconds). This yields a different result than (10 TPS * 10 seconds) + (100 TPS * 1 year).

Recommendation: Consider the individual length of an epoch when calculating the rewards.

ARK-4
Debt Entries Can Be Overwritten

● Medium ⓘ Fixed

✓ **Update**

Marked as "Fixed" by the client.
Addressed in: `f12aeacb9b0f6015270cfdf3ca1602217739bd6a` .

File(s) affected: `DebtLibrary.col` , `Fund.sol` , `MoneyAccountant.sol`

Description: Part of the execution flow of `Fund.forward()` involves calling `MoneyAccount.spendMoney(amount, reward, block.timestamp)` , where `block.timestamp` serves as a nonce. If `spendMoney()` is called more than once in the same block with identical parameters, any child calls to `createDebtIfNecessary()` will overwrite previous debt entries, and not all debt will be accounted for. This is in part because the `block.timestamp` acts as a salt rather than a true nonce.

Recommendation: If it is possible for `Fund.forward()` to be called with the same parameters in a single block, consider using a different source for the nonce.

ARK-5
Privileged Roles and Ownership

● Medium ⓘ Acknowledged

ⓘ **Update**

Marked as "Acknowledged" by the client.
The client provided the following explanation:

We acknowledge this, and always stress on a fact that our margin engine is centralized and disclose this in our marketing , technical and product documentation

File(s) affected: `Account.sol` , `Dispatcher.sol` , `Pool.sol`

Description: We would like to emphasize that Arkis is a centralized protocol by design. Users should be aware that a compromised protocol admin would have the power to reroute funds by:

1. Liquidating any Margin Account at any time, regardless of position health.
2. Draining all Arkis liquidity pools.

Recommendation: This centralization of power needs to be made clear to the users, especially depending on the level of privilege the contract allows to the owner.

ARK-6

Compliance May Be Bypassed for Curve

● Low ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
>
> Addressed in: `6246e0d18a7295095b6cc2930b671f7b100592c1` .

File(s) affected: `CurveFiValidatorSwapRouter.sol`

Description: To add liquidity to Curve, it is required that the protocol is supported, but to withdraw or exchange it may be either supported or suspended. The curve function `Swaps.exchange_multiple` takes a `_swap_params` argument that determines the swap type. If the argument passed is `7, 8, 9, 10` or `11` then the swap will call `add_liquidity()` and add liquidity to the pool. The compliance check for `exchange_multiple()` on Arkis does not check the `_swap_params` so it may be used to add liquidity to Curve should it ever become suspended.

Recommendation: Validate the `uint256[3][4]``_swap_params` argument, to ensure that it is not bypassing restricted protocol functions.

ARK-7

Missing Whitelist Enforcements

● Low ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
>
> Addressed in: `e8fcab8c558911405058b457d95b228cf51b8b5d` .

File(s) affected: `CurveFiEvaluator.sol`

Description: We uncovered a few issues relating to whitelisting/permissions of different protocol interactions.

1. `UniswapV3Evaluator.evaluate(address, ExchangeRequest)` enforces that both the input token and output token are supported. Requiring that the input token be supported (rather than supported or suspended) may prevent favorable trades when liquidating margin accounts. Given that other dexes without this restriction are available, the issue has been marked as Informational severity.
2. The `CurveFiValidatorPlainPool.remove_liquidity()` checks that the pool coins are supported or suspended before creating the `Command` to remove liquidity. However, no token validation is done when adding liquidity.
3. The documentation states the following regarding whitelist enforcements for exchanges:

> For exchange: `operator`, `pool` and `input token` MAY be either supported or suspended, but `output token` MUST be supported.

However, `CurveFiEvaluator.evaluate(address, ExchangeRequest)` does not enforce that the output token is supported.

Recommendation:

1. Consider allowing the input token to be supported or suspended in `UniswapV3Evaluator.evaluate(address, ExchangeRequest)`.
2. Validate that the output tokens are supported in `CurveFiValidatorPlainPool.add_liquidity()`.
3. Validate that the output token is supported in `CurveFiEvaluator.evaluate(address, ExchangeRequest)`.

ARK-8
Liquidity Providers Can Lose Tokens Due to Unsafe Casting

● Low ⓘ Fixed

✓ **Update**

Marked as "Fixed" by the client.
Addressed in: `284504531f3c964ec2c8967336ba76f705905f08`.

File(s) affected: `DebtLibrary.sol`

Description: The `DebtLibrary.createDebt()` function returns a new `Debt` object with the debt amount and rewards. However, these two values are cast from `uint256` to `uint128` without making sure that the values fit in 128 bits. This could potentially lead to the `Fund` forwarding less than it should to its corresponding `Pool` which means that users might end up with fewer tokens than deposited, and also fewer rewards.

Recommendation: Consider reverting if the `uint256` value is greater than the max value of a `uint128` .

ARK-9 Missing Input Validation

● Low ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `f6022f6baf9f9af23733d7e8ffaa1508b6168b65` .

File(s) affected: `Account.sol` , `CommandSafeExecutor.sol` , `Pool.sol` , `PoolFactory.sol`

Related Issue(s): SWC-123

Description: It is important to validate inputs, even if they only come from trusted addresses, to avoid human error. The following is a non-exhaustive list of inputs that should be validated:

1. `Account.constructor()` : Validate that the `_marginEngine` is not `address(0)` since it is an immutable variable and would need to be redeployed otherwise.
2. `CurveFiLiquidityPoolsRepository.initializePool()` : Validate that the pool has the specified `numberOfTokens` .
3. `CommandSafeExecutor.constructor()` : Validate that `compliance` is not `address(0)` since it is an immutable variable and would need to be redeployed otherwise.
4. `Fund.initialize()` : Validate that the `debtAdmin` is a non-zero address.
5. `ProtocolsRepository.updateProtocolSupport()` : Validate that `_protocol` is a non-empty string.
6. `ProtocolsRepository.updateOperatorSupport()` : Validate that `_protocol` is a non-empty string.
7. `PoolFactory.createPool()` and `Pool.initialize()` : Neither function validates the borrower and token address against `address(0)` . There is also no validation on `thresholdOnTotalDeposit_` making it possible for it to be zero. All three values are only set during the initialization of the pool and cannot be set later on. A wrong configuration would mean redeploying the pool.

Recommendation: We recommend adding the relevant checks.

ARK-10 Trapped Tokens in ConvexFi

● Low ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `cfcf1904d3b9990556239ba3bc512beaf9824d28` .

File(s) affected: `ConvexFiDecreasePosition.sol` , `ConvexFiValidator.sol`

Description: If a user is liquidated, their Convex positions are assumed to be staked into the `RewardPool` or `Booster` . However, it is possible that the user has Deposit Tokens that have not been staked. Liquidating these tokens would require a tedious process as they will be omitted by the `DecreasePositionRequest` .

Recommendation: Require users to stake their deposit tokens by validating that `stake == true` in `ConvexFiValidator.deposit(uint256, uint256, bool)` and `ConvexFiValidator.depositAll()` . Additionally, disable the `ConvexFiValidator.withdraw(uint256, bool)` and `ConvexFiValidator.withdrawAll(bool)` functions such that the user cannot unstake and receive Deposit Tokens.

ARK-11
Fetch Once and Reuse to Improve Gas Consumption

● Informational ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `5c9185669f31b281a89711753eba914ea22219de` .

File(s) affected: `DebtManager.sol` , `ProtocolsRepository.sol` , `RewardsMath.sol`

Description: The following are some opportunities for gas savings:

1. `ProtocolsRepository.updateProtocolSupport()` fetches the given protocol twice instead of once and reusing it. The condition in the `else if` branch can just call `prot.status` instead of `protocol(_protocol).status` .
2. `DebtManager.tryRepay()` calls `self.peek()` twice in stead of once and reuse it. The body of the `if` branch could just call `debt.partialRepay()` instead of using `self.peek().partialRepay()` .
3. `RewardsMath.calculateNewUserVolume()` fetches `depositEpoch.timeWhenUserVolumeWasLastUpdated` twice instead of once and reusing it.

ARK-12 Unlocked Pragma

● Informational ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `0ebfaa45c8345789d616e82e606cb712f81d3d3c` .

File(s) affected: `All Contracts`

Related Issue(s): SWC-103

Description: Every Solidity file specifies in the header a version number of the format `pragma solidity (^)0.8.*` . The caret (`^`) before the version number implies an unlocked pragma, meaning that the compiler will use the specified version *and above*, hence the term "unlocked".

Recommendation: For consistency and to prevent unexpected behavior in the future, we recommend to remove the caret to lock the file onto a specific Solidity version.

ARK-13 'Dead' Code

● Informational ⓘ Fixed

> ✓ **Update**
>
> Marked as "Fixed" by the client.
> Addressed in: `91b0fdd9719e460ccb20a773bde6f8fb775a6512` .

File(s) affected: `AccountFactory.sol` , `ConvexFiImmutableState.sol` , `InternalModifierDS.sol`

Related Issue(s): SWC-131, SWC-135

Description: Dead code should be avoided since it might consume more resources during development, testing, and compilation without contributing to the software's functionality. It makes the codebase harder to understand and may mislead developers, leading to potential bugs or wasted time. In the case of solidity, it might also increase the bytecode size increasing deployment costs.

The following is a non-exhaustive list of dead or unused code instances:

1. The contract `ConvexFiImmutableState` is never imported or used anywhere in the codebase.
2. The variable `borrower` in the `AccountFactory` contract is private and is not used anywhere in the contract.
3. The abstract contract `InternalModifierDS` is never imported or used anywhere in the codebase.

Recommendation: We recommend that the team look into this further and determine whether the code can be removed.

ARK-14 Checks-Effects-Interactions Pattern Violation

● Informational ⓘ Fixed

> ✓ **Update**
> Marked as "Fixed" by the client.
> Addressed in: `422487670b0a2ba268fe794f68541bc57563b5df` .

File(s) affected: `Pool.sol`

Related Issue(s): SWC-107

Description: The Checks-Effects-Interactions coding pattern is meant to mitigate any chance of other contracts manipulating the state of the blockchain in unexpected and possibly malicious ways before control is returned to the original contract. As the name implied, only after checking whether appropriate conditions are met and acting internally on those conditions should any external calls to, or interactions with, other contracts be done.

The function `Pool.deposit()` updates the state through `staking.increasePosition()` after doing the external call `token.transferFrom()` .

Recommendation: We recommend refactoring the code so that it conforms to the Checks-Effects-Interactions pattern.

ARK-15 Inconsistent Naming Hinders Code Comprehension & Collaboration

● Informational ⓘ Fixed

> ✓ **Update**
> Marked as "Fixed" by the client.
> Addressed in: `a52227e4237923c77122e34e82d0d143e38a8379` .

File(s) affected: `liquidityManagement/insuranceFund/libraries/Debt.sol` , `interfaces/liquidityManagement/insuranceFund/Debt.sol` , `liquidityManagement/liquidityPool/libraries/DebtManager.sol`

Description: Having two classes or files with the same name should be avoided since it causes ambiguity, confusion, and potential naming conflicts. It also compromises code readability, comprehension, and collaboration. There are two structs called `Debt` in the codebase: the first struct is defined in `interfaces/liquidityManagement/insuranceFund/Debt.sol` , and the second is defined in `liquidityManagement/liquidityPool/libraries/DebtManager.sol` . Additionally, there are two files called `Debt.sol` : the one already mentioned and `liquidityManagement/insuranceFund/libraries/Debt.sol` .

Recommendation: We recommend renaming at least one of the data structures and one of the files.

ARK-16

`GetOperator()` Function Overloads the Payload Information

● Undetermined ⓘ

Acknowledged

Update

Marked as "Acknowledged" by the client.
The client provided the following explanation:

We understand the issue and will fix it later. This is not subject platform to any risks right now because we have not added any validator with "bytes" argument (like 1inch validator). Before adding such validator the issue will be mitigated.

File(s) affected: `AbstractValidator.sol` , `CommandSafeExecutor.sol` , `SafeCall.sol`

Description: The `AbstractValidator.getOperator()` function validates the status of the operator defined by the last word (32 bytes) of `msg.data` . However, the same `msg.data` is used to form a command and call a function. Hence, the message data is overloaded as it needs to specify both a function and an operator. This could accidentally send incorrect msg.data.

Though extraneous `msg.data` is usually discarded, if the final argument of a function is a bytes array, the operator's address may be included as a function argument.

Recommendation: Ensure that any appended data is not accidentally sent out when making an external function call to a whitelisted operator. Confirm whether any of the protocol integrations may contain a function that would overload the intended parameters.

ARK-17 MultiBlock MEV Vulnerability

● Undetermined ⓘ Acknowledged

> **Update**
> Marked as "Acknowledged" by the client.
> The client provided the following explanation:
>
> We acknowledge this fact and will notify users. However, taking into account that most of pools lenders are single parties - the probability of the exploit is low.

File(s) affected: `RewardsMath.sol`

Description: Currently, block builders and validators can collude to guarantee multiple blocks in a row. If such collusion were to occur it would be possible for these miners to artificially inflate token volume without taking any risk by making a very large deposit at the first block and then a withdrawal at the last block, while censoring any Arkis-related transactions in between.

As such they can benefit from an inflated token volume without assuming any of the risk normally associated with lending out tokens.

Recommendation: Ensure that users are made aware of the risks, or consider only offering rewards to funds that have been utilized by the fund manager.

Definitions

- **High severity** – High-severity issues usually put a large number of users' sensitive information at risk, or are reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
- **Medium severity** – Medium-severity issues tend to put a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or are reasonably likely to lead to moderate financial impact.

- **Low severity** – The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
- **Informational** – The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
- **Undetermined** – The impact of the issue is uncertain.
- **Fixed** – Adjusted program implementation, requirements or constraints to eliminate the risk.
- **Mitigated** – Implemented actions to minimize the impact or likelihood of the risk.
- **Acknowledged** – The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).

Appendix

File Signatures

The following are the SHA-256 hashes of the reviewed files. A file with a different SHA-256 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review.

Files

- `bd7...20f ./contracts/interfaces/base/proxy/IBeacon.sol`
- `ed1...209 ./contracts/interfaces/marginEngine/Envelope.sol`
- `508...c43 ./contracts/interfaces/marginEngine/Package.sol`
- `4e0...7f8 ./contracts/interfaces/marginEngine/IDispatcher.sol`
- `2eb...536 ./contracts/interfaces/common/IInitializable.sol`
- `e9c...ed0 ./contracts/interfaces/accountAbstraction/compliance/IWhitelistingController.sol`
- `1c6...ac2 ./contracts/interfaces/accountAbstraction/compliance/Asset.sol`
- `862...bf7 ./contracts/interfaces/accountAbstraction/compliance/oneinchV5/index.sol`

- a46...c89 ./contracts/interfaces/accountAbstraction/compliance/oneinchV5/IAggregationRouterV5.sol
- 6fe...01e ./contracts/interfaces/accountAbstraction/compliance/oneinchV5/IUniswapPool.sol
- b6a...08b ./contracts/interfaces/accountAbstraction/compliance/lidoFi/IStEth.sol
- 930...f1a ./contracts/interfaces/accountAbstraction/compliance/lidoFi/IWstEth.sol
- e10...529 ./contracts/interfaces/accountAbstraction/compliance/curveFi/index.sol
- 041...34e ./contracts/interfaces/accountAbstraction/compliance/curveFi/ICurveFiZapper.sol
- 66f...0d9 ./contracts/interfaces/accountAbstraction/compliance/curveFi/ICurveFiGauge.sol
- bb9...047 ./contracts/interfaces/accountAbstraction/compliance/curveFi/ICurveFiMinter.sol
- da9...6d6 ./contracts/interfaces/accountAbstraction/compliance/curveFi/ICurveFiRouter.sol
- be8...254 ./contracts/interfaces/accountAbstraction/compliance/curveFi/ICurveFiPool.sol
- b8b...6af ./contracts/interfaces/accountAbstraction/compliance/uniswapV3/index.sol
- 1e7...447 ./contracts/interfaces/accountAbstraction/compliance/uniswapV3/IUniswapV3Pool.sol
- cb2...17e ./contracts/interfaces/accountAbstraction/compliance/uniswapV3/INonfungiblePositionManager.sol
- 129...0b9 ./contracts/interfaces/accountAbstraction/compliance/uniswapV3/ISwapRouter.sol

- 807...349 ./contracts/interfaces/accountAbstraction/compliance/convexFi/index.sol
- db6...ea6 ./contracts/interfaces/accountAbstraction/compliance/convexFi/ICrvDepositor.sol
- a7e...46e ./contracts/interfaces/accountAbstraction/compliance/convexFi/IClaimZap.sol
- 5f8...830 ./contracts/interfaces/accountAbstraction/compliance/convexFi/IBooster.sol
- d5a...232 ./contracts/interfaces/accountAbstraction/compliance/convexFi/IRewardPool.sol
- 2c2...94d ./contracts/interfaces/accountAbstraction/marginAccount/IAccount.sol
- eba...a33 ./contracts/interfaces/accountAbstraction/marginAccount/IAccountFactory.sol
- 67b...2f7 ./contracts/interfaces/accountAbstraction/interpreter/ILiquidityPoolsController.sol
- ca3...883 ./contracts/interfaces/accountAbstraction/interpreter/IJitCompiler.sol
- 406...0ca ./contracts/interfaces/accountAbstraction/interpreter/Command.sol
- 8ca...d7f ./contracts/interfaces/accountAbstraction/interpreter/IInterpreter.sol
- bbf...361 ./contracts/interfaces/accountAbstraction/interpreter/Script.sol
- 72f...52c ./contracts/interfaces/accountAbstraction/interpreter/adapters/index.sol
- d96...b83 ./contracts/interfaces/accountAbstraction/interpreter/adapters/PositionDescriptor.sol

- 407...c3e ./contracts/interfaces/accountAbstraction/interpreter/adapters/IDecreasePositionEvaluator.sol
- 0c6...d67 ./contracts/interfaces/accountAbstraction/interpreter/adapters/IIncreasePositionEvaluator.sol
- 662...12e ./contracts/interfaces/accountAbstraction/interpreter/adapters/ILiquidityPoolsRepository.sol
- 8bc...72d ./contracts/interfaces/accountAbstraction/interpreter/adapters/IExchangeEvaluator.sol
- eeb...ea6 ./contracts/interfaces/liquidityManagement/liquidityPool/IPoolInitializer.sol
- 962...d5e ./contracts/interfaces/liquidityManagement/liquidityPool/ISuspendable.sol
- 8aa...ff9 ./contracts/interfaces/liquidityManagement/liquidityPool/IMerkleTreeWhitelist.sol
- 282...27d ./contracts/interfaces/liquidityManagement/liquidityPool/IPool.sol
- 5d9...37b ./contracts/interfaces/liquidityManagement/liquidityPool/ILiquidityPool.sol
- 6db...5e3 ./contracts/interfaces/liquidityManagement/liquidityPool/IPoolFactory.sol
- 062...6db ./contracts/interfaces/liquidityManagement/insuranceFund/IFund.sol
- ad2...e59 ./contracts/interfaces/liquidityManagement/insuranceFund/Debt.sol
- 6af...895 ./contracts/interfaces/liquidityManagement/insuranceFund/IFundInitializer.sol
- 241...7ff ./contracts/interfaces/liquidityManagement/insuranceFund/IFundFactory.sol
- 710...450 ./contracts/base/CommonErrors.sol

- 55b...174 ./contracts/base/FixedU256x32.sol
- 3c3...708 ./contracts/base/StateMachine.sol
- 89a...4ab ./contracts/base/auth/AccessControlDS.sol
- 71a...b1f ./contracts/base/auth/OwnableReadonlyDS.sol
- b5d...0f3 ./contracts/base/auth/InternalModifierDS.sol
- 627...37c ./contracts/base/auth/OwnableAssignable.sol
- db7...61f ./contracts/base/auth/OwnableReadonly.sol
- 986...c77 ./contracts/base/proxy/ImmutableBeaconProxy.sol
- 367...711 ./contracts/base/proxy/BeaconDS.sol
- 289...57f ./contracts/marginEngine/Dispatcher.sol
- bd7...805 ./contracts/marginEngine/base/SignatureProcessor.sol
- e19...1b3 ./contracts/marginEngine/base/ThresholdsVerifier.sol
- 925...8c3 ./contracts/marginEngine/libraries/Envelope.sol
- f54...02e ./contracts/marginEngine/libraries/Package.sol
- b54...b3d ./contracts/accountAbstraction/compliance/WhitelistingController.sol
- a38...63f ./contracts/accountAbstraction/compliance/AbstractValidator.sol
- 4d5...a96 ./contracts/accountAbstraction/compliance/approve/ApproveValidator.sol
- 68f...496 ./contracts/accountAbstraction/compliance/lidoFi/LidoFiValidator.sol
- 663...458 ./contracts/accountAbstraction/compliance/curveFi/CurveFiValidator.sol
- b8e...cd9 ./contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorMetapool.sol
- 928...104 ./contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorSwapRouter.sol
- f03...6bc ./contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorPlainPool.sol

- b5b...916 ./contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorZapper.sol
- f2c...d01 ./contracts/accountAbstraction/compliance/libraries/TokensRepository.sol
- 6e2...9e7 ./contracts/accountAbstraction/compliance/libraries/ProtocolsRepository.sol
- 4bb...3bc ./contracts/accountAbstraction/compliance/uniswapV3/UniswapV3Validator.sol
- 159...ff0 ./contracts/accountAbstraction/compliance/convexFi/ConvexFiValidator.sol
- b43...9ba ./contracts/accountAbstraction/marginAccount/Account.sol
- 5f3...279 ./contracts/accountAbstraction/marginAccount/AccountFactory.sol
- 05a...28e ./contracts/accountAbstraction/marginAccount/base/CommandSafeExecutor.sol
- b85...422 ./contracts/accountAbstraction/marginAccount/libraries/AccountFactoryRepository.sol
- 82a...585 ./contracts/accountAbstraction/interpreter/LiquidityPoolsController.sol
- d5f...848 ./contracts/accountAbstraction/interpreter/JitCompiler.sol
- 057...865 ./contracts/accountAbstraction/interpreter/base/LiquidityPoolsRepository.sol
- a71...297 ./contracts/accountAbstraction/interpreter/arkis/LiquidityPoolEvaluator.sol
- 408...117 ./contracts/accountAbstraction/interpreter/arkis/InsuranceFundEvaluator.sol
- 7fd...7c3 ./contracts/accountAbstraction/interpreter/arkis/MarginAccountEvaluator.sol

- 84b...ee0 ./contracts/accountAbstraction/interpreter/oneinchV5/OneInchV5Evaluator.sol
- 0df...086 ./contracts/accountAbstraction/interpreter/oneinchV5/base/OneInchV5Hub.sol
- afd...d50 ./contracts/accountAbstraction/interpreter/oneinchV5/base/OneInchV5ImmutableState.sol
- 02f...9fc ./contracts/accountAbstraction/interpreter/oneinchV5/actions/OneInchV5Exchange.sol
- 6c1...548 ./contracts/accountAbstraction/interpreter/oneinchV5/libraries/UniswapTokens.sol
- 3ed...d9f ./contracts/accountAbstraction/interpreter/lidoFi/LidoFiEvaluator.sol
- 879...8ac ./contracts/accountAbstraction/interpreter/lidoFi/LidoFiLiquidityPoolsRepository.sol
- 2aa...243 ./contracts/accountAbstraction/interpreter/lidoFi/base/LidoFiImmutableState.sol
- d53...af8 ./contracts/accountAbstraction/interpreter/curveFi/CurveFiLiquidityPoolsRepository.sol
- 1b5...81f ./contracts/accountAbstraction/interpreter/curveFi/CurveFiEvaluator.sol
- 6bc...d5f ./contracts/accountAbstraction/interpreter/curveFi/actions/CurveFiDecreasePosition.sol
- 353...4d3 ./contracts/accountAbstraction/interpreter/curveFi/actions/CurveFiHarvestYield.sol
- 8c9...726 ./contracts/accountAbstraction/interpreter/curveFi/actions/CurveFiExchange.sol
- 203...168 ./contracts/accountAbstraction/interpreter/curveFi/libraries/CurveFiLib.sol

- 3ea...f00 ./contracts/accountAbstraction/interpreter/libraries/ScriptCompiler.sol
- d4f...607 ./contracts/accountAbstraction/interpreter/libraries/Path.sol
- 248...a7e ./contracts/accountAbstraction/interpreter/libraries/Config.sol
- 1b8...763 ./contracts/accountAbstraction/interpreter/transfer/TransferEvaluator.sol
- d99...d3e ./contracts/accountAbstraction/interpreter/uniswapV3/UniswapV3Evaluator.sol
- 77b...3a8 ./contracts/accountAbstraction/interpreter/uniswapV3/UniswapV3LiquidityPoolsRepository.sol
- d75...0e7 ./contracts/accountAbstraction/interpreter/uniswapV3/base/UniswapV3ImmutableState.sol
- 5e8...c70 ./contracts/accountAbstraction/interpreter/uniswapV3/actions/UniswapV3DecreasePosition.sol
- d26...de2 ./contracts/accountAbstraction/interpreter/uniswapV3/actions/UniswapV3HarvestYield.sol
- a63...362 ./contracts/accountAbstraction/interpreter/uniswapV3/actions/UniswapV3Exchange.sol
- e1c...313 ./contracts/accountAbstraction/interpreter/uniswapV3/libraries/UniswapV3Path.sol
- b32...2a5 ./contracts/accountAbstraction/interpreter/convexFi/ConvexFiLiquidityPoolsRepository.sol
- 0ff...475 ./contracts/accountAbstraction/interpreter/convexFi/ConvexFiEvaluator.sol
- 4fa...e4d ./contracts/accountAbstraction/interpreter/convexFi/base/ConvexFiImmutableState.sol
- 704...fa8 ./contracts/accountAbstraction/interpreter/convexFi/actions/C

onvexFiDecreasePosition.sol

- 9b1...58e ./contracts/libraries/AddressRegistry.sol
- 719...53e ./contracts/libraries/Nonce.sol
- 89c...a44 ./contracts/libraries/Address.sol
- 202...154 ./contracts/libraries/SafeCall.sol
- bba...7af ./contracts/libraries/Command.sol
- 6f1...c24 ./contracts/libraries/CalldataLibrary.sol
- a70...59e ./contracts/libraries/DiamondLib.sol
- 241...f8b ./contracts/libraries/Asset.sol
- 5d0...8f6 ./contracts/liquidityManagement/liquidityPool/PoolFactory.sol
- ea7...b7a ./contracts/liquidityManagement/liquidityPool/MerkleTreeWhitelist.sol
- a26...37f ./contracts/liquidityManagement/liquidityPool/base/Suspendable.sol
- d84...0fb ./contracts/liquidityManagement/liquidityPool/pool/Pool.sol
- 19f...b9f ./contracts/liquidityManagement/liquidityPool/libraries/Queue.sol
- 416...d19 ./contracts/liquidityManagement/liquidityPool/libraries/MerkleTreeRepository.sol
- f8d...7bc ./contracts/liquidityManagement/liquidityPool/libraries/DebtManager.sol
- 747...dcf ./contracts/liquidityManagement/liquidityPool/libraries/staking/index.sol
- 272...bb8 ./contracts/liquidityManagement/liquidityPool/libraries/staking/errors.sol
- d1a...d8e ./contracts/liquidityManagement/liquidityPool/libraries/staking/RewardsMath.sol
- 037...1df ./contracts/liquidityManagement/liquidityPool/libraries/staking/PositionManager.sol

- 823...aa5 ./contracts/liquidityManagement/insuranceFund/FundFactory.sol
- acb...684 ./contracts/liquidityManagement/insuranceFund/fund/Fund.sol
- a83...898 ./contracts/liquidityManagement/insuranceFund/libraries/MoneyAccountant.sol
- bff...5a8 ./contracts/liquidityManagement/insuranceFund/libraries/Debt.sol

Tests

- c8e...242 ./test/fixtures.ts
- 6ef...6b1 ./test/helpers.ts
- 9d0...287 ./test/base/Address.unit.t.sol
- 67d...130 ./test/base/StateMachine.unit.t.sol
- 666...ea4 ./test/base/FixedU256x32.unit.t.sol
- c3b...3ce ./test/base/auth/AccessControlDS.unit.t.sol
- acc...6b5 ./test/base/auth/OwnableReadonlyDS.unit.t.sol
- 863...36f ./test/base/auth/OwnableReadonly.unit.t.sol
- 87d...dab ./test/base/auth/InternalModifier.unit.t.sol
- 8e6...ff8 ./test/base/auth/OwnableAssignable.unit.t.sol
- 99d...8bd ./test/base/proxy/BeaconDS.unit.t.sol
- 50d...d69 ./test/base/proxy/ImmutableBeaconProxy.unit.t.sol
- 5bf...897 ./test/marginEngine/Dispatcher&AccountFactory.integration.t.sol
- 02d...43d ./test/marginEngine/base/ThresholdsVerifier.unit.t.sol
- 112...5b9 ./test/marginEngine/base/SignatureProcessor&Nonce.integration.t.sol
- c10...392 ./test/marginEngine/libraries/Envelope&Script.integration.t.sol
- f5e...987 ./test/marginEngine/libraries/Package&Envelope&Script.integration.t.sol
- 613...f35 ./test/e2e/allocation.e2e.spec.ts
- 6e1...6aa ./test/e2e/liquidation_1inch.e2e.spec.ts

- 34d...c4e ./test/e2e/liquidation.e2e.spec.ts
- de3...52f ./test/e2e/steps/submitPlan.ts
- 10d...0f1 ./test/e2e/steps/signRegisterRequest.ts
- 7b0...c75 ./test/e2e/steps/open3poolPosition.ts
- 57f...286 ./test/e2e/steps/registerAccount.ts
- 920...749 ./test/e2e/steps/index.ts
- 4a9...57d ./test/e2e/steps/addLiquidity.ts
- 63c...06d ./test/e2e/utils/get3poolInstance.ts
- 2fb...a35 ./test/e2e/utils/asset.ts
- 537...8fc ./test/e2e/utils/index.ts
- 241...af8 ./test/e2e/utils/getMarginEngineInstance.ts
- c1a...ebf ./test/e2e/utils/expectAccountInternalState.ts
- 0c8...51c ./test/extensions/index.ts
- b9d...03d ./test/extensions/chai/common.ts
- ef9...1bf ./test/extensions/chai/types.ts
- 390...c40 ./test/extensions/chai/index.ts
- 247...2d4 ./test/extensions/chai/matchers/increaseTokenBalance.ts
- 25e...033 ./test/extensions/chai/matchers/increaseTokensBalances.ts
- 3f0...f80 ./test/extensions/chai/matchers/decreaseTokenBalance.ts
- 386...49a ./test/extensions/chai/matchers/decreaseTokensBalances.ts
- 6f8...ba2 ./test/extensions/chai/matchers/changeTokensBalances.ts
- 8f4...bd0 ./test/utils/DynamicArrays.sol
- bca...954 ./test/utils/index.sol
- 116...45f ./test/utils/MockERC20.sol
- 86a...e3e ./test/utils/MockedInstructionsExecutor.sol
- 7ab...296 ./test/utils/MockJitCompiler.sol
- f11...eb3 ./test/utils/InstructionsMocker.sol
- ad2...3d2 ./test/accountAbstraction/createMarginAccount.ts
- 957...bed ./test/accountAbstraction/compliance/WhitelistingController.unit.t.sol
- 523...6ab ./test/accountAbstraction/compliance/AbstractValidator.unit.t

.sol

- 467...e18 ./test/accountAbstraction/compliance/approve/ApproveValidator.unit.t.sol
- be2...d39 ./test/accountAbstraction/compliance/lidoFi/validator.liquidity.test.ts
- a4f...c7f ./test/accountAbstraction/compliance/curveFi/validator.swap.test.ts
- 544...a63 ./test/accountAbstraction/compliance/curveFi/validator.liquidity.test.ts
- 835...05c ./test/accountAbstraction/compliance/libraries/ProtocolsRepository.unit.t.sol
- 906...c2a ./test/accountAbstraction/compliance/libraries/StatusTestUtils.sol
- 44f...e89 ./test/accountAbstraction/compliance/libraries/TokensRepository.unit.t.sol
- bf8...3ec ./test/accountAbstraction/compliance/uniswapV3/UniswapV3ValidatorLiquidity.unit.t.sol
- de8...e23 ./test/accountAbstraction/marginAccount/AccountFactory.unit.t.sol
- 844...525 ./test/accountAbstraction/marginAccount/Account&StateMachine.integration.t.sol
- 308...21c ./test/accountAbstraction/marginAccount/base/CommandSafeExecutor&AbstractValidator.integration.t.sol
- 0e5...93d ./test/accountAbstraction/interpreter/LiquidityPoolsController.unit.t.sol
- 56b...ca8 ./test/accountAbstraction/interpreter/callManyInSingleBlock.ts
- b2b...14c ./test/accountAbstraction/interpreter/arkis/LiquidityPoolEvaluator.test.ts

- a23...dd2 ./test/accountAbstraction/interpreter/arkis/InsuranceFundEvaluator.test.ts
- 9e3...af9 ./test/accountAbstraction/interpreter/arkis/MarginAccountEvaluator.test.ts
- c32...a8f ./test/accountAbstraction/interpreter/oneInchV5/OneInchV5Evaluator.unit.t.sol
- 767...e90 ./test/accountAbstraction/interpreter/lidoFi/evaluator.liquidity.test.ts
- ee3...e41 ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorPlainPoolAddLiquidity.unit.t.sol
- fc2...928 ./test/accountAbstraction/interpreter/curveFi/evaluator.swap.test.ts
- 1e5...d16 ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorPlainPoolExchange.unit.t.sol
- 28c...9b8 ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorSwapRouter.unit.t.sol
- 0fc...da6 ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorZapperRemoveLiquidity.unit.t.sol
- 56b...cd9 ./test/accountAbstraction/interpreter/curveFi/evaluator.liquidity.test.ts
- a17...b1d ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorZapperAddLiquidity.unit.t.sol
- 600...1d0 ./test/accountAbstraction/interpreter/curveFi/CurveFiValidatorPlainPoolRemoveLiquidity.unit.t.sol
- 4cc...1b5 ./test/accountAbstraction/interpreter/libraries/ScriptCompiler.unit.t.sol
- bf6...d33 ./test/accountAbstraction/interpreter/libraries/Path.unit.t.sol

- `ca4...d90 ./test/accountAbstraction/interpreter/uniswapV3/evaluator.swap.test.ts`
- `425...886 ./test/accountAbstraction/interpreter/uniswapV3/liquidity.e2e.test.ts`
- `848...302 ./test/accountAbstraction/interpreter/uniswapV3/validator.swap.test.ts`
- `e06...802 ./test/accountAbstraction/interpreter/convexFi/validator.liquidity.test.ts`
- `f48...fd0 ./test/accountAbstraction/interpreter/convexFi/evaluator.liquidity.test.ts`
- `456...128 ./test/libraries/Asset.unit.t.sol`
- `3f3...a29 ./test/libraries/CalldataLibrary.unit.t.sol`
- `a8c...e7a ./test/libraries/ValidatorTestUtility.sol`
- `eee...d8b ./test/libraries/Nonce.unit.t.sol`
- `ddd...66f ./test/libraries/SafeCall.unit.t.sol`
- `44b...4e5 ./test/libraries/Command.t.utils.sol`
- `3ed...f70 ./test/libraries/AddressRegistry.unit.t.sol`
- `fc6...2b9 ./test/libraries/Command.unit.t.sol`
- `974...36d ./test/liquidityManagement/liquidityPool/PoolFactory.unit.t.sol`
- `bad...da6 ./test/liquidityManagement/liquidityPool/MerkleTreeWhitelist.unit.t.sol`
- `096...fd4 ./test/liquidityManagement/liquidityPool/base/Suspendable.unit.t.sol`
- `fbd...11c ./test/liquidityManagement/liquidityPool/pool/Pool.unit.t.sol`
- `3b0...b1b ./test/liquidityManagement/liquidityPool/pool/pool.deposit.test.ts`
- `739...2f4 ./test/liquidityManagement/liquidityPool/utils/helpers.sol`
- `7c4...05d ./test/liquidityManagement/liquidityPool/libraries/DebtManage`

.unit.t.sol

- db8...7d9 ./test/liquidityManagement/liquidityPool/libraries/Queue.unit.t.sol
- 7a7...5ee ./test/liquidityManagement/liquidityPool/libraries/MerkleTreeRepository.unit.t.sol
- 9f9...eb1 ./test/liquidityManagement/liquidityPool/libraries/staking/RewardsMath.unit.t.sol
- ae5...562 ./test/liquidityManagement/liquidityPool/libraries/staking/RewardsMath.e2e.t.sol
- e7c...69a ./test/liquidityManagement/liquidityPool/libraries/staking/PositionManager.unit.t.sol
- f23...70d ./test/liquidityManagement/insuranceFund/FundFactory.unit.t.sol
- 47f...c0e ./test/liquidityManagement/insuranceFund/Fund.unit.t.sol
- a14...e68 ./test/liquidityManagement/insuranceFund/libraries/MoneyAccountant.unit.t.sol

Toolset

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

Setup

Tool Setup:

- Slither v0.8.3

Steps taken to run the tools:

1. Install the Slither tool: `pip3 install slither-analyzer`
2. Run Slither from the project directory: `slither .`

Automated Analysis

Slither

All relevant findings have been included in the main section of the report.

Test Suite Results

The forge tests were gathered by running `forge test` . The hardhat results were gathered by running `pnpm hh test` .

```
// FORGE TESTS
Running 1 test for
test/base/auth/AccessControlDS.unit.t.sol:AccessControlDSTe
st
[PASS] test_hasRole_defaultAdminRole() (gas: 25859)
Test result: ok. 1 passed; 0 failed; 0 skipped; finished in
3.09ms

Running 4 tests for
test/libraries/AddressRegistry.unit.t.sol:AddressRegistryTe
st
[PASS] test_cannotRegister_AddressAlreadyRegistered() (gas:
27692)
[PASS] test_cannotRetrieve_AddressIsNotRegisteredUnderKey()
(gas: 6680)
[PASS] test_isRegistered() (gas: 23850)
[PASS] test_register() (gas: 23875)
Test result: ok. 4 passed; 0 failed; 0 skipped; finished in
3.27ms

Running 4 tests for
test/liquidityManagement/liquidityPool/libraries/staking/Po
sitionManager.unit.t.sol:PositionManagerTest
[PASS]
test_decreasePosition_mustNotChangeTestPositionRewardMissed
() (gas: 86484)
[PASS] test_decreasePosition_mustSetUserBalanceToZero()
(gas: 86558)
[PASS]
test_increasePosition_mustSetTotalPositionsValueToAmountToI
ncrease() (gas: 104825)
[PASS]
test_increasePosition_mustSetUserBalanceToAmountToIncrease(
) (gas: 104941)
Test result: ok. 4 passed; 0 failed; 0 skipped; finished in
321.96µs
```

```
Running 5 tests for
test/accountAbstraction/compliance/approve/ApproveValidator
.unit.t.sol:ApproveValidatorTest
[PASS]
test_whenOperatorNotSupported_OperatorIsNotSupported()
(gas: 31613)
[PASS] test_whenTokenNotSupported_TokenIsNotSupported()
(gas: 21524)
[PASS] test_whenTokenSupported_andOperatorIsSupported()
(gas: 37373)
[PASS] test_whenTokenSupported_andOperatorIsSuspended()
(gas: 37351)
[PASS] test_whenTokenSuspended_andOperatorIsSupported()
(gas: 37395)
Test result: ok. 5 passed; 0 failed; 0 skipped; finished in
4.38ms

Running 13 tests for
test/accountAbstraction/compliance/libraries/ProtocolsRepos
itory.unit.t.sol:ProtocolsRepositoryTest
[PASS]
test_enforceProtocolSupportedOrSuspended_whenSupported()
(gas: 25802)
[PASS]
test_enforceProtocolSupportedOrSuspended_whenSuspended()
(gas: 27211)
[PASS]
test_enforceProtocolSupportedOrSuspended_whenUndefined()
(gas: 9088)
[PASS] test_enforceProtocolSupported_whenSupported() (gas:
25777)
[PASS] test_enforceProtocolSupported_whenSuspended() (gas:
31947)
[PASS] test_enforceProtocolSupported_whenUndefined() (gas:
9163)
[PASS] test_getProtocolEvaluator() (gas: 62412)
[PASS] test_getProtocolEvaluator_whenEvaluatorUpdated()
(gas: 65525)
[PASS]
test_updateOperatorSupport_mustReturnCorrectStorageUpdatedF
lag_protocol() (gas: 52412)
[PASS]
test_updateOperatorSupport_mustReturnCorrectStorageUpdatedF
lag_status() (gas: 51181)
[PASS]
test_updateProtocolSupport_mustCorrectlySwitchStatuses()
(gas: 64608)
```

```
[PASS]
test_updateProtocolSupport_mustReturnCorrectStorageUpdatedF
lag_evaluator() (gas: 52912)
[PASS]
test_updateProtocolSupport_mustReturnCorrectStorageUpdatedF
lag_status() (gas: 52032)
Test result: ok. 13 passed; 0 failed; 0 skipped; finished
in 879.29µs

Running 8 tests for
test/liquidityManagement/liquidityPool/libraries/Queue.unit
.t.sol:QueueTest
[PASS] test_cannotDequeue_QueueIsEmpty() (gas: 8240)
[PASS] test_dequeue_mustReturnDebt() (gas: 91499)
[PASS] test_dequeue_mustReturnFirstDebt() (gas: 135867)
[PASS] test_enqueue_mustSetDebtQueueLengthToOne() (gas:
69641)
[PASS] test_getLength_mustReturnOne() (gas: 69433)
[PASS] test_isEmpty_mustReturnFalse() (gas: 69503)
[PASS] test_isEmpty_mustReturnTrue() (gas: 4714)
[PASS] test_peek_mustReturnFirstDebt() (gas: 115218)
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
289.04µs

Running 10 tests for
test/accountAbstraction/marginAccount/AccountFactory.unit.t
.sol:AccountFactoryTest
[PASS]
test_borrowAccount_mustDeployNewAccount_whenPoolEmpty()
(gas: 412192)
[PASS]
test_borrowAccount_mustNotDeployNewAccount_whenPoolNotEmpty
() (gas: 423144)
[PASS] test_cannotBorrowAccount_missingRole() (gas: 13938)
[PASS]
test_cannotDeployMarginAccounts_UnauthorizedAccount() (gas:
12245)
[PASS] test_cannotReturnAccount_missingRole() (gas: 14340)
[PASS] test_cannotUpgradeTo_AlreadyUpToDate() (gas: 15759)
[PASS] test_cannotUpgradeTo_UnauthorizedAccount() (gas:
12279)
[PASS] test_deployMarginAccounts_when0Passed() (gas: 15329)
[PASS] test_deployMarginAccounts_when1Passed() (gas:
456137)
[PASS] test_returnAccount_mustReuseAccount() (gas: 418543)
Test result: ok. 10 passed; 0 failed; 0 skipped; finished
in 5.85ms
```

```
Running 10 tests for
test/libraries/Asset.unit.t.sol:AssetTest
[PASS] test_cannotForwardERC20_AmountMustNotBeZero() (gas:
10651)
[PASS] test_cannotForwardETH_AmountMustNotBeZero() (gas:
8292)
[PASS] test_enforceReceivedERC20_AmountMustNotBeZero()
(gas: 12550)
[PASS] test_enforceReceivedERC20_NotEnoughReceived() (gas:
54149)
[PASS] test_enforceReceivedERC20_NotEnoughReceived_0()
(gas: 19597)
[PASS] test_enforceReceivedETH_AmountMustNotBeZero() (gas:
10234)
[PASS] test_enforceReceivedETH_NotEnoughReceived() (gas:
20923)
[PASS] test_enforceReceivedETH_NotEnoughReceived_0() (gas:
11493)
[PASS] test_forwardERC20() (gas: 47849)
[PASS] test_forwardETH() (gas: 17454)
Test result: ok. 10 passed; 0 failed; 0 skipped; finished
in 1.43ms

Running 18 tests for
test/accountAbstraction/compliance/AbstractValidator.unit.t
.sol:AbstractValidatorTest
[PASS]
test_enforceOperatorSupportedOrSuspended_whenProtocolIsSusp
ended_andOperatorIsNotSuspended() (gas: 49681)
[PASS]
test_enforceOperatorSupportedOrSuspended_whenProtocolIsSusp
ended_andOperatorIsSuspended() (gas: 50832)
[PASS]
test_enforceOperatorSupportedOrSuspended_whenProtocolSuppor
ted_andOperatorNotSuspended() (gas: 58369)
[PASS]
test_enforceOperatorSupportedOrSuspended_whenProtocolSuppor
ted_andOperatorSuspended() (gas: 49371)
[PASS]
test_enforceOperatorSupported_whenProtocolIsSuspended_andOp
eratorIsNotSuspended() (gas: 55800)
[PASS]
test_enforceOperatorSupported_whenProtocolIsSuspended_andOp
eratorIsSuspended() (gas: 57017)
[PASS]
test_enforceOperatorSupported_whenProtocolSupported_andOper
```

```
atorNotSuspended() (gas: 59758)
[PASS]
test_enforceOperatorSupported_whenProtocolSupported_andOper
atorSuspended() (gas: 54685)
[PASS]
test_enforceOperatorSupported_whenProtocolUndefined() (gas:
10356)
[PASS]
test_getOperator_SupportNotRequired_whenProtocolIsSuspended
_andOperatorIsNotSuspended() (gas: 52540)
[PASS]
test_getOperator_SupportNotRequired_whenProtocolIsSuspended
_andOperatorIsSuspended() (gas: 53733)
[PASS]
test_getOperator_SupportNotRequired_whenProtocolSupported_a
ndOperatorNotSuspended() (gas: 63838)
[PASS]
test_getOperator_SupportNotRequired_whenProtocolSupported_a
ndOperatorSuspended() (gas: 52231)
[PASS]
test_getOperator_SupportRequired_whenProtocolIsSuspended_an
dOperatorIsNotSuspended() (gas: 58417)
[PASS]
test_getOperator_SupportRequired_whenProtocolIsSuspended_an
dOperatorIsSuspended() (gas: 59590)
[PASS]
test_getOperator_SupportRequired_whenProtocolSupported_andO
peratorNotSuspended() (gas: 65308)
[PASS]
test_getOperator_SupportRequired_whenProtocolSupported_andO
peratorSuspended() (gas: 57267)
[PASS]
test_getOperator_SupportRequired_whenProtocolUndefined()
(gas: 13017)
Test result: ok. 18 passed; 0 failed; 0 skipped; finished
in 6.39ms

Running 15 tests for
test/accountAbstraction/interpreter/LiquidityPoolsControlle
r.unit.t.sol:LiquidityPoolsControllerTest
[PASS] test_cannotGetPoolId_ProtocolIsNotSupported() (gas:
10146)
[PASS] test_cannotGetPoolId_whenEvaluatorAddressWrong()
(gas: 13513)
[PASS] test_cannotGetPoolStatus_ProtocolIsNotSupported()
(gas: 9724)
[PASS] test_cannotGetPoolStatus_whenEvaluatorAddressWrong()
```

```
(gas: 12793)
[PASS] test_cannotSetModules_AlreadyUpToDate() (gas: 15187)
[PASS] test_cannotSetModules_UnauthorizedAccount() (gas:
8444)
[PASS] test_cannotUpdatePoolsSupport_AlreadyUpToDate()
(gas: 20096)
[PASS]
test_cannotUpdatePoolsSupport_ProtocolIsNotSupported()
(gas: 13607)
[PASS] test_cannotUpdatePoolsSupport_ProtocolIsSuspended()
(gas: 13627)
[PASS] test_cannotUpdatePoolsSupport_UnauthorizedAccount()
(gas: 9575)
[PASS]
test_cannotUpdatePoolsSupport_whenEvaluatorAddressWrong()
(gas: 17468)
[PASS] test_getPoolId_whenProtocolSupported() (gas: 20651)
[PASS] test_getPoolId_whenProtocolSuspended() (gas: 20606)
[PASS] test_getPoolStatus_whenProtocolSupported() (gas:
51918)
[PASS] test_getPoolStatus_whenProtocolSuspended() (gas:
51895)
Test result: ok. 15 passed; 0 failed; 0 skipped; finished
in 6.69ms

Running 5 tests for
test/base/auth/OwnableAssignable.unit.t.sol:OwnableAssignab
leTest
[PASS] test_assignOwner() (gas: 28833)
[PASS] test_assignOwner_previousOwnerExists() (gas: 30796)
[PASS]
test_cannotAssignOwner_NewOwnerMustBeNonZeroAddress() (gas:
3308)
[PASS] test_cannotUnassignOwner_OwnerDoesNotExist() (gas:
5504)
[PASS] test_unassignOwner() (gas: 19580)
Test result: ok. 5 passed; 0 failed; 0 skipped; finished in
197.83µs

Running 4 tests for
test/liquidityManagement/liquidityPool/libraries/MerkleTree
Repository.unit.t.sol:MerkleTreeRepositoryTest
[PASS] test_setRoot_mustSetRootToNewRootHash() (gas: 25695)
[PASS] test_verify_mustReturnFalse_whenProofInvalid() (gas:
26962)
[PASS] test_verify_mustReturnTrue_whenProofValid() (gas:
26951)
```

```
[PASS] test_verify_mustSkipVerificationIfSpecialRootIsSet()
(gas: 25187)
Test result: ok. 4 passed; 0 failed; 0 skipped; finished in
222.50µs

Running 5 tests for
test/base/proxy/BeaconDS.unit.t.sol:BeaconDSTest
[PASS]
test_cannotGetImplementation_ImplementationAddressIsZero()
(gas: 8619)
[PASS] test_cannotUpgradeTo_AlreadyUpToDate() (gas: 33382)
[PASS] test_cannotUpgradeTo_ImplementationAddressIsZero()
(gas: 9618)
[PASS] test_cannotUpgradeTo_UnauthorizedAccount() (gas:
9995)
[PASS] test_upgradeTo_mustSetImplementation() (gas: 32454)
Test result: ok. 5 passed; 0 failed; 0 skipped; finished in
250.79µs

Running 8 tests for
test/libraries/CalldataLibrary.unit.t.sol:CalldataLibraryTe
st
[PASS] test_appendWord_whenEmptyDataPassed() (gas: 11197)
[PASS] test_appendWord_whenMaliciousMsgDataPassed() (gas:
20614)
[PASS] test_appendWord_whenMsgDataPassed() (gas: 12638)
[PASS] test_appendWord_whenNonEmptyDataPassed() (gas:
19619)
[PASS] test_extractLastWord_maliciousMsgData() (gas: 8307)
[PASS] test_extractLastWord_whenEmptyDataPassed() (gas:
6685)
[PASS] test_extractLastWord_whenMsgDataPassed() (gas: 7214)
[PASS] test_extractLastWord_whenNonEmptyDataPassed() (gas:
7745)
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
625.79µs

Running 3 tests for
test/base/auth/OwnableReadonly.unit.t.sol:OwnableReadonlyTe
st
[PASS] test_callConsumer() (gas: 22716)
[PASS]
test_cannotCallConsumer_CallerIsNotOwner_ownerNotSet()
(gas: 6458)
[PASS] test_cannotCallConsumer_CallerIsNotOwner_ownerSet()
(gas: 26581)
Test result: ok. 3 passed; 0 failed; 0 skipped; finished in
```

```
134.29µs

Running 2 tests for
test/liquidityManagement/liquidityPool/MerkleTreeWhitelist.
unit.t.sol:MerkleTreeWhitelistTest
[PASS] test_cannotSetRoot_UnauthorizedAccount() (gas: 7457)
[PASS] test_setRoot() (gas: 29747)
Test result: ok. 2 passed; 0 failed; 0 skipped; finished in
142.08µs

Running 2 tests for
test/base/auth/OwnableReadonlyDS.unit.t.sol:OwnableReadonly
DSTest
[PASS] test_callConsumer() (gas: 22842)
[PASS] test_cannotCallConsumer_CallerIsNotOwner() (gas:
26773)
Test result: ok. 2 passed; 0 failed; 0 skipped; finished in
109.54µs

Running 3 tests for
test/accountAbstraction/marginAccount/base/CommandSafeExecu
tor&AbstractValidator.integration.t.sol:CommandSafeExecutor
Test
[PASS] testFail_cannotValidateAndExecute() (gas: 14281)
[PASS] test_validateAndExecute() (gas: 39342)
[PASS] test_validateAndExecute_whenEmptyPayloadPassed()
(gas: 39560)
Test result: ok. 3 passed; 0 failed; 0 skipped; finished in
612.17µs

Running 3 tests for
test/liquidityManagement/liquidityPool/libraries/staking/Re
wardsMath.e2e.t.sol:RewardsMathTest
[PASS] test_E2E_scenarioOne() (gas: 366199)
[PASS] test_E2E_scenarioThree() (gas: 305984)
[PASS] test_E2E_scenarioTwo() (gas: 439683)
Test result: ok. 3 passed; 0 failed; 0 skipped; finished in
2.96ms

Running 6 tests for
test/marginEngine/libraries/Package&Envelope&Script.integra
tion.t.sol:PackageTest
[PASS] testFail_run_mustNotCallOnComplete_whenActionFails()
(gas: 53030)
[PASS] test_cannotRun_CrossChainActionIsForbidden() (gas:
14335)
[PASS]
```

```
test_run_mustCallAllEnvelopesInOnComplete_whenEvenFirstFail
s() (gas: 137929)
[PASS] test_run_mustReturnNumberOfFailures_whenCallback()
(gas: 137864)
[PASS] test_run_mustReturnNumberOfFailures_whenNoCallback()
(gas: 99090)
[PASS] test_run_mustRunOnComplete_whenActionSucceeds()
(gas: 106026)
Test result: ok. 6 passed; 0 failed; 0 skipped; finished in
2.32ms

Running 12 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rPlainPoolAddLiquidity.unit.t.sol:CurveFiValidatorPlainPool
AddLiquidityUnitTest
[PASS] test_add_liquidity_0x029b2f34() (gas: 83480)
[PASS] test_add_liquidity_0x029b2f34_withEth() (gas: 86809)
[PASS] test_add_liquidity_0x0b4c7e4d() (gas: 55340)
[PASS] test_add_liquidity_0x0b4c7e4d_withEth() (gas: 58625)
[PASS] test_add_liquidity_0x4515cef3() (gas: 69487)
[PASS] test_add_liquidity_0x4515cef3_withEth() (gas: 72772)
[PASS]
test_cannot_add_liquidity_0x029b2f34_OperatorIsNotSupported
_whenOperatorNotSupported() (gas: 39145)
[PASS]
test_cannot_add_liquidity_0x029b2f34_OperatorIsNotSupported
_whenOperatorSuspended() (gas: 35738)
[PASS]
test_cannot_add_liquidity_0x0b4c7e4d_OperatorIsNotSupported
_whenOperatorNotSupported() (gas: 34245)
[PASS]
test_cannot_add_liquidity_0x0b4c7e4d_OperatorIsNotSupported
_whenOperatorSuspended() (gas: 30948)
[PASS]
test_cannot_add_liquidity_0x4515cef3_OperatorIsNotSupported
_whenOperatorNotSupported() (gas: 36705)
[PASS]
test_cannot_add_liquidity_0x4515cef3_OperatorIsNotSupported
_whenOperatorSuspended() (gas: 33344)
Test result: ok. 12 passed; 0 failed; 0 skipped; finished
in 2.09ms

Running 8 tests for
test/liquidityManagement/liquidityPool/libraries/staking/Re
wardsMath.unit.t.sol:RewardsMathTest
[PASS] test_cannotIncreaseInterest_TokenVolumeIsZero()
(gas: 109808)
```

```
[PASS]
test_getUserRewards_mustReturnAlicesRewardsEqualToTwoThirdO
fAmountToDistribute() (gas: 244746)
[PASS]
test_getUserRewards_mustReturnUserRewardsEqualToAmountToDis
tribute() (gas: 181401)
[PASS] test_increaseInterest_mustSetTpssToNewTpss() (gas:
176081)
[PASS]
test_updateUserRewards_mustSetAccumulatedRewardsToAmountToD
istributeDividedByThree() (gas: 323391)
[PASS] test_updateUserRewards_mustSetIncompleteEpoch()
(gas: 105362)
[PASS]
test_updateUserRewards_mustSetNewIncompleteEpochOnSecondDep
osit() (gas: 211359)
[PASS] test_updateUserRewards_mustUpdateIncompleteEpoch()
(gas: 117030)
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
2.22ms

Running 24 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rPlainPoolExchange.unit.t.sol:CurveFiValidatorPlainPoolExch
angeUnitTest
[PASS]
test_cannot_exchange_0x353ca424_whenTokenOutNotSupported()
(gas: 30418)
[PASS]
test_cannot_exchange_0x353ca424_whenTokenOutSuspended()
(gas: 30382)
[PASS]
test_cannot_exchange_0x394747c5_whenTokenInNotSupportedNorS
uspended() (gas: 26322)
[PASS]
test_cannot_exchange_0x394747c5_whenTokenOutNotSupported()
(gas: 30378)
[PASS]
test_cannot_exchange_0x394747c5_whenTokenOutSuspended()
(gas: 30385)
[PASS]
test_cannot_exchange_0x3df02124_OperatorIsNotSupported()
(gas: 29793)
[PASS]
test_cannot_exchange_0x3df02124_whenTokenInNotSupportedNorS
uspended() (gas: 26294)
[PASS]
```

```
test_cannot_exchange_0xce7d6503_whenTokenInNotSupportedNorS
uspended() (gas: 26752)
[PASS]
test_cannot_exchange_0xce7d6503_whenTokenOutNotSupported()
(gas: 30719)
[PASS]
test_cannot_exchange_0xce7d6503_whenTokenOutSuspended()
(gas: 30771)
[PASS] test_exchange_0x394747c5_OperatorIsNotSupported()
(gas: 30023)
[PASS] test_exchange_0x394747c5_whenOperatorSuspended()
(gas: 67332)
[PASS] test_exchange_0x394747c5_whenTokenInSupported()
(gas: 61442)
[PASS] test_exchange_0x394747c5_whenTokenInSuspended()
(gas: 61487)
[PASS] test_exchange_0x394747c5_withEth() (gas: 61336)
[PASS] test_exchange_0x3df02124_whenOperatorSuspended()
(gas: 60502)
[PASS] test_exchange_0x3df02124_whenTokenInSupported()
(gas: 54635)
[PASS] test_exchange_0x3df02124_whenTokenInSuspended()
(gas: 54615)
[PASS] test_exchange_0x3df02124_withEth() (gas: 54508)
[PASS] test_exchange_0xce7d6503_OperatorIsNotSupported()
(gas: 30409)
[PASS] test_exchange_0xce7d6503_whenOperatorSuspended()
(gas: 75367)
[PASS] test_exchange_0xce7d6503_whenTokenInSupported()
(gas: 69390)
[PASS] test_exchange_0xce7d6503_whenTokenInSuspended()
(gas: 69412)
[PASS] test_exchange_0xce7d6503_withETH() (gas: 68773)
Test result: ok. 24 passed; 0 failed; 0 skipped; finished
in 13.01ms

Running 8 tests for
test/libraries/SafeCall.unit.t.sol:SafeCallTest
[PASS] test_safeCallAll() (gas: 20953)
[PASS] test_safeCallAll_revertOneShouldRevertTx() (gas:
21173)
[PASS] test_safeCall_noValue() (gas: 11319)
[PASS] test_safeCall_noValue_revert() (gas: 14648)
[PASS] test_safeCall_withValue() (gas: 17973)
[PASS] test_safeCall_withValue_revert() (gas: 21345)
[PASS] test_safeDelegateCall() (gas: 30290)
[PASS] test_safeDelegateCall_revert() (gas: 13857)
```

```
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
553.58µs

Running 18 tests for
test/base/Address.unit.t.sol:AddressTest
[PASS] testFuzz_isEth_false(address) (runs: 256, µ: 4224,
~: 4224)
[PASS] test_isEth_address0() (gas: 386)
[PASS] test_isEth_addressE() (gas: 365)
[PASS] test_set_get_slot0() (gas: 22931)
[PASS] test_set_get_slot1() (gas: 22930)
[PASS] test_set_get_slotKeccak256() (gas: 22612)
[PASS] test_sort_0_1() (gas: 469)
[PASS] test_sort_0_1_2_3() (gas: 2493)
[PASS] test_sort_0_1_3_2() (gas: 2523)
[PASS] test_sort_0_3_1_2() (gas: 2510)
[PASS] test_sort_1_0() (gas: 481)
[PASS] test_sort_1_1() (gas: 458)
[PASS] test_sort_1_1_2_2() (gas: 2512)
[PASS] test_sort_2_1_3_0() (gas: 2574)
[PASS] test_sort_2_3_0_1() (gas: 2534)
[PASS] test_sort_3_2_1_0() (gas: 2532)
[PASS] test_sort_3_3_3_2() (gas: 2607)
[PASS] test_sort_3_3_3_3() (gas: 2542)
Test result: ok. 18 passed; 0 failed; 0 skipped; finished
in 13.93ms

Running 5 tests for
test/marginEngine/base/SignatureProcessor&Nonce.integration
.t.sol:SignatureProcessorTest
[PASS] test_cannotProcessSignature_InvalidSignature() (gas:
26618)
[PASS] test_cannotProcessSignature_NonceAlreadyUsed() (gas:
42353)
[PASS] test_cannotProcessSignature_SignatureExpired() (gas:
18887)
[PASS] test_cannotProcessSignature_SignerIsNotAllowed()
(gas: 33288)
[PASS] test_processSignature_mustUseNonce() (gas: 52945)
Test result: ok. 5 passed; 0 failed; 0 skipped; finished in
5.50ms

Running 8 tests for
test/marginEngine/base/ThresholdsVerifier.unit.t.sol:Thresh
oldsVerifierTest
[PASS]
test_cannotVefiryThresholds_TokenLevelInsufficient_leverage
```

```
() (gas: 28984)
[PASS]
test_cannotVerifyThresholds_AmountMustNotBeZero_collateral0
() (gas: 35126)
[PASS]
test_cannotVerifyThresholds_AmountMustNotBeZero_collateral1
() (gas: 37422)
[PASS]
test_cannotVerifyThresholds_AmountMustNotBeZero_leverage()
(gas: 27860)
[PASS] test_cannotVerifyThresholds_RiskFactorIsTooLow()
(gas: 23258)
[PASS]
test_cannotVerifyThresholds_TokenLevelInsufficient_collater
al0() (gas: 40967)
[PASS]
test_cannotVerifyThresholds_TokenLevelInsufficient_collater
al1() (gas: 45351)
[PASS] test_verifyThresholds() (gas: 34904)
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
2.05ms

Running 34 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rPlainPoolRemoveLiquidity.unit.t.sol:CurveFiValidatorPlainP
oolAddLiquidityUnitTest
[PASS]
test_cannot_remove_liquidity_0x5b36389c_OperatorIsNotSuppor
ted() (gas: 30149)
[PASS]
test_cannot_remove_liquidity_0x7d49d875_OperatorIsNotSuppor
ted() (gas: 31024)
[PASS]
test_cannot_remove_liquidity_0xecb586a5_OperatorIsNotSuppor
ted() (gas: 30553)
[PASS]
test_cannot_remove_liquidity_imbalance_0x18a7bd76_OperatorI
sNotSupported() (gas: 31003)
[PASS]
test_cannot_remove_liquidity_imbalance_0x9fdaea0c_OperatorI
sNotSupported() (gas: 30510)
[PASS]
test_cannot_remove_liquidity_imbalance_0xe3103273_OperatorI
sNotSupported() (gas: 30060)
[PASS]
test_cannot_remove_liquidity_one_coin_0x1a4d01d2_OperatorIs
NotSupported() (gas: 29550)
```

```
[PASS]
test_cannot_remove_liquidity_one_coin_0x1a4d01d2_TokenIsNot
Supported() (gas: 26061)
[PASS]
test_cannot_remove_liquidity_one_coin_0xf1dc3cc9_OperatorIs
NotSupported() (gas: 29485)
[PASS]
test_cannot_remove_liquidity_one_coin_0xf1dc3cc9_TokenIsNot
Supported() (gas: 25839)
[PASS]
test_remove_liquidity_0x5b36389c_whenOperatorSuspended()
(gas: 52305)
[PASS]
test_remove_liquidity_0x5b36389c_whenTokenSuspended() (gas:
50878)
[PASS]
test_remove_liquidity_0x5b36389c_whenTokensSupported()
(gas: 46395)
[PASS]
test_remove_liquidity_0x7d49d875_whenOperatorSuspended()
(gas: 71659)
[PASS]
test_remove_liquidity_0x7d49d875_whenTokenSuspended() (gas:
69974)
[PASS]
test_remove_liquidity_0x7d49d875_whenTokensSupported()
(gas: 65425)
[PASS]
test_remove_liquidity_0xecb586a5_whenOperatorSuspended()
(gas: 61977)
[PASS]
test_remove_liquidity_0xecb586a5_whenTokenSuspended() (gas:
60443)
[PASS]
test_remove_liquidity_0xecb586a5_whenTokensSupported()
(gas: 55937)
[PASS]
test_remove_liquidity_imbalance_0x18a7bd76_whenOperatorSusp
ended() (gas: 71912)
[PASS]
test_remove_liquidity_imbalance_0x18a7bd76_whenTokenSupport
ed() (gas: 65746)
[PASS]
test_remove_liquidity_imbalance_0x18a7bd76_whenTokenSuspend
ed() (gas: 70185)
[PASS]
test_remove_liquidity_imbalance_0x9fdaea0c_whenOperatorSusp
```

```
ended() (gas: 62166)
[PASS]
test_remove_liquidity_imbalance_0x9fdaea0c_whenTokenSupport
ed() (gas: 56039)
[PASS]
test_remove_liquidity_imbalance_0x9fdaea0c_whenTokenSuspend
ed() (gas: 60611)
[PASS]
test_remove_liquidity_imbalance_0xe3103273_whenOperatorSusp
ended() (gas: 52386)
[PASS]
test_remove_liquidity_imbalance_0xe3103273_whenTokenSuspend
ed() (gas: 50982)
[PASS]
test_remove_liquidity_imbalance_0xe3103273_whenTokensSuppor
ted() (gas: 46453)
[PASS]
test_remove_liquidity_one_coin_0x1a4d01d2_whenOperatorSuspe
nded() (gas: 48966)
[PASS]
test_remove_liquidity_one_coin_0x1a4d01d2_whenTokenSupporte
d() (gas: 43272)
[PASS]
test_remove_liquidity_one_coin_0x1a4d01d2_whenTokenSuspende
d() (gas: 43373)
[PASS]
test_remove_liquidity_one_coin_0xf1dc3cc9_whenOperatorSuspe
nded() (gas: 48814)
[PASS]
test_remove_liquidity_one_coin_0xf1dc3cc9_whenTokenSupporte
d() (gas: 43074)
[PASS]
test_remove_liquidity_one_coin_0xf1dc3cc9_whenTokenSuspende
d() (gas: 43153)
Test result: ok. 34 passed; 0 failed; 0 skipped; finished
in 5.56ms

Running 38 tests for
test/accountAbstraction/marginAccount/Account&StateMachine.
integration.t.sol:AccountTest
[PASS] test_allocationInfo() (gas: 222056)
[PASS] test_cannotClose_ArrayMustNotBeEmpty() (gas: 239082)
[PASS] test_cannotClose_whenStateIsClosed() (gas: 296622)
[PASS] test_cannotClose_whenStateIsRegistered() (gas:
225466)
[PASS] test_cannotClose_whenStateUndefined() (gas: 14014)
[PASS] test_cannotExecute_UnauthorizedAccount() (gas:
```

```
239877)
[PASS] test_cannotExecute_whenStateIsClosed() (gas: 297273)
[PASS] test_cannotExecute_whenStateIsRegistered() (gas:
226356)
[PASS] test_cannotExecute_whenStateIsSuspended() (gas:
338047)
[PASS] test_cannotExecute_whenStateUndefined() (gas: 16798)
[PASS] test_cannotExecute_whenValidatorThrowError() (gas:
247829)
[PASS] test_cannotRegister_AmountMustNotBeZero() (gas:
22237)
[PASS] test_cannotRegister_NotEnoughReceived() (gas: 27152)
[PASS] test_cannotRegister_Unathorized() (gas: 13808)
[PASS] test_cannotRegister_whenStateIsOpened() (gas:
241784)
[PASS] test_cannotRegister_whenStateIsRegistered() (gas:
226310)
[PASS] test_cannotRegister_whenStateIsSuspended() (gas:
339473)
[PASS] test_cannotSupply_AmountMustNotBeZero() (gas:
224431)
[PASS] test_cannotSupply_whenStateIsClosed() (gas: 296300)
[PASS] test_cannotSupply_whenStateIsOpened() (gas: 240558)
[PASS] test_cannotSupply_whenStateIsSuspended() (gas:
336453)
[PASS] test_cannotSupply_whenStateUndefined() (gas: 13591)
[PASS] test_close_mustCallTargetOfScript() (gas: 293955)
[PASS] test_close_mustDeleteOwner_and_mustDeleteLeverage()
(gas: 293555)
[PASS]
test_close_mustEmitAccountClosed_whenScriptSucceeded()
(gas: 370030)
[PASS] test_close_mustEmitAccountSuspended() (gas: 334069)
[PASS]
test_execute_mustCallValidationHub_and_mustCallTargetOfOper
ation() (gas: 255093)
[PASS] test_execute_mustDontChangeAccountOwner() (gas:
254967)
[PASS] test_register_mustCallBalanceOfOnCollateralToken()
(gas: 224268)
[PASS] test_register_mustEmitAccountRegistered() (gas:
226423)
[PASS] test_register_mustSetOwnerAndLeverage() (gas:
221651)
[PASS] test_stateInfo() (gas: 220399)
[PASS]
test_supply_mustEmitLeverageSupplied_and_mustEmitAccountOpe
```

```
ned_whenAllLeverageSupplied() (gas: 242171)
[PASS]
test_supply_mustEmitLeverageSupplied_whenNotAllLeverageSupp
lied() (gas: 252330)
[PASS]
test_supply_mustNotSetStateToOpened_whenNotAllLeverageSuppl
ied() (gas: 253760)
[PASS]
test_supply_mustSetStateToOpened_whenAllLeverageSupplied()
(gas: 240575)
[PASS]
test_supply_mustSetStateToSuspended_whenTooMuchLeverageSupp
lied() (gas: 242216)
[PASS]
test_supply_mustSetStateToSuspened_whenSupplyLimitExceeded(
) (gas: 240965)
Test result: ok. 38 passed; 0 failed; 0 skipped; finished
in 16.24ms

Running 6 tests for
test/liquidityManagement/liquidityPool/base/Suspendable.uni
t.t.sol:SuspendableTest
[PASS] test_cannotSuspend_missingRole() (gas: 8121)
[PASS] test_cannotSuspend_whenIsSuspended() (gas: 31553)
[PASS] test_cannotSuspend_whenNotIsSuspended() (gas: 8580)
[PASS] test_cannotUnsuspend_missingRole() (gas: 8120)
[PASS] test_suspend_mustSetIsSuspendedToTrue() (gas: 32351)
[PASS] test_unsuspend_mustSetIsSuspendedToFalse() (gas:
24044)
Test result: ok. 6 passed; 0 failed; 0 skipped; finished in
318.67µs

Running 14 tests for
test/accountAbstraction/compliance/uniswapV3/UniswapV3Valid
atorLiquidity.unit.t.sol:UniswapV3ValidatorLiquidityUnitTes
t
[PASS] testFail_cannotIncreaseLiquidity_PoolIdNotFound()
(gas: 36060)
[PASS] testFail_cannotIncreaseLiquidity_PoolIsSuspended()
(gas: 35928)
[PASS] testFail_cannotMint_PoolIdNotFound() (gas: 28096)
[PASS] testFail_cannotMint_PoolIsSuspended() (gas: 27986)
[PASS] test_cannotCollect_OperatorIsNotSupported() (gas:
37462)
[PASS]
test_cannotDecreaseLiquidity_OperatorIsNotSupported() (gas:
40535)
```

```
[PASS]
test_cannotIncreaseLiquidity_OperatorIsNotSupported() (gas:
42953)
[PASS] test_cannotIncreaseLiquidity_OperatorIsSuspended()
(gas: 39614)
[PASS] test_cannotMint_OperatorIsNotSupported() (gas:
55051)
[PASS] test_cannotMint_OperatorIsSuspended() (gas: 51665)
[PASS] test_collect() (gas: 55283)
[PASS] test_decreaseLiquidity() (gas: 65134)
[PASS] test_increasePosition() (gas: 83770)
[PASS] test_mint() (gas: 124415)
Test result: ok. 14 passed; 0 failed; 0 skipped; finished
in 8.17ms

Running 12 tests for
test/accountAbstraction/interpreter/libraries/Path.unit.t.s
ol:PathTest
[PASS] testFuzz_ensureValid(uint8) (runs: 256, μ: 6880, ~:
7201)
[PASS] test_cannotEnsureValid_whenEmpty() (gas: 5752)
[PASS] test_cannotEnsureValid_whenNotEmpty() (gas: 6241)
[PASS] test_cannotExtractPool_InvalidPathLength() (gas:
6880)
[PASS] test_cannotExtractTokenIn_InvalidPathLength() (gas:
5983)
[PASS] test_cannotExtractTokenOut_InvalidPathLength() (gas:
6028)
[PASS] test_cannotGetNumberOfPools_InvalidPathLength()
(gas: 6042)
[PASS] test_ensureValid() (gas: 3909)
[PASS] test_extractPool() (gas: 15615)
[PASS] test_extractTokenIn() (gas: 3927)
[PASS] test_extractTokenOut() (gas: 4158)
[PASS] test_getNumberOfPools() (gas: 4915)
Test result: ok. 12 passed; 0 failed; 0 skipped; finished
in 12.78ms

Running 26 tests for
test/base/StateMachine.unit.t.sol:StateMachineTest
[PASS] test_DeleteTransition() (gas: 11379)
[PASS] test_cannotChangeState_InvalidState_0() (gas: 4571)
[PASS] test_cannotChangeState_InvalidState_notPowerOf2()
(gas: 4597)
[PASS] test_cannotChangeState_InvalidState_undefined()
(gas: 4531)
[PASS] test_cannotChangeState_TransitionDoesNotExist()
```

```
(gas: 11711)
[PASS]
test_cannotCreateStateFromId_IdIsReservedForUndefinedState(
) (gas: 4314)
[PASS]
test_cannotCreateTransitionToUndefined_InvalidState() (gas:
4775)
[PASS]
test_cannotCreateTransition_TransitionAlreadyExists() (gas:
8269)
[PASS] test_cannotDeleteTransition_InvalidState() (gas:
4837)
[PASS] test_cannotDeleteTransition_TransitionDoesNotExist()
(gas: 8264)
[PASS] test_changeState() (gas: 38092)
[PASS] test_changeState_mustCallCallback() (gas: 39667)
[PASS] test_changeState_mustCallDifferentCallbacks() (gas:
72527)
[PASS] test_createTransition() (gas: 65940)
[PASS] test_eq() (gas: 466)
[PASS] test_neq() (gas: 428)
[PASS] test_newStateFromId() (gas: 712)
[PASS]
test_onlyState_notRevert_bitmapHasManyStates_initialized()
(gas: 66846)
[PASS]
test_onlyState_notRevert_bitmapHasManyStates_notInitialized
() (gas: 34039)
[PASS]
test_onlyState_notRevert_bitmapHasOnlyOneState_initialized(
) (gas: 33491)
[PASS]
test_onlyState_notRevert_bitmapHasOnlyOneState_notInitializ
ed() (gas: 2596)
[PASS]
test_onlyState_revert_bitmapHasManyStates_initialized()
(gas: 38542)
[PASS]
test_onlyState_revert_bitmapHasManyStates_notInitialized()
(gas: 7703)
[PASS]
test_onlyState_revert_bitmapHasOnlyOneState_initialized()
(gas: 38392)
[PASS]
test_onlyState_revert_bitmapHasOnlyOneState_notInitialized(
) (gas: 7597)
[PASS] test_or() (gas: 356)
```

```
Test result: ok. 26 passed; 0 failed; 0 skipped; finished
in 6.53ms

Running 8 tests for
test/libraries/Nonce.unit.t.sol:NonceTest
[PASS] test_isUsed_whenNonZeroNonceIsNotUsed() (gas: 2556)
[PASS] test_isUsed_whenNonZeroNonceIsUsed() (gas: 23211)
[PASS] test_isUsed_whenZeroNonceIsNotUsed() (gas: 2622)
[PASS] test_isUsed_whenZeroNonceIsUsed() (gas: 23234)
[PASS] test_revertIfUsed_whenNonZeroNonceIsNotUsed() (gas:
2570)
[PASS] test_revertIfUsed_whenNonZeroNonceIsUsed() (gas:
27143)
[PASS] test_revertIfUsed_whenZeroNonceIsNotUsed() (gas:
2549)
[PASS] test_revertIfUsed_whenZeroNonceIsUsed() (gas: 27101)
Test result: ok. 8 passed; 0 failed; 0 skipped; finished in
248.75µs

Running 18 tests for
test/liquidityManagement/liquidityPool/pool/Pool.unit.t.sol
:PoolTest
[PASS] test_borrow() (gas: 189987)
[PASS] test_cannotBorrow_borrowAmountExceedsBalance() (gas:
16136)
[PASS] test_cannotBorrow_missingBorrowerRole() (gas: 8669)
[PASS] test_cannotClaim_NoPendingRewards() (gas: 75497)
[PASS] test_cannotDeposit_merkleTreeVerificationFailed()
(gas: 12529)
[PASS] test_cannotDeposit_thresholdOnTotalDepositExeeded()
(gas: 177203)
[PASS] test_cannotDeposit_whenSuspended() (gas: 32362)
[PASS] test_cannotReturnAndDistribute_missingRepayerRole()
(gas: 9053)
[PASS] test_cannotSetFund_alreadyUpToDate() (gas: 9485)
[PASS] test_cannotSetFund_missingDefaultAdminRole() (gas:
8672)
[PASS] test_cannotWithdraw_withdrawAmountExceedsBalance()
(gas: 8173)
[PASS] test_deposit() (gas: 171942)
[PASS] test_getToken_mustReturnTokenAddress() (gas: 3493)
[PASS] test_returnAndDistribute() (gas: 260349)
[PASS] test_setUp_mustInitializeAllVariables() (gas: 25237)
[PASS] test_withdraw_toZeroAddress() (gas: 159937)
[PASS] test_withdraw_whenInsufficientPoolBalance() (gas:
217463)
[PASS] test_withdraw_whenSufficientPoolBalance() (gas:
```

```
159952)
Test result: ok. 18 passed; 0 failed; 0 skipped; finished
in 4.69ms

Running 6 tests for
test/accountAbstraction/compliance/WhitelistingController.u
nit.t.sol:WhitelistingControllerTest
[PASS] test_cannotUpdateOperatorsSupport_AlreadyUpToDate()
(gas: 13400)
[PASS]
test_cannotUpdateOperatorsSupport_UnauthorizedAccount()
(gas: 9312)
[PASS] test_cannotUpdateProtocolSupport_AlreadyUpToDate()
(gas: 11815)
[PASS]
test_cannotUpdateProtocolSupport_UnauthorizedAccount()
(gas: 8634)
[PASS]
test_cannotUpdateTokensSupport_AlreadyUpToDateAndExpectEven
ts() (gas: 13248)
[PASS]
test_cannotUpdateTokensSupport_UnauthorizedAccountAndExpect
Events() (gas: 8801)
Test result: ok. 6 passed; 0 failed; 0 skipped; finished in
1.46ms

Running 21 tests for
test/accountAbstraction/interpreter/libraries/ScriptCompile
r.unit.t.sol:ScriptCompilerTest
[PASS] test_cannotcompileAt_InvalidSequenceAtIndex0() (gas:
32948)
[PASS] test_cannotcompileAt_InvalidSequenceAtIndexN() (gas:
32882)
[PASS] test_compileAt_doubleDPI() (gas: 45061)
[PASS] test_compileAt_doubleEAI() (gas: 46045)
[PASS] test_compileAt_doubleEI() (gas: 45574)
[PASS] test_compileAt_doubleIPI() (gas: 43798)
[PASS] test_compileAt_everyDouble_0_1_2_3_4_5_6_7() (gas:
280172)
[PASS] test_compileAt_everyDouble_3_5_1_7_0_4_2_6() (gas:
280085)
[PASS] test_compileAt_everyDouble_6_7_0_1_5_4_2_3() (gas:
280105)
[PASS] test_compileAt_everyDouble_7_6_5_4_3_2_1_0() (gas:
280149)
[PASS] test_compileAt_everySingle_0_1_2_3() (gas: 106239)
[PASS] test_compileAt_everySingle_2_0_3_1() (gas: 106260)
```

```
[PASS] test_compileAt_everySingle_3_2_1_0() (gas: 106282)
[PASS] test_compileAt_random_1_2_4_5_3_0() (gas: 185032)
[PASS] test_compileAt_random_2_0_1() (gas: 72695)
[PASS] test_compileAt_random_4_2_0_3_1() (gas: 143708)
[PASS] test_compileAt_random_6_3_0_1_2_4_5() (gas: 230582)
[PASS] test_compileAt_singleDPI() (gas: 20857)
[PASS] test_compileAt_singleEAI() (gas: 21293)
[PASS] test_compileAt_singleEI() (gas: 21006)
[PASS] test_compileAt_singleIPI() (gas: 20326)
Test result: ok. 21 passed; 0 failed; 0 skipped; finished
in 14.05ms

Running 2 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rZapperAddLiquidity.unit.t.sol:CurveFiValidatorPlainPoolAdd
LiquidityUnitTest
[PASS] test_add_liquidity() (gas: 76918)
[PASS] test_cannot_add_liquidity_OperatorIsNotSupported()
(gas: 39319)
Test result: ok. 2 passed; 0 failed; 0 skipped; finished in
740.50µs

Running 20 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rSwapRouter.unit.t.sol:CurveFiValidatorSwapRouterTest
[PASS]
test_cannot_exchange_multiple_0x0651cb35_whenOperatorNotSup
ported() (gas: 96776)
[PASS]
test_cannot_exchange_multiple_0x0651cb35_whenTokenInNotSupp
ortedNorSuspended() (gas: 95033)
[PASS]
test_cannot_exchange_multiple_0x0651cb35_whenTokenOutNotSup
ported() (gas: 98550)
[PASS]
test_cannot_exchange_multiple_0x353ca424_OperatorIsNotSuppo
rted() (gas: 85412)
[PASS]
test_cannot_exchange_multiple_0x353ca424_whenTokenInNotSupp
ortedNorSuspended() (gas: 83715)
[PASS]
test_cannot_exchange_multiple_0x353ca424_whenTokenOutNotSup
ported() (gas: 87189)
[PASS]
test_cannot_exchange_multiple_0x9db4f7aa_whenOperatorNotSup
ported() (gas: 96226)
[PASS]
```

```
test_cannot_exchange_multiple_0x9db4f7aa_whenTokenInNotSupp
ortedNorSuspended() (gas: 94421)
[PASS]
test_cannot_exchange_multiple_0x9db4f7aa_whenTokenOutNotSup
ported() (gas: 97849)
[PASS]
test_exchange_multiple_0x0651cb35_whenOperatorSuspended()
(gas: 311094)
[PASS]
test_exchange_multiple_0x0651cb35_whenTokenInSuspended()
(gas: 312678)
[PASS]
test_exchange_multiple_0x0651cb35_whenTokensSupported()
(gas: 307983)
[PASS]
test_exchange_multiple_0x353ca424_whenOperatorSuspended()
(gas: 253956)
[PASS]
test_exchange_multiple_0x353ca424_whenTokenInSuspended()
(gas: 255560)
[PASS]
test_exchange_multiple_0x353ca424_whenTokensSupported()
(gas: 250889)
[PASS] test_exchange_multiple_0x353ca424_withEth() (gas:
251971)
[PASS]
test_exchange_multiple_0x9db4f7aa_whenOperatorSuspended()
(gas: 294355)
[PASS]
test_exchange_multiple_0x9db4f7aa_whenTokenInSuspended()
(gas: 296006)
[PASS]
test_exchange_multiple_0x9db4f7aa_whenTokensSupported()
(gas: 291332)
[PASS] test_exchange_multiple_0x9db4f7aa_withEth() (gas:
292328)
Test result: ok. 20 passed; 0 failed; 0 skipped; finished
in 11.78ms

Running 24 tests for
test/accountAbstraction/interpreter/curveFi/CurveFiValidato
rZapperRemoveLiquidity.unit.t.sol:CurveFiValidatorZapperRem
oveLiquidityUnitTest
[PASS]
test_cannot_remove_liquidity_0xad5cc918_OperatorNotSupporte
d() (gas: 31198)
[PASS]
```

```
test_cannot_remove_liquidity_0xcbc399e5_OperatorNotSupporte
d() (gas: 31590)
[PASS]
test_cannot_remove_liquidity_imbalance_0x4329c8cc_OperatorN
otSupported() (gas: 32961)
[PASS]
test_cannot_remove_liquidity_imbalance_0xac24f771_OperatorN
otSupported() (gas: 32699)
[PASS]
test_cannot_remove_liquidity_one_coin_0x1e700cbb_whenOperat
orNotSupported() (gas: 30165)
[PASS]
test_cannot_remove_liquidity_one_coin_0x29ed2862_OperatorNo
tSupported() (gas: 29596)
[PASS] test_remove_liquidity_0xad5cc918() (gas: 64125)
[PASS]
test_remove_liquidity_0xad5cc918_whenOperatorSuspended()
(gas: 67147)
[PASS]
test_remove_liquidity_0xad5cc918_whenTokenSuspended() (gas:
70608)
[PASS] test_remove_liquidity_0xcbc399e5() (gas: 71974)
[PASS]
test_remove_liquidity_0xcbc399e5_whenOperatorSuspended()
(gas: 74997)
[PASS]
test_remove_liquidity_0xcbc399e5_whenTokenSuspended() (gas:
78526)
[PASS] test_remove_liquidity_imbalance_0x4329c8cc() (gas:
74593)
[PASS]
test_remove_liquidity_imbalance_0x4329c8cc_whenOperatorSusp
ended() (gas: 77641)
[PASS]
test_remove_liquidity_imbalance_0x4329c8cc_whenTokenSuspend
ed() (gas: 81037)
[PASS] test_remove_liquidity_imbalance_0xac24f771() (gas:
65585)
[PASS]
test_remove_liquidity_imbalance_0xac24f771_whenOperatorSusp
ended() (gas: 68563)
[PASS]
test_remove_liquidity_imbalance_0xac24f771_whenTokenSuspend
ed() (gas: 72069)
[PASS] test_remove_liquidity_one_coin_0x1e700cbb() (gas:
55892)
[PASS]
```

```
test_remove_liquidity_one_coin_0x1e700cbb_whenOperatorSuspe
nded() (gas: 59002)
[PASS]
test_remove_liquidity_one_coin_0x1e700cbb_whenTokenSuspende
d() (gas: 55979)
[PASS] test_remove_liquidity_one_coin_0x29ed2862() (gas:
48009)
[PASS]
test_remove_liquidity_one_coin_0x29ed2862_whenOperatorSuspe
nded() (gas: 51095)
[PASS]
test_remove_liquidity_one_coin_0x29ed2862_whenTokenSuspende
d() (gas: 48074)
Test result: ok. 24 passed; 0 failed; 0 skipped; finished
in 4.86ms

Running 16 tests for
test/liquidityManagement/liquidityPool/PoolFactory.unit.t.s
ol:PoolFactoryTest
[PASS] test_cannotCreatePool_UnauthorizedAccount() (gas:
8468)
[PASS] test_cannotGetPool_whenPoolDoesntExist() (gas: 7991)
[PASS] test_cannotIsSuspended_whenInvalidAddressProvided()
(gas: 7206)
[PASS] test_cannotSetFund() (gas: 432840)
[PASS] test_cannotSuspendPool_UnauthorizedAccount() (gas:
432431)
[PASS] test_cannotUnsuspendPool_unauthorizedAccount() (gas:
459446)
[PASS] test_cannotUpgradeTo_UnauthorizedAccount() (gas:
7556)
[PASS] test_cannotUpgradeTo_withZeroAddress() (gas: 7257)
[PASS] test_createPool() (gas: 442158)
[PASS] test_getImplementation() (gas: 5621)
[PASS]
test_isPoolExist_mustReturnFalse_whenPoolDoesNotExist()
(gas: 4177)
[PASS]
test_isSuspended_mustReturnTrue_whenPoolIsSuspended() (gas:
461401)
[PASS] test_setFund() (gas: 463902)
[PASS] test_suspendPool() (gas: 456584)
[PASS] test_unsuspendPool() (gas: 443627)
[PASS] test_upgradeTo() (gas: 13089)
Test result: ok. 16 passed; 0 failed; 0 skipped; finished
in 7.55ms
```

```
Running 14 tests for
test/marginEngine/Dispatcher&AccountFactory.integration.t.s
ol:AccountFactoryTest
[PASS]
test_cannotRegisterMarginAccount_whenErrorInSignatureProces
sing() (gas: 31252)
[PASS]
test_cannotRegisterMarginAccount_whenErrorInThresholdsVerif
ication() (gas: 55868)
[PASS] test_cannotSubmitPlan_AccountMissingRole() (gas:
14066)
[PASS] test_cannotSupplyMarginAccount_AccountMissingRole()
(gas: 18613)
[PASS]
test_cannotSupplyMarginAccount_InvalidLeverageSupplied()
(gas: 652038)
[PASS]
test_cannotTryCloseMarginAccount_AccountMissingRole() (gas:
16209)
[PASS]
test_cannotTryCloseMarginAccount_CrossChainActionIsForbidde
n() (gas: 15489)
[PASS]
test_registerMarginAccount_mustDeployMarginAccount_whenMarg
inAccountsPoolIsEmpty() (gas: 643790)
[PASS]
test_registerMarginAccount_mustEmitTransferOnCollateralToke
n() (gas: 646764)
[PASS]
test_registerMarginAccount_mustReturnAddressOfMarginAccount
() (gas: 643642)
[PASS] test_submitPlan_mustCallPackageTarget() (gas: 52016)
[PASS]
test_supplyMarginAccount_mustEmitTransferOnLeverageToken()
(gas: 749089)
[PASS]
test_tryCloseMarginAccount_mustCallLiquidationPlanTarget()
(gas: 747709)
[PASS]
test_tryCloseMarginAccount_mustReturnFalse_whenExecuteBefor
eFailed() (gas: 752736)
Test result: ok. 14 passed; 0 failed; 0 skipped; finished
in 8.85ms

Running 5 tests for
test/liquidityManagement/liquidityPool/libraries/DebtManage
.unit.t.sol:DebtManageTest
```

```
[PASS]
test_addDebt_mustSetDebtLiquidityProviderToAlicesAddress()
(gas: 71265)
[PASS]
test_tryRepayDebts_mustSetAlicesBalanceToAmountOfDebt_whenT
hreeDebtExistsAndTokensReturnedToContract() (gas: 441336)
[PASS]
test_tryRepayDebts_mustSetAlicesBalanceToAmountOfMint()
(gas: 247461)
[PASS]
test_tryRepayDebts_mustSetAlicesTokenBalanceToAmountOfDebt(
) (gas: 263997)
[PASS]
test_tryRepayDebtst_mustSetAlicesBalanceToAmountOfMint_when
ConditionsForPartialRepayMet() (gas: 342739)
Test result: ok. 5 passed; 0 failed; 0 skipped; finished in
1.85ms

Running 11 tests for
test/marginEngine/libraries/Envelope&Script.integration.t.s
ol:EnvelopeTest
[PASS] testFail_run_mustStopIfScriptFailed() (gas: 49406)
[PASS] test_cannotRunMany_CrossChainActionIsForbidden()
(gas: 14760)
[PASS] test_cannotRun_CrossChainActionIsForbidden() (gas:
13492)
[PASS] test_runMany_happyPath() (gas: 138841)
[PASS] test_runMany_mustContinueEvenIfFirstFailed() (gas:
100312)
[PASS] test_runMany_mustReturn0_whenAllSuccess() (gas:
99168)
[PASS] test_runMany_mustReturn1_whenOneFailed() (gas:
95370)
[PASS] test_runMany_mustReturn2_whenTwoFailed() (gas:
70954)
[PASS] test_run_happyPath() (gas: 100525)
[PASS] test_run_mustReturnFalseWhenFailure() (gas: 37517)
[PASS] test_run_mustReturnTrueWhenSuccess() (gas: 62625)
Test result: ok. 11 passed; 0 failed; 0 skipped; finished
in 5.11ms

Running 1 test for
test/base/FixedU256x32.unit.t.sol:FixedU256x32Test
[PASS] test_toUint256() (gas: 1335)
Test result: ok. 1 passed; 0 failed; 0 skipped; finished in
88.13µs
```

```
Running 20 tests for
test/liquidityManagement/insuranceFund/Fund.unit.t.sol:Fund
Test
[PASS]
testFail_forward_mustNotCallReturnAndDistribute_whenSurplus
EqZero() (gas: 220193)
[PASS] test_authorize_mustDeleteDebt() (gas: 348866)
[PASS] test_authorize_mustEmitDebtPaid() (gas: 345358)
[PASS] test_cannotAuthorize_DebtAmountExceedsBalance()
(gas: 228109)
[PASS] test_cannotAuthorize_DebtDoesNotExists() (gas:
194923)
[PASS] test_cannotAuthorize_fromNonDebtAdminAccount() (gas:
195402)
[PASS] test_cannotForward_fromNonForwarderAccount() (gas:
195713)
[PASS] test_cannotForward_whenNotInitialized() (gas: 9732)
[PASS] test_cannotInitalize_whenAlreadyInitialized() (gas:
191039)
[PASS] test_cannotSupply_fromNonForwarderAccount() (gas:
195441)
[PASS] test_cannotSupply_whenNotInitialized() (gas: 9523)
[PASS]
test_forward_mustCallReturnAndDistribute_whenEnoughSurplus(
) (gas: 248872)
[PASS]
test_forward_mustCallReturnAndDistribute_whenNotEnoughSurpl
us() (gas: 284957)
[PASS] test_forward_mustCreateDebt_whenSurplusIsZero()
(gas: 223904)
[PASS]
test_forward_mustCreateDebt_whenSurplusLessThanAmounts()
(gas: 292273)
[PASS] test_initialize_mustApproveTokenToLP() (gas: 189986)
[PASS] test_initialize_mustAskTokenInLP() (gas: 189545)
[PASS] test_initialize_mustGrantRoles() (gas: 195706)
[PASS] test_supply_mustEmitSupplied() (gas: 254096)
[PASS] test_supply_mustTransferFromForwarder() (gas:
246592)
Test result: ok. 20 passed; 0 failed; 0 skipped; finished
in 3.71ms

Running 6 tests for
test/base/proxy/ImmutableBeaconProxy.unit.t.sol:ImmutableBe
aconProxyTest
[PASS] test_cannotDeployProxy_BeaconCallFailed() (gas:
40265)
```

```
[PASS] test_cannotDeployProxy_BeaconReturnedAddressZero()
(gas: 40414)
[PASS]
test_cannotDeployProxy_BeaconReturnedUnexpectedNumberOfByte
s_whenMsgSenderImplementsInterface() (gas: 40680)
[PASS]
test_cannotDeployProxy_BeaconReturnedUnexpectedNumberOfByte
s_whenMsgSenderIsNotAContract() (gas: 39711)
[PASS] test_constructor_mustExecuteInitData() (gas: 274239)
[PASS] test_fallback() (gas: 273530)
Test result: ok. 6 passed; 0 failed; 0 skipped; finished in
485.08µs

Running 2 tests for
test/base/auth/InternalModifier.unit.t.sol:InternalModifier
DSTest
[PASS] test_cannotCallInternalFunc_UnauthorizedAccount()
(gas: 5283)
[PASS] test_internalFunc() (gas: 705)
Test result: ok. 2 passed; 0 failed; 0 skipped; finished in
109.83µs

Running 10 tests for
test/liquidityManagement/insuranceFund/FundFactory.unit.t.s
ol:FundFactoryTest
[PASS] test_cannotCreateFund_AddressAlreadyRegistered()
(gas: 486609)
[PASS] test_cannotCreateFund_UnauthorizedAccount() (gas:
8287)
[PASS] test_cannotGetFund_AddressIsNotRegisteredUnderKey()
(gas: 8124)
[PASS] test_cannotUpgradeTo_UnauthorizedAccount() (gas:
7556)
[PASS] test_cannotUpgradeTo_withZeroAddress() (gas: 7229)
[PASS] test_createFund_mustCallInitCall() (gas: 259825)
[PASS] test_createFund_mustRegisterNewFund() (gas: 262022)
[PASS] test_getFund() (gas: 260352)
[PASS] test_getImplementation() (gas: 3445)
[PASS] test_upgradeTo() (gas: 13016)
Test result: ok. 10 passed; 0 failed; 0 skipped; finished
in 649.08µs

Running 6 tests for
test/liquidityManagement/insuranceFund/libraries/MoneyAccou
ntant.unit.t.sol:MoneyAccountantTest
[PASS]
testFuzz_calculateAcceptableExpenses_whenGTE(uint256,uint8)
```

```
(runs: 256, μ: 10448, ~: 9920)
[PASS]
testFuzz_calculateAcceptableExpenses_whenLTE(uint256,uint8)
(runs: 256, μ: 8560, ~: 8049)
[PASS]
testFuzz_spendMoney_mustEmitNewDebt_whenGT(uint256,uint8)
(runs: 256, μ: 39400, ~: 39019)
[PASS] test_createDebtIfNecessary() (gas: 31059)
[PASS] test_createDebtIfNecessary_whenNotNecessary() (gas:
7487)
[PASS] test_deleteDebt() (gas: 20960)
Test result: ok. 6 passed; 0 failed; 0 skipped; finished in
46.01ms

Running 16 tests for
test/accountAbstraction/compliance/libraries/TokensReposito
ry.unit.t.sol:TokensRepositoryTest
[PASS]
testFuzz_cannotUpdateTokensSupport_CannotSetPermissionToNon
e(uint8) (runs: 256, μ: 32872, ~: 32960)
[PASS]
testFuzz_enforceTokenHasPermission_whenCollateral(uint8)
(runs: 256, μ: 32864, ~: 31778)
[PASS]
testFuzz_enforceTokenHasPermission_whenFullAccess(uint8)
(runs: 256, μ: 31300, ~: 31793)
[PASS]
testFuzz_enforceTokenHasPermission_whenLeverage(uint8)
(runs: 256, μ: 33196, ~: 31875)
[PASS] testFuzz_enforceTokenHasPermission_whenNone(uint8)
(runs: 256, μ: 12451, ~: 14193)
[PASS]
testFuzz_enforceTokenHasPermission_whenTradeOnly(uint8)
(runs: 256, μ: 33810, ~: 35250)
[PASS]
test_enforceTokenSupportedOrSuspended_whenSupported() (gas:
24751)
[PASS]
test_enforceTokenSupportedOrSuspended_whenSuspended() (gas:
26487)
[PASS]
test_enforceTokenSupportedOrSuspended_whenUndefined() (gas:
6648)
[PASS] test_enforceTokenSupported_whenSupported() (gas:
24795)
[PASS] test_enforceTokenSupported_whenSuspended() (gas:
30503)
```

```
[PASS] test_enforceTokenSupported_whenUndefined() (gas:
6721)
[PASS]
test_updateTokensSupport_mustCorrectlySwitchPermissions()
(gas: 61080)
[PASS]
test_updateTokensSupport_mustCorrectlySwitchStatuses()
(gas: 53081)
[PASS]
test_updateTokensSupport_mustReturnCorrectStorageUpdatedFla
g_whenPermissionDiffers() (gas: 57919)
[PASS]
test_updateTokensSupport_mustReturnCorrectStorageUpdatedFla
g_whenStatusDiffers() (gas: 54718)
Test result: ok. 16 passed; 0 failed; 0 skipped; finished
in 43.23ms

Running 30 tests for
test/libraries/Command.unit.t.sol:CommandUnitTest
[PASS] test_append() (gas: 54908)
[PASS] test_asArray() (gas: 13122)
[PASS] test_concat() (gas: 25589)
[PASS] test_concat_with_array() (gas: 39430)
[PASS] test_last() (gas: 27851)
[PASS] test_last_modification() (gas: 24696)
[PASS] test_populateWithApprove_arr() (gas: 46193)
[PASS] test_populateWithApprove_arr_amounts_zero() (gas:
25623)
[PASS] test_populateWithApprove_plain() (gas: 32042)
[PASS] test_populateWithApprove_plain_amounts_zero() (gas:
13134)
[PASS] test_populateWithApprove_tokens2() (gas: 52398)
[PASS] test_populateWithApprove_tokens2_amount0_zero()
(gas: 32511)
[PASS] test_populateWithApprove_tokens2_amount1_zero()
(gas: 32554)
[PASS] test_populateWithApprove_tokens2_amounts_zero()
(gas: 13578)
[PASS] test_populateWithApprove_tokens3() (gas: 72925)
[PASS] test_populateWithApprove_tokens3_amount0_zero()
(gas: 53004)
[PASS] test_populateWithApprove_tokens3_amount1_zero()
(gas: 53188)
[PASS] test_populateWithApprove_tokens3_amount2_zero()
(gas: 53187)
[PASS] test_populateWithApprove_tokens3_amounts_zero()
(gas: 14139)
```

```
[PASS] test_populateWithApprove_tokens4() (gas: 93760)
[PASS] test_populateWithApprove_tokens4_amount0_zero()
(gas: 73614)
[PASS] test_populateWithApprove_tokens4_amount1_zero()
(gas: 73819)
[PASS] test_populateWithApprove_tokens4_amount2_zero()
(gas: 73917)
[PASS] test_populateWithApprove_tokens4_amount3_zero()
(gas: 73918)
[PASS] test_populateWithApprove_tokens4_amounts_zero()
(gas: 14957)
[PASS] test_populateWithRevokeAndApprove_plain() (gas:
52491)
[PASS]
test_populateWithRevokeAndApprove_plain_amounts_zero()
(gas: 33043)
[PASS] test_push() (gas: 39094)
[PASS] test_unshift() (gas: 39496)
[PASS] test_unshift_with_array() (gas: 46852)
Test result: ok. 30 passed; 0 failed; 0 skipped; finished
in 53.79ms

Running 66 tests for
test/accountAbstraction/interpreter/oneInchV5/OneInchV5Eval
uator.unit.t.sol:OneInchV5EvaluatorTest
[PASS]
test_cannotConstructClipperSwapToWithPermit_whenTokenInUnde
fined() (gas: 31461)
[PASS]
test_cannotConstructClipperSwapToWithPermit_whenTokenOutUnd
efined() (gas: 28917)
[PASS]
test_cannotConstructClipperSwapTo_whenTokenInUndefined()
(gas: 29461)
[PASS]
test_cannotConstructClipperSwapTo_whenTokenOutUndefined()
(gas: 26912)
[PASS]
test_cannotConstructClipperSwap_whenTokenInUndefined()
(gas: 29397)
[PASS]
test_cannotConstructClipperSwap_whenTokenOutUndefined()
(gas: 26893)
[PASS] test_cannotConstructSwap_whenTokenInUndefined()
(gas: 32982)
[PASS] test_cannotConstructSwap_whenTokenOutUndefined()
(gas: 30437)
```

```
[PASS]
test_cannotConstructUniswapV3SwapToWithPermit_whenTokenInUn
defined() (gas: 41466)
[PASS]
test_cannotConstructUniswapV3SwapToWithPermit_whenTokenOutU
ndefined() (gas: 38941)
[PASS]
test_cannotConstructUniswapV3SwapTo_whenTokenInUndefined()
(gas: 38583)
[PASS]
test_cannotConstructUniswapV3SwapTo_whenTokenOutUndefined()
(gas: 36057)
[PASS]
test_cannotConstructUniswapV3Swap_whenTokenInUndefined()
(gas: 38584)
[PASS]
test_cannotConstructUniswapV3Swap_whenTokenOutUndefined()
(gas: 36102)
[PASS]
test_cannotConstructUnoswapToWithPermit_whenTokenInUndefine
d() (gas: 40597)
[PASS]
test_cannotConstructUnoswapToWithPermit_whenTokenOutUndefin
ed() (gas: 38138)
[PASS] test_cannotConstructUnoswapTo_whenTokenInUndefined()
(gas: 38458)
[PASS]
test_cannotConstructUnoswapTo_whenTokenOutUndefined() (gas:
35956)
[PASS] test_cannotConstructUnoswap_whenTokenInUndefined()
(gas: 38459)
[PASS] test_cannotConstructUnoswap_whenTokenOutUndefined()
(gas: 35870)
[PASS] test_constructClipperSwap() (gas: 90973)
[PASS] test_constructClipperSwapTo() (gas: 91015)
[PASS] test_constructClipperSwapToWithPermit() (gas:
113345)
[PASS]
test_constructClipperSwapToWithPermit_whenEthSuspended()
(gas: 116617)
[PASS] test_constructClipperSwapToWithPermit_withApprove()
(gas: 135247)
[PASS]
test_constructClipperSwapToWithPermit_withApprove_whenToken
InSuspended() (gas: 137149)
[PASS] test_constructClipperSwapTo_whenEthSuspended() (gas:
94199)
```

```
[PASS] test_constructClipperSwapTo_withApprove() (gas:
112827)
[PASS]
test_constructClipperSwapTo_withApprove_whenTokenInSuspende
d() (gas: 114885)
[PASS] test_constructClipperSwap_whenEthSuspended() (gas:
94179)
[PASS] test_constructClipperSwap_withApprove() (gas:
112854)
[PASS]
test_constructClipperSwap_withApprove_whenTokenInSuspended(
) (gas: 114775)
[PASS] test_constructSwap() (gas: 128303)
[PASS] test_constructSwap_whenEthSuspended() (gas: 131597)
[PASS] test_constructSwap_withApprove() (gas: 150230)
[PASS]
test_constructSwap_withApprove_whenTokenInSuspended() (gas:
152198)
[PASS] test_constructUniswapV3Swap() (gas: 82375)
[PASS] test_constructUniswapV3SwapTo() (gas: 82396)
[PASS] test_constructUniswapV3SwapToWithPermit() (gas:
112315)
[PASS]
test_constructUniswapV3SwapToWithPermit_whenEthSuspended()
(gas: 115633)
[PASS]
test_constructUniswapV3SwapToWithPermit_whenTokenOutIsRever
sed() (gas: 115563)
[PASS]
test_constructUniswapV3SwapToWithPermit_withApprove() (gas:
134174)
[PASS]
test_constructUniswapV3SwapToWithPermit_withApprove_whenTok
enInSuspended() (gas: 136207)
[PASS] test_constructUniswapV3SwapTo_whenEthSuspended()
(gas: 85690)
[PASS]
test_constructUniswapV3SwapTo_whenTokenOutIsReversed()
(gas: 85707)
[PASS] test_constructUniswapV3SwapTo_withApprove() (gas:
104317)
[PASS]
test_constructUniswapV3SwapTo_withApprove_whenTokenInSuspen
ded() (gas: 106305)
[PASS] test_constructUniswapV3Swap_whenEthSuspended() (gas:
85693)
[PASS] test_constructUniswapV3Swap_whenTokenOutIsReversed()
```

```
(gas: 85642)
[PASS] test_constructUniswapV3Swap_withApprove() (gas:
104251)
[PASS]
test_constructUniswapV3Swap_withApprove_whenTokenInSuspende
d() (gas: 106263)
[PASS] test_constructUnoswap() (gas: 88964)
[PASS] test_constructUnoswapTo() (gas: 89070)
[PASS] test_constructUnoswapToWithPermit() (gas: 111468)
[PASS] test_constructUnoswapToWithPermit_whenEthSuspended()
(gas: 114697)
[PASS]
test_constructUnoswapToWithPermit_whenTokenOutIsReversed()
(gas: 114681)
[PASS] test_constructUnoswapToWithPermit_withApprove()
(gas: 133368)
[PASS]
test_constructUnoswapToWithPermit_withApprove_whenTokenInSu
spended() (gas: 135314)
[PASS] test_constructUnoswapTo_whenEthSuspended() (gas:
92320)
[PASS] test_constructUnoswapTo_whenTokenOutIsReversed()
(gas: 92241)
[PASS] test_constructUnoswapTo_withApprove() (gas: 110903)
[PASS]
test_constructUnoswapTo_withApprove_whenTokenInSuspended()
(gas: 112937)
[PASS] test_constructUnoswap_whenEthSuspended() (gas:
92214)
[PASS] test_constructUnoswap_whenTokenOutIsReversed() (gas:
92200)
[PASS] test_constructUnoswap_withApprove() (gas: 110841)
[PASS]
test_constructUnoswap_withApprove_whenTokenInSuspended()
(gas: 112805)
Test result: ok. 66 passed; 0 failed; 0 skipped; finished
in 36.90ms


// HARDHAT TESTS
  CurveFi validator liquidity tests
Whitelisting diamond deployment finished
Executing update action for whitelisted for trading tokens
Successfully updated whitelisted for trading tokens
interpreter's evaluators deployment finished
Executing update action for OneInchV5 protocol
Successfully updated OneInchV5 protocol
```

```
Executing update action for Arkis.MarginAccount protocol
Successfully updated Arkis.MarginAccount protocol
Executing update action for Arkis.InsuranceFund protocol
Successfully updated Arkis.InsuranceFund protocol
Executing update action for Arkis.LiquidityPool protocol
Successfully updated Arkis.LiquidityPool protocol
Executing update action for Transfer protocol
Successfully updated Transfer protocol
Executing update action for ConvexFi protocol
Successfully updated ConvexFi protocol
Executing update action for CurveFi protocol
Successfully updated CurveFi protocol
Executing update action for LidoFi protocol
Successfully updated LidoFi protocol
Executing update action for UniswapV3 protocol
Successfully updated UniswapV3 protocol
Executing update action for ConvexFi protocol's operators
Successfully updated ConvexFi protocol's operators
Executing update action for CurveFi protocol's operators
Successfully updated CurveFi protocol's operators
Executing update action for LidoFi protocol's operators
Successfully updated LidoFi protocol's operators
Executing update action for UniswapV3 protocol's operators
Successfully updated UniswapV3 protocol's operators
LiquidityPool diamond deployment finished
Executing update action for LiquidityPool implementation
Successfully updated LiquidityPool implementation
MerkleTreeRoot updated
MarginAccount diamond deployment finished
MarginEngine diamond deployment finished
Executing update action for LiquidityPool for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Successfully updated LiquidityPool for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Executing update action for LiquidityPool for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Successfully updated LiquidityPool for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Executing update action for LiquidityPool for
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Successfully updated LiquidityPool for
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Executing update action for LiquidityPool for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Successfully updated LiquidityPool for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Executing update action for LiquidityPool for
```

```
0x853d955aCEf822Db058eb8505911ED77F175b99e
Successfully updated LiquidityPool for
0x853d955aCEf822Db058eb8505911ED77F175b99e
Executing update action for LiquidityPool for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Successfully updated LiquidityPool for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Executing update action for LiquidityPool for
0x6B175474E89094C44Da98b954EedeAC495271d0F
Successfully updated LiquidityPool for
0x6B175474E89094C44Da98b954EedeAC495271d0F
InsuranceFund diamond deployment finished
Executing update action for AssemblySandbox's config
Successfully updated AssemblySandbox's config
Executing update action for ConvexFi protocol's pools
Successfully updated ConvexFi protocol's pools
Executing update action for CurveFi protocol's pools
Successfully updated CurveFi protocol's pools
Executing update action for LidoFi protocol's pools
Successfully updated LidoFi protocol's pools
Executing update action for UniswapV3 protocol's pools
Successfully updated UniswapV3 protocol's pools
Granting role 0x939e90d5...c6a1ad99 to
0xc3b99d27eF3B07C94Ee3cFD670281F0CF98A02f1...
Executing update action for MarginAccount implementation
Successfully updated MarginAccount implementation
Executing update action for InsuranceFund implementation
Successfully updated InsuranceFund implementation
Executing update action for InsuranceFund for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Successfully updated InsuranceFund for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Executing update action for SetFund on LiquidityPool for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Successfully updated SetFund on LiquidityPool for
0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
Executing update action for InsuranceFund for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Successfully updated InsuranceFund for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Executing update action for SetFund on LiquidityPool for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Successfully updated SetFund on LiquidityPool for
0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
Executing update action for InsuranceFund for
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Successfully updated InsuranceFund for
```

```
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Executing update action for SetFund on LiquidityPool for
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Successfully updated SetFund on LiquidityPool for
0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
Executing update action for InsuranceFund for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Successfully updated InsuranceFund for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Executing update action for SetFund on LiquidityPool for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Successfully updated SetFund on LiquidityPool for
0xdAC17F958D2ee523a2206206994597C13D831ec7
Executing update action for InsuranceFund for
0x853d955aCEf822Db058eb8505911ED77F175b99e
Successfully updated InsuranceFund for
0x853d955aCEf822Db058eb8505911ED77F175b99e
Executing update action for SetFund on LiquidityPool for
0x853d955aCEf822Db058eb8505911ED77F175b99e
Successfully updated SetFund on LiquidityPool for
0x853d955aCEf822Db058eb8505911ED77F175b99e
Executing update action for InsuranceFund for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Successfully updated InsuranceFund for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Executing update action for SetFund on LiquidityPool for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Successfully updated SetFund on LiquidityPool for
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
Executing update action for InsuranceFund for
0x6B175474E89094C44Da98b954EedeAC495271d0F
Successfully updated InsuranceFund for
0x6B175474E89094C44Da98b954EedeAC495271d0F
Executing update action for SetFund on LiquidityPool for
0x6B175474E89094C44Da98b954EedeAC495271d0F
Successfully updated SetFund on LiquidityPool for
0x6B175474E89094C44Da98b954EedeAC495271d0F
Granting role 0xbd8ac73f...6efb0a29 to
0xc3b99d27eF3B07C94Ee3cFD670281F0CF98A02f1...
Granting role 0x73dc7116...2a288995 to
abc123abc123abc123abc123abc123abc123abc1...
    ✔ 1. TradingCompliance should have SwapRouter
selectors

  CurveFi validator swap tests
    ✔ 1. TradingCompliance should have SwapRouter
selectors
```

```
  LidoFi validator liquidity tests
    ✔ 1. TradingCompliance should have
NonFungiblePositionManager selectors
    ✔ 2. Should allow to stake eth and get steth
    ✔ 3. Should allow to wrap steth and get wsteth &&
unwrap wsteth and get steth back
    ✔ 4. Should allow to use shortcut to wrap eth to
wsteth

  InsuranceFundEvaluator tests
    ✔ 1. Supply ERC20 (ExchangeInstruction)
    ✔ 2. Supply ETH is forbidden(ExchangeInstruction)
    ✔ 3. Forward (DecreasePositionInstruction) - OK
    ✔ 4. Forward (DecreasePositionInstruction) - invalid
input

  LiquidityPoolEvaluator tests
    ✔ 1. returnAndDistribute (DecreasePositionInstruction)

  MarginAccountEvaluator tests
    ✔ 1. Should evaluate correct commands for the
instruction when USDT
    ✔ 2. Should evaluate correct commands for the
instruction when ETH

  ConvexFi evaluator liquidity tests
    ✔ 1. Should allow to unstake & withdraw from tricrypto
convex pool (1076ms)
    ✔ 2. Should allow to unstake cvxCRV

  ConvexFi validator liquidity tests
    ✔ 1. TradingCompliance should have SwapRouter
selectors
    ✔ 2. Should allow to deposit to booster with and
without staking option and withdraw(All) from rewardPool
and then withdraw(All) from booster
    ✔ 3. Should allow to depositAll to booster with and
without staking option, stake and then
withdraw(All)AndUnwrap from rewardPool

  CurveFi evaluator liquidity tests
    Positive scenarios
      ✔ 0. Should allow to remove liquidity from 3pool
      ✔ 1. Should allow to remove liquidity from frax_usdc
      ✔ 2. Should allow to remove liquidity from frax
      ✔ 3. Should allow to remove liquidity from steth
      ✔ 4. Should allow to remove liquidity from tricrypto

  CurveFi evaluator swap tests
    Positive scenarios
      ✔ 0. Should allow to swap from USDC to USDT via
3pool pool
      ✔ 1. Should allow to swap from USDC to USDT via frax
pool
      ✔ 2. Should allow to swap from USDT to FRAX via frax
pool (1090ms)
      ✔ 3. Should allow to swap from USDC to FRAX via
frax_usdc pool
      ✔ 4. Should allow to swap from ETH to stETH via
steth pool
      ✔ 5. Should allow to swap from stETH to ETH via
steth pool
      ✔ 6. Should allow to swap from WETH to WBTC via
tricrypto pool (1920ms)

  LidoFi evaluator liquidity tests
    ✔ 1. Should correctly compile instructions

  UniswapV3 evaluator swap tests
    ✔ 1. Should successfully swap USDC for WETH
    ✔ 2. Should successfully swap USDC for WBTC via WETH

  UniswapV3 liquidity E2E tests
    ✔ 1. WETH-USDC pool

  UniswapV3 validator swap tests
    ✔ 1. TradingCompliance should have SwapRouter
selectors
    ✔ 2. Should successfully execute "exactInputSingle"
    ✔ 3. Should successfully execute "exactInput"

  Margin Account allocation E2E flow specification
    ✔ Trader registers margin account using backend
signature (1569ms)
    ✔ Margin Engine submits allocation plan and opens the
account
    ✔ Trader now able to use his account, e.g. open a
position in CurveFi (1052ms)

  Margin Account liquidation E2E flow specification
    ✔ Margin engine submits allocation plan and thus
liquidates the account
    ✔ Liquidity provider can claim interest rewards from
```

```
liquidation

  Margin Account liquidation with 1inch E2E flow
specification
    ✔ Margin engine submits DSL and thus liquidates the
account

  LiquidityPool deployment health check
    ✔ 1. deposit + withdraw USDC Pool


  44 passing (42s)
```

Code Coverage

The code coverage for the forge tests was gathered by running `forge coverage`. We were unable to gather coverage results for the hardhat test.

Given the protocols use of composition as opposed to inheritance, coverage is likely larger than the tests indicate.

File	% Lines	% Statements	% Branches	% Func
contracts/accountAbstraction/compliance/AbstractValidator.sol	30.43% (**7**/23)	25.71% (**9**/35)	15.00% (**3**/20)	66.67% (**4**/6)
contracts/accountAbstraction/compliance/WhitelistingController.sol	0.00% (**0**/21)	0.00% (**0**/30)	0.00% (**0**/10)	0.00% (**0**/8)
contracts/accountAbstraction/compliance/approve/App	0.00% (**0**/5)	0.00% (**0**/7)	100.00% (**0**/0)	0.00% (**0**/2)

File	% Lines	% Statements	% Branches	% Funcs
roveValidator.sol				
contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorPlainPool.sol	0.00% (**0**/61)	0.00% (**0**/109)	0.00% (**0**/8)	0.00% (**0**/15)
contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorSwapRouter.sol	0.00% (**0**/14)	0.00% (**0**/22)	0.00% (**0**/2)	0.00% (**0**/5)
contracts/accountAbstraction/compliance/curveFi/validators/CurveFiValidatorZapper.sol	0.00% (**0**/24)	0.00% (**0**/27)	100.00% (**0**/0)	0.00% (**0**/7)
contracts/accountAbstraction/compliance/libraries/ProtocolsRepository.sol	55.88% (**19**/34)	47.83% (**22**/46)	14.29% (**2**/14)	54.55% (**6**/11)

File	% Lines	% Statements	% Branches	% Func
contracts/accountAbstraction/compliance/libraries/TokensRepository.sol	0.00% (**0**/36)	0.00% (**0**/58)	0.00% (**0**/28)	0.00% (**0**/10)
contracts/accountAbstraction/compliance/uniswapV3/UniswapV3Validator.sol	0.00% (**0**/29)	0.00% (**0**/29)	100.00% (**0**/0)	0.00% (**0**/7)
contracts/accountAbstraction/interpreter/JitCompiler.sol	17.39% (**4**/23)	17.95% (**7**/39)	100.00% (**0**/0)	20.00% (**1**/5)
contracts/accountAbstraction/interpreter/LiquidityPoolsController.sol	0.00% (**0**/18)	0.00% (**0**/26)	0.00% (**0**/4)	0.00% (**0**/4)
contracts/accountAbstraction/interpreter/base/LiquidityPoolsRepository.sol	0.00% (**0**/13)	0.00% (**0**/20)	0.00% (**0**/8)	0.00% (**0**/2)
contracts/accountAbstraction/interpreter/curveFi/CurveFiLiquidityP	0.00% (**0**/23)	0.00% (**0**/31)	0.00% (**0**/6)	0.00% (**0**/8)

File	% Lines	% Statements	% Branches	% Funcs
oolsRepository.sol				
contracts/accountAbstraction/interpreter/curveFi/libraries/CurveFiLib.sol	0.00% (**0**/15)	0.00% (**0**/26)	0.00% (**0**/10)	0.00% (**0**/3)
contracts/accountAbstraction/interpreter/libraries/Config.sol	0.00% (**0**/17)	0.00% (**0**/20)	0.00% (**0**/12)	0.00% (**0**/5)
contracts/accountAbstraction/interpreter/libraries/Path.sol	0.00% (**0**/17)	0.00% (**0**/23)	0.00% (**0**/4)	0.00% (**0**/8)
contracts/accountAbstraction/interpreter/libraries/ScriptCompiler.sol	0.00% (**0**/15)	0.00% (**0**/19)	0.00% (**0**/8)	0.00% (**0**/1)
contracts/accountAbstraction/interpreter/oneinchV5/OneInchV5Evaluator.sol	0.00% (**0**/7)	0.00% (**0**/8)	0.00% (**0**/2)	0.00% (**0**/1)
contracts/accountAbstraction/interpreter/one	0.00% (**0**/14)	0.00% (**0**/14)	100.00% (**0**/0)	0.00% (**0**/7)

File	% Lines	% Statements	% Branches	% Func
inchV5/actions/OneInchV5Exchange.sol				
contracts/accountAbstraction/interpreter/oneinchV5/base/OneInchV5Hub.sol	0.00% (**0/**68)	0.00% (**0/**75)	0.00% (**0/**20)	0.00% (**0/**11)
contracts/accountAbstraction/interpreter/oneinchV5/libraries/UniswapTokens.sol	0.00% (**0/**4)	0.00% (**0/**8)	100.00% (**0/**0)	0.00% (**0/**2)
contracts/accountAbstraction/marginAccount/Account.sol	100.00% (**47/**47)	100.00% (**60/**60)	100.00% (**10/**10)	100.00 (**14/**14
contracts/accountAbstraction/marginAccount/AccountFactory.sol	100.00% (**10/**10)	100.00% (**14/**14)	100.00% (**0/**0)	100.00 (**4/**4)
contracts/accountAbstraction/marginAccount/base/CommandSafeExecutor.sol	100.00% (**12/**12)	100.00% (**20/**20)	100.00% (**0/**0)	100.00 (**5/**5)

File	% Lines	% Statements	% Branches	% Func
contracts/accountAbstraction/marginAccount/libraries/AccountFactoryRepository.sol	80.00% (**8/**10)	66.67% (**10/**15)	50.00% (**1/**2)	66.67 (**4/**6)
contracts/base/StateMachine.sol	73.08% (**19/**26)	59.09% (**26/**44)	43.75% (**7/**16)	63.64 (**7/**11)
contracts/base/auth/AccessControlDS.sol	100.00% (**2/**2)	100.00% (**5/**5)	100.00% (**0/**0)	50.00 (**1/**2)
contracts/base/auth/OwnableAssignable.sol	100.00% (**8/**8)	83.33% (**10/**12)	50.00% (**2/**4)	100.00 (**3/**3)
contracts/base/auth/OwnableReadonly.sol	100.00% (**2/**2)	100.00% (**5/**5)	100.00% (**2/**2)	100.00 (**2/**2)
contracts/base/auth/OwnableReadonlyDS.sol	100.00% (**2/**2)	100.00% (**3/**3)	100.00% (**0/**0)	100.00 (**1/**1)
contracts/base/proxy/BeaconDS.sol	100.00% (**6/**6)	100.00% (**12/**12)	100.00% (**6/**6)	100.00 (**3/**3)
contracts/base/proxy/ImmutableBeaconProxy.sol	100.00% (**5/**5)	70.00% (**7/**10)	50.00% (**3/**6)	100.00 (**1/**1)

File	% Lines	% Statements	% Branches	% Func
contracts/libraries/Address.sol	0.00% (**0**/8)	0.00% (**0**/13)	100.00% (**0**/0)	0.00% (**0**/5)
contracts/libraries/AddressRegistry.sol	0.00% (**0**/8)	0.00% (**0**/13)	0.00% (**0**/4)	0.00% (**0**/4)
contracts/libraries/Asset.sol	0.00% (**0**/6)	0.00% (**0**/11)	0.00% (**0**/8)	0.00% (**0**/2)
contracts/libraries/CalldataLibrary.sol	0.00% (**0**/5)	0.00% (**0**/9)	100.00% (**0**/0)	0.00% (**0**/2)
contracts/libraries/Command.sol	1.56% (**1**/64)	1.16% (**1**/86)	0.00% (**0**/22)	5.88% (**1**/17)
contracts/libraries/DiamondLib.sol	100.00% (**2**/2)	100.00% (**2**/2)	100.00% (**0**/0)	100.00 (**1**/1)
contracts/libraries/Nonce.sol	0.00% (**0**/6)	0.00% (**0**/7)	0.00% (**0**/2)	0.00% (**0**/4)
contracts/libraries/SafeCall.sol	0.00% (**0**/6)	0.00% (**0**/8)	100.00% (**0**/0)	0.00% (**0**/5)
contracts/liquidityManagement/insuranceFund/FundFactory.sol	0.00% (**0**/5)	0.00% (**0**/8)	100.00% (**0**/0)	0.00% (**0**/3)

File	% Lines	% Statements	% Branches	% Func
contracts/liquidityManagement/insuranceFund/fund/Fund.sol	100.00% (23/23)	100.00% (32/32)	100.00% (6/6)	100.00 (6/6)
contracts/liquidityManagement/insuranceFund/libraries/Debt.sol	100.00% (2/2)	100.00% (2/2)	100.00% (0/0)	100.00 (1/1)
contracts/liquidityManagement/insuranceFund/libraries/MoneyAccountant.sol	100.00% (16/16)	95.45% (21/22)	83.33% (5/6)	100.00 (7/7)
contracts/liquidityManagement/liquidityPool/MerkleTreeWhitelist.sol	0.00% (0/2)	0.00% (0/3)	100.00% (0/0)	0.00% (0/2)
contracts/liquidityManagement/liquidityPool/PoolFactory.sol	0.00% (0/9)	0.00% (0/13)	100.00% (0/0)	0.00% (0/7)
contracts/liquidityManagement/liquidityPool/base/Suspendable.sol	100.00% (5/5)	100.00% (6/6)	100.00% (0/0)	100.00 (4/4)

File	% Lines	% Statements	% Branches	% Func
contracts/liquidityManagement/liquidityPool/libraries/DebtManager.sol	0.00% (**0**/15)	0.00% (**0**/22)	0.00% (**0**/2)	0.00% (**0**/6)
contracts/liquidityManagement/liquidityPool/libraries/MerkleTreeRepository.sol	0.00% (**0**/6)	0.00% (**0**/9)	0.00% (**0**/2)	0.00% (**0**/4)
contracts/liquidityManagement/liquidityPool/libraries/Queue.sol	0.00% (**0**/6)	0.00% (**0**/10)	0.00% (**0**/2)	0.00% (**0**/5)
contracts/liquidityManagement/liquidityPool/libraries/staking/PositionManager.sol	0.00% (**0**/6)	0.00% (**0**/6)	100.00% (**0**/0)	0.00% (**0**/2)
contracts/liquidityManagement/liquidityPool/libraries/staking/RewardsMath.sol	0.00% (**0**/80)	0.00% (**0**/97)	0.00% (**0**/20)	0.00% (**0**/16)
contracts/liquidityManagement/liquidityPool	16.00% (**8**/50)	13.79% (**8**/58)	4.55% (**1**/22)	18.18% (**2**/11)

File	% Lines	% Statements	% Branches	% Func
/pool/Pool.sol				
contracts/marginEngine/Dispatcher.sol	100.00% (**19**/19)	100.00% (**28**/28)	83.33% (**5**/6)	100.00 (**4**/4)
contracts/marginEngine/base/SignatureProcessor.sol	100.00% (**8**/8)	86.67% (**13**/15)	50.00% (**2**/4)	100.00 (**3**/3)
contracts/marginEngine/base/ThresholdsVerifier.sol	100.00% (**8**/8)	80.00% (**12**/15)	62.50% (**5**/8)	100.00 (**1**/1)
contracts/marginEngine/libraries/Envelope.sol	0.00% (**0**/12)	0.00% (**0**/22)	0.00% (**0**/2)	0.00% (**0**/3)
contracts/marginEngine/libraries/Package.sol	0.00% (**0**/6)	0.00% (**0**/6)	0.00% (**0**/4)	0.00% (**0**/1)
test/accountAbstraction/compliance/libraries/StatusTestUtils.sol	0.00% (**0**/4)	0.00% (**0**/4)	100.00% (**0**/0)	0.00% (**0**/4)
test/accountAbstraction/marginAccount/Account&StateMachine.int	100.00% (**2**/2)	100.00% (**3**/3)	100.00% (**0**/0)	100.00 (**2**/2)

File	% Lines	% Statements	% Branches	% Func
egration.t.sol				
test/accountAbstraction/marginAccount/base/CommandSafeExecutor&AbstractValidator.integration.t.sol	100.00% (**8**/8)	100.00% (**10**/10)	100.00% (**0**/0)	100.00 (**7**/7)
test/base/proxy/ImmutableBeaconProxy.unit.t.sol	100.00% (**3**/3)	66.67% (**2**/3)	50.00% (**1**/2)	100.00 (**1**/1)
test/libraries/Asset.unit.t.sol	100.00% (**1**/1)	100.00% (**1**/1)	100.00% (**0**/0)	100.00 (**1**/1)
test/libraries/Command.t.utils.sol	0.00% (**0**/19)	0.00% (**0**/29)	100.00% (**0**/0)	0.00% (**0**/7)
test/libraries/SafeCall.unit.t.sol	100.00% (**4**/4)	50.00% (**2**/4)	75.00% (**6**/8)	100.00 (**4**/4)
test/libraries/ValidatorTestUtility.sol	0.00% (**0**/1)	0.00% (**0**/1)	100.00% (**0**/0)	0.00% (**0**/1)
test/liquidityManagement/liquidityPool/utils/helpers.sol	0.00% (**0**/8)	0.00% (**0**/12)	100.00% (**0**/0)	0.00% (**0**/5)

File	% Lines	% Statements	% Branches	% Func
test/utils/DynamicArrays.sol	0.00% (**0/**66)	0.00% (**0/**66)	100.00% (**0/**0)	0.00% (**0/**17)
test/utils/InstructionsMocker.sol	0.00% (**0/**10)	0.00% (**0/**20)	100.00% (**0/**0)	0.00% (**0/**4)
test/utils/MockJitCompiler.sol	83.33% (**5/**6)	90.00% (**9/**10)	100.00% (**0/**0)	16.67% (**1/**6)
test/utils/MockedInstructionsExecutor.sol	0.00% (**0/**4)	0.00% (**0/**7)	0.00% (**0/**2)	0.00% (**0/**1)
Total	23.54% (**266/**1130)	23.13% (**362/**1565)	20.06% (**67/**334)	27.87% (**102/**3

Changelog

- 2023-12-11 - Initial Report
- 2024-01-12 - Final Report

About Quantstamp

Quantstamp is a global leader in blockchain security. Founded in 2017, Quantstamp's mission is to securely onboard the next billion users to Web3 through its best-in-class Web3 security products and services.

Quantstamp's team consists of cybersecurity experts hailing from globally recognized organizations including Microsoft, AWS, BMW, Meta, and the Ethereum Foundation. Quantstamp engineers hold PhDs or advanced computer science degrees, with decades of combined experience in formal verification, static analysis, blockchain audits, penetration testing, and original leading-edge research.

To date, Quantstamp has performed more than 500 audits and secured over $200 billion in digital asset risk from hackers. Quantstamp has worked with a diverse range of customers, including startups, category leaders and financial institutions. Brands that Quantstamp has worked with include Ethereum 2.0, Binance, Visa, PayPal, Polygon, Avalanche, Curve, Solana, Compound, Lido, MakerDAO, Arbitrum, OpenSea and the World Economic Forum.

Quantstamp's collaborations and partnerships showcase our commitment to world-class research, development and security. We're honored to work with some of the top names in the industry and proud to secure the future of web3.

Notable Collaborations & Customers:

- Blockchains: Ethereum 2.0, Near, Flow, Avalanche, Solana, Cardano, Binance Smart Chain, Hedera Hashgraph, Tezos
- DeFi: Curve, Compound, Maker, Lido, Polygon, Arbitrum, SushiSwap
- NFT: OpenSea, Parallel, Dapper Labs, Decentraland, Sandbox, Axie Infinity, Illuvium, NBA Top Shot, Zora
- Academic institutions: National University of Singapore, MIT

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication or other making available of the report to you by Quantstamp.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites&aspo; owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on any website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any output generated by such software.

Disclaimer

The review and this report are provided on an as-is, where-is, and as-available basis. To the fullest extent permitted by law, Quantstamp disclaims all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. You agree that your access and/or use of the report and other results of the review, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. 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. This report is based on the scope of materials and documentation provided for a limited review at the time provided. You acknowledge that Blockchain technology remains under development and is subject to unknown risks and flaws and, as such, the report may not be complete or inclusive of all vulnerabilities. The review is limited to the materials identified in the report and does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. The report does not indicate the endorsement by Quantstamp of any particular project or team, nor guarantee its security, and may not be represented as such. No third party is entitled to rely on the report in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. Quantstamp does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party, or 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, or any related services and products, any hyperlinked websites, or any other websites or mobile applications, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third party. 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.

Quantstamp

Arkis