STATE MIND

Aggregation Router v5

18-07-2022 - 29-07-2022

Table of contents

1. Project Brief

Title	Description
Client	1inch
Project name	Aggregation Router v5
Timeline	18-07-2022 - 29-07-2022
Number of auditors	4
Initial commit	47f1bc6b5d715efc2d9a8af2d20987ed71722d02
Final commit	8db60cc1052440c6fb0f8b764086dc9aa0961bba

Short Overview

The 1inch Aggregation Router is a decentralized exchanger with a cost-efficient router algorithm. The protocol aggregates multiple sources of liquidity to find a route with the best token swap rate and minimal slippage.

Project Scope

The audit covered the following files:

- AggregationRouterV5.sol
- ClipperRouter.sol
- GenericRouter.sol
- UnoswapRouter.sol
- UnoswapV3Router.sol
- Errors.sol
- OrderMixin.sol
- OrderRFQMixin.sol
- OrderLib.sol
- OrderRFQLib.sol
- AmountCalculator.sol
- NonceManager.sol
- PredicateHelper.sol
- ArgumentsDecoder.sol
- Callib.sol
- Errors.sol
- EthReceiver.sol
- StringUtil.sol
- UniERC20.sol
- SafeERC20.sol
- ECDSA.sol
- RevertReasonForwarder.sol

2. Finding Severity breakdown

All vulnerabilities discovered during the audit are classified based on its potential severity and has the following classification:

Severity	Description
Critical	Bugs leading to assets theft, fund access locking, or any other loss funds to be transferred to any party.
High	Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.
Medium	Bugs that can break the intended contract logic or expose it to DoS attacks, but do not cause direct loss funds.
Informational	Bugs that do not have a significant immediate impact and could be easily fixed.

Based on the feedback received from the Customer regarding the list of findings discovered by the Contractor, they are assigned the following statuses:

Status	Description
Fixed	Recommended fixes have been made to the project code and no longer affect its security.
Acknowledged	The Customer is aware of the finding. Recommendations for the finding are planned to be resolved in the future.

3. Summary of findings

Severity	# of Findings
Critical	0
High	0
Medium	0
Informational	16

4. Conclusion

Deployment

File name	Contract deployed on mainnet
contracts/AggregationRouterV5.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/routers/ClipperRouter.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/routers/GenericRouter.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/routers/UnoswapRouter.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/routers/UnoswapV3Router.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/helpers/Errors.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/OrderMixin.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/OrderRFQMixin.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/OrderLib.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/OrderRFQLib.sol	0x1111111254EEB25477B68fb85Ed929f73A960582

File name	Contract deployed on mainnet
contracts/helpers/AmountCalculator.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/helpers/NonceManager.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/helpers/PredicateHelper.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/ArgumentsDecoder.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/Callib.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/Errors.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/EthReceiver.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/StringUtil.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/UniERC20.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/SafeERC20.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/ECDSA.sol	0x1111111254EEB25477B68fb85Ed929f73A960582
contracts/libraries/RevertReasonForwarder.sol	0x1111111254EEB25477B68fb85Ed929f73A960582

5. Findings report

Informational

No check for zero address	Fixed at 5e682c

Description

In constructor at AggregationRouterV5.sol#L22 there is no check if `clipperExchange` address is zero.

Recommendation

We recommend to add check if `address(clipperExchange) == address(0)`

Unclear selectors	Fixed at 219486

Description

At the line UnoswapV3Router.sol#L26 the `_SELECTORS` constant stores selectors for `token0()`, `token1()`, `fee()`, `transfer()`, `transferFrom()` functions, but it is not immediately clear which selectors are stored in the variable.

Recommendation

It is recommended to add a comment to improve readability.

Indirect inheritance of receive()	Fixed at PR#161

Description

At the line OrderRFQMixin.sol#L231 the contract `OrderRFQMixin` receives ETH from the `WETH` contract, but it doesn't have a `receive()` function. `AggregationRouterV5` inherits `EthReceiver` from router contracts, so it is not an issue for it, but it might be for other contracts in the future that inherit from `OrderRFQMixin`.

Recommendation

It is recommended to inherit `EthReceiver` in the `OrderRFQMixin` contract.

Variable shadowing	Fixed at a0adeb

Description

At the line PredicateHelper.sol#L102 the variable `nonce` shadows the state variable `nonce` inherited from the `NonceManager` contract.

Recommendation

It is recommended to rename the variable to avoid shadowing.

Missing NatSpec comments	Fixed at PR#156

Description

At the lines:

- IOrderMixin.sol#L73
- IOrderMixin.sol#L98
- IOrderMixin.sol#L121

There are no NatSpec comments for parameter `interaction`.

At the line GenericRouter.sol#L41 there is no NatSpec comment for parameter `permit`.

Recommendation

It is recommended to add NatSpec comments where needed.

TODO comment in the source code	Fixed at c1aaf5

Description

At the line NotificationReceiver.sol#L6 there is a `TODO` comment.

Recommendation

It is recommended to remove `TODO` comments before deployment.

Typo in the function name	Fixed at 2d8931

Description

At the line UniERC20.sol#L62 there is a typo in `"SYBMOL()"`.

Recommendation

It is recommended to change to `"SYMBOL()"`.

Gas optimization by using constant selectors	Acknowledged

Description

At the lines:

- ClipperRouter.sol#L102-L103
- ClipperRouter.sol#L132
- ClipperRouter.sol#L157
- ClipperRouter.sol#L182
- ClipperRouter.sol#L208-L209
- ClipperRouter.sol#L231
- OrderMixin.sol#L310
- SafeERC20.sol#L21
- SafeERC20.sol#L41
- SafeERC20.sol#L48-L50
- ECDSA.sol#L110
- ECDSA.sol#L129
- ECDSA.sol#L152
- ECDSA.sol#L174

It is possible to save gas by using constant selectors.

Recommendation

It is recommended to use constant selectors to save gas.

Client's comments

> We decided to use Contract.function.selector notation instead of 4 byte constant to increase readability and rely on compile-time checks

Gas optimization by removing len variable	Fixed at 1be62a

Description

At the lines:

- ECDSA.sol#L114
- ECDSA.sol#L133
- ECDSA.sol#L156
- ECDSA.sol#L178

The `len` variable is unnecessary. It can be precomputed and written directly or computed inside the `staticcall()`.

Recommendation

It is recommended to remove the `len` variable.

Gas optimization by using assembly for external calls	Acknowledged

Description

At the lines:

- SafeERC20.sol#L58
- SafeERC20.sol#L64

In the contract `SafeERC20`, the external calls are written in assembly to save gas, except when getting allowance `token.allowance(address(this), spender)`. It is possible to save gas by doing these calls in assembly as well.

At the lines:

- UnoswapV3Router.sol#L101
- UnoswapV3Router.sol#L117

It is possible to save gas by making external calls to `_WETH` in assembly.

Recommendation

It is recommended to make external calls in assembly where possible.

Client's comments

> We don't really use safeIncreaseAllowance and safeDecreaseAllowance, so won't fix

Unnecessary imports	Fixed at 2034c9

Description

At the lines:

- OrderMixin.sol#L17
- AmountCalculator.sol#L6

The imported library `Callib` is not used.

At the line UniERC20.sol#L7 the imported library `RevertReasonForwarder` is not used.

Recommendation

It is recommended to remove these imports.

Unused error	Fixed at 105da7

Description

At the line UniERC20.sol#L18 there is an unused error `ERC20OperationFailed`.

Recommendation

It is recommended to remove this error.

Missing address zero check	Fixed at PR#33

Description

At the lines:

- ECDSA.sol#L80
- ECDSA.sol#L87
- ECDSA.sol#L94
- ECDSA.sol#L101

In the functions `recoverOrIsValidSignature`, if the address `signer == address(0)` and `recover()` returns `address(0)`, then the functions return `true`.

Recommendation

Consider returning `false` in this case.

Unnecessary return statement	Acknowledged

Description

At the line ClipperRouter.sol#L256 the function `clipperSwapTo()` returns `outputAmount`, but the value `outputAmount` is taken as a function parameter and it is not changed inside the function making the return statement unnecessary.

Recommendation

Consider removing the return statement to save gas.

Client's comments

Won't fix

More gas optimization	Acknowledged

Description

As AggregationRouterV5 working in pair with backend, it may be useful to change names of frequently called non-view functions for more gas optimization.

Recommendation

Make sure that selector of the most common functions will be on the top.

Client's comments

Won't fix for now

Different number systems in contracts	Fixed at 3b2700

Description

In some contracts you are using different number systems, mixing hexidecimal and decimal. In the future this may result in increasing time for review or updating contracts. Or it can lead to possible errors, working inside assembly{...} blocks. UnoswapV3Router.sol#L156 OrderMixin.sol#L320 SafeERC20.sol#L31 ...

Recommendation

Bring it all to one number system.

6. Appendix A. Linter

1inch-contract

Error/max-line-length

- contracts/libs/CallDescription.sol:58 - Line length must be no more than 100 but current length is 125.
- contracts/libs/CallDescription.sol:66 - Line length must be no more than 100 but current length is 125.
- contracts/libs/CallDescription.sol:67 - Line length must be no more than 100 but current length is 124.
- contracts/libs/CallDescription.sol:171 - Line length must be no more than 100 but current length is 128.
- contracts/libs/CallDescription.sol:176 - Line length must be no more than 100 but current length is 134.
- contracts/libs/CallDescription.sol:184 - Line length must be no more than 100 but current length is 141.
- contracts/routers/ClipperRouter.sol:50 - Line length must be no more than 100 but current length is 105.
- contracts/routers/ClipperRouter.sol:70 - Line length must be no more than 100 but current length is 115.
- contracts/routers/ClipperRouter.sol:130 - Line length must be no more than 100 but current length is 158.
- contracts/routers/ClipperRouter.sol:155 - Line length must be no more than 100 but current length is 138.
- contracts/routers/ClipperRouter.sol:180 - Line length must be no more than 100 but current length is 142.
- contracts/routers/ClipperRouter.sol:229 - Line length must be no more than 100 but current length is 146.
- contracts/routers/GenericRouter.sol:31 - Line length must be no more than 100 but current length is 115.
- contracts/routers/GenericRouter.sol:87 - Line length must be no more than 100 but current length is 121.
- contracts/routers/GenericRouter.sol:92 - Line length must be no more than 100 but current length is 112.
- contracts/routers/UnoswapRouter.sol:20 - Line length must be no more than 100 but current length is 114.
- contracts/routers/UnoswapRouter.sol:21 - Line length must be no more than 100 but current length is 114.
- contracts/routers/UnoswapRouter.sol:22 - Line length must be no more than 100 but current length is 114.
- contracts/routers/UnoswapRouter.sol:23 - Line length must be no more than 100 but current length is 114.
- contracts/routers/UnoswapRouter.sol:39 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapRouter.sol:60 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapRouter.sol:76 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapRouter.sol:108 - Line length must be no more than 100 but current length is 123.
- contracts/routers/UnoswapRouter.sol:119 - Line length must be no more than 100 but current length is 122.
- contracts/routers/UnoswapRouter.sol:130 - Line length must be no more than 100 but current length is 132.
- contracts/routers/UnoswapRouter.sol:148 - Line length must be no more than 100 but current length is 118.
- contracts/routers/UnoswapRouter.sol:178 - Line length must be no more than 100 but current length is 119.
- contracts/routers/UnoswapV3Router.sol:24 - Line length must be no more than 100 but current length is 119.
- contracts/routers/UnoswapV3Router.sol:25 - Line length must be no more than 100 but current length is 110.
- contracts/routers/UnoswapV3Router.sol:26 - Line length must be no more than 100 but current length is 109.
- contracts/routers/UnoswapV3Router.sol:27 - Line length must be no more than 100 but current length is 114.
- contracts/routers/UnoswapV3Router.sol:28 - Line length must be no more than 100 but current length is 120.
- contracts/routers/UnoswapV3Router.sol:30 - Line length must be no more than 100 but current length is 120.
- contracts/routers/UnoswapV3Router.sol:31 - Line length must be no more than 100 but current length is 101.
- contracts/routers/UnoswapV3Router.sol:44 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapV3Router.sol:62 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapV3Router.sol:76 - Line length must be no more than 100 but current length is 106.
- contracts/routers/UnoswapV3Router.sol:104 - Line length must be no more than 100 but current length is 119.
- contracts/routers/UnoswapV3Router.sol:109 - Line length must be no more than 100 but current length is 128.
- contracts/routers/UnoswapV3Router.sol:111 - Line length must be no more than 100 but current length is 144.
- contracts/routers/UnoswapV3Router.sol:144 - Line length must be no more than 100 but current length is 123.
- contracts/routers/UnoswapV3Router.sol:156 - Line length must be no more than 100 but current length is 103.
- contracts/routers/UnoswapV3Router.sol:159 - Line length must be no more than 100 but current length is 103.
- contracts/routers/UnoswapV3Router.sol:180 - Line length must be no more than 100 but current length is 107.

- contracts/routers/UnoswapV3Router.sol:207 - Line length must be no more than 100 but current length is 114.

Error/code-complexity

- contracts/routers/ClipperRouter.sol:83 - Function has cyclomatic complexity 9 but allowed no more than 5
- contracts/routers/GenericRouter.sol:38 - Function has cyclomatic complexity 12 but allowed no more than 5
- contracts/routers/UnoswapV3Router.sol:86 - Function has cyclomatic complexity 8 but allowed no more than 5

Error/function-max-lines

- contracts/libs/CallDescription.sol:54 - Function body contains 165 lines but allowed no more than 40 lines
- contracts/routers/ClipperRouter.sol:83 - Function body contains 173 lines but allowed no more than 40 lines
- contracts/routers/GenericRouter.sol:38 - Function body contains 60 lines but allowed no more than 40 lines
- contracts/routers/UnoswapRouter.sol:86 - Function body contains 154 lines but allowed no more than 40 lines
- contracts/routers/UnoswapV3Router.sol:124 - Function body contains 80 lines but allowed no more than 40 lines

limit-order-protocol

Error/max-line-length

- contracts/helpers/AmountCalculator.sol:14 - Line length must be no more than 100 but current length is 136.
- contracts/helpers/AmountCalculator.sol:20 - Line length must be no more than 100 but current length is 136.
- contracts/helpers/ChainlinkCalculator.sol:21 - Line length must be no more than 100 but current length is 105.
- contracts/helpers/ChainlinkCalculator.sol:26 - Line length must be no more than 100 but current length is 129.
- contracts/helpers/ChainlinkCalculator.sol:31 - Line length must be no more than 100 but current length is 112.
- contracts/helpers/ChainlinkCalculator.sol:33 - Line length must be no more than 100 but current length is 112.
- contracts/helpers/ChainlinkCalculator.sol:39 - Line length must be no more than 100 but current length is 173.
- contracts/helpers/ChainlinkCalculator.sol:44 - Line length must be no more than 100 but current length is 149.
- contracts/helpers/ChainlinkCalculator.sol:46 - Line length must be no more than 100 but current length is 152.
- contracts/helpers/ChainlinkCalculator.sol:48 - Line length must be no more than 100 but current length is 113.
- contracts/helpers/ERC1155Proxy.sol:18 - Line length must be no more than 100 but current length is 113.
- contracts/helpers/ERC1155Proxy.sol:21 - Line length must be no more than 100 but current length is 112.
- contracts/helpers/ERC1155Proxy.sol:22 - Line length must be no more than 100 but current length is 115.
- contracts/helpers/ERC1155Proxy.sol:23 - Line length must be no more than 100 but current length is 151.
- contracts/helpers/ERC721Proxy.sol:18 - Line length must be no more than 100 but current length is 111.
- contracts/helpers/ERC721Proxy.sol:21 - Line length must be no more than 100 but current length is 108.
- contracts/helpers/ERC721Proxy.sol:22 - Line length must be no more than 100 but current length is 115.
- contracts/helpers/ERC721Proxy.sol:23 - Line length must be no more than 100 but current length is 109.
- contracts/helpers/ERC721Proxy.sol:24 - Line length must be no more than 100 but current length is 135.
- contracts/helpers/ERC721ProxySafe.sol:18 - Line length must be no more than 100 but current length is 119.
- contracts/helpers/ERC721ProxySafe.sol:21 - Line length must be no more than 100 but current length is 108.
- contracts/helpers/ERC721ProxySafe.sol:22 - Line length must be no more than 100 but current length is 115.
- contracts/helpers/ERC721ProxySafe.sol:23 - Line length must be no more than 100 but current length is 108.
- contracts/helpers/ERC721ProxySafe.sol:24 - Line length must be no more than 100 but current length is 135.
- contracts/helpers/PredicateHelper.sol:17 - Line length must be no more than 100 but current length is 116.
- contracts/helpers/PredicateHelper.sol:72 - Line length must be no more than 100 but current length is 105.
- contracts/helpers/PredicateHelper.sol:80 - Line length must be no more than 100 but current length is 106.
- contracts/helpers/SeriesNonceManager.sol:37 - Line length must be no more than 100 but current length is 110.

- contracts/helpers/WethUnwrapper.sol:25 - Line length must be no more than 100 but current length is 110.
- contracts/helpers/WhitelistChecker.sol:33 - Line length must be no more than 100 but current length is 120.
- contracts/helpers/WhitelistChecker.sol:36 - Line length must be no more than 100 but current length is 106.
- contracts/interfaces/IOrderMixin.sol:27 - Line length must be no more than 100 but current length is 108.
- contracts/interfaces/IOrderMixin.sol:32 - Line length must be no more than 100 but current length is 110.
- contracts/interfaces/IOrderMixin.sol:44 - Line length must be no more than 100 but current length is 119.
- contracts/interfaces/IOrderMixin.sol:57 - Line length must be no more than 100 but current length is 116.
- contracts/interfaces/IOrderMixin.sol:60 - Line length must be no more than 100 but current length is 110.
- contracts/interfaces/IOrderMixin.sol:65 - Line length must be no more than 100 but current length is 144.
- contracts/interfaces/IOrderMixin.sol:77 - Line length must be no more than 100 but current length is 106.
- contracts/interfaces/IOrderMixin.sol:88 - Line length must be no more than 100 but current length is 144.
- contracts/interfaces/IOrderMixin.sol:90 - Line length must be no more than 100 but current length is 103.
- contracts/interfaces/IOrderMixin.sol:112 - Line length must be no more than 100 but current length is 144.
- contracts/interfaces/IOrderMixin.sol:126 - Line length must be no more than 100 but current length is 106.
- contracts/interfaces/NotificationReceiver.sol:8 - Line length must be no more than 100 but current length is 103.
- contracts/libraries/ArgumentsDecoder.sol:10 - Line length must be no more than 100 but current length is 102.
- contracts/libraries/ArgumentsDecoder.sol:26 - Line length must be no more than 100 but current length is 117.
- contracts/libraries/ArgumentsDecoder.sol:35 - Line length must be no more than 100 but current length is 118.
- contracts/libraries/Callib.sol:8 - Line length must be no more than 100 but current length is 119.
- contracts/LimitOrderProtocol.sol:16 - Line length must be no more than 100 but current length is 223.
- contracts/LimitOrderProtocol.sol:19 - Line length must be no more than 100 but current length is 180.
- contracts/mocks/CallsSimulator.sol:14 - Line length must be no more than 100 but current length is 119.
- contracts/mocks/ContractRFQ.sol:73 - Line length must be no more than 100 but current length is 110.
- contracts/mocks/EIP712Alien.sol:8 - Line length must be no more than 100 but current length is 119.
- contracts/mocks/EIP712Alien.sol:10 - Line length must be no more than 100 but current length is 116.
- contracts/mocks/EIP712Alien.sol:11 - Line length must be no more than 100 but current length is 116.
- contracts/mocks/EIP712Alien.sol:14 - Line length must be no more than 100 but current length is 116.
- contracts/mocks/EIP712Alien.sol:15 - Line length must be no more than 100 but current length is 104.
- contracts/mocks/EIP712Alien.sol:18 - Line length must be no more than 100 but current length is 119.
- contracts/mocks/EIP712Alien.sol:21 - Line length must be no more than 100 but current length is 114.
- contracts/mocks/EIP712Alien.sol:28 - Line length must be no more than 100 but current length is 120.
- contracts/mocks/EIP712Alien.sol:45 - Line length must be no more than 100 but current length is 105.
- contracts/mocks/EIP712Alien.sol:48 - Line length must be no more than 100 but current length is 113.
- contracts/mocks/EIP712Alien.sol:54 - Line length must be no more than 100 but current length is 123.
- contracts/mocks/EIP712Alien.sol:59 - Line length must be no more than 100 but current length is 101.
- contracts/mocks/EIP712Alien.sol:74 - Line length must be no more than 100 but current length is 131.
- contracts/mocks/EIP712Alien.sol:87 - Line length must be no more than 100 but current length is 113.
- contracts/mocks/EIP712Alien.sol:90 - Line length must be no more than 100 but current length is 106.
- contracts/mocks/HashChecker.sol:22 - Line length must be no more than 100 but current length is 103.
- contracts/mocks/HashChecker.sol:43 - Line length must be no more than 100 but current length is 120.
- contracts/mocks/HashChecker.sol:46 - Line length must be no more than 100 but current length is 106.
- contracts/mocks/RecursiveMatcher.sol:60 - Line length must be no more than 100 but current length is 107.
- contracts/OrderLib.sol:20 - Line length must be no more than 100 but current length is 115.
- contracts/OrderLib.sol:21 - Line length must be no more than 100 but current length is 115.
- contracts/OrderLib.sol:23 - Line length must be no more than 100 but current length is 110.
- contracts/OrderLib.sol:26 - Line length must be no more than 100 but current length is 155.
- contracts/OrderLib.sol:103 - Line length must be no more than 100 but current length is 104.
- contracts/OrderLib.sol:110 - Line length must be no more than 100 but current length is 117.
- contracts/OrderMixin.sol:22 - Line length must be no more than 100 but current length is 102.
- contracts/OrderMixin.sol:94 - Line length must be no more than 100 but current length is 115.
- contracts/OrderMixin.sol:116 - Line length must be no more than 100 but current length is 117.
- contracts/OrderMixin.sol:136 - Line length must be no more than 100 but current length is 125.
- contracts/OrderMixin.sol:137 - Line length must be no more than 100 but current length is 115.
- contracts/OrderMixin.sol:152 - Line length must be no more than 100 but current length is 117.

- contracts/OrderMixin.sol:158 - Line length must be no more than 100 but current length is 111.
- contracts/OrderMixin.sol:172 - Line length must be no more than 100 but current length is 105.
- contracts/OrderMixin.sol:182 - Line length must be no more than 100 but current length is 106.
- contracts/OrderMixin.sol:185 - Line length must be no more than 100 but current length is 107.
- contracts/OrderMixin.sol:211 - Line length must be no more than 100 but current length is 168.
- contracts/OrderMixin.sol:214 - Line length must be no more than 100 but current length is 119.
- contracts/OrderMixin.sol:216 - Line length must be no more than 100 but current length is 168.
- contracts/OrderMixin.sol:219 - Line length must be no more than 100 but current length is 172.
- contracts/OrderMixin.sol:223 - Line length must be no more than 100 but current length is 118.
- contracts/OrderMixin.sol:238 - Line length must be no more than 100 but current length is 123.
- contracts/OrderMixin.sol:240 - Line length must be no more than 100 but current length is 129.
- contracts/OrderMixin.sol:255 - Line length must be no more than 100 but current length is 112.
- contracts/OrderMixin.sol:256 - Line length must be no more than 100 but current length is 114.
- contracts/OrderMixin.sol:272 - Line length must be no more than 100 but current length is 108.
- contracts/OrderMixin.sol:287 - Line length must be no more than 100 but current length is 124.
- contracts/OrderMixin.sol:289 - Line length must be no more than 100 but current length is 130.
- contracts/OrderMixin.sol:309 - Line length must be no more than 100 but current length is 141.
- contracts/OrderMixin.sol:321 - Line length must be no more than 100 but current length is 112.
- contracts/OrderMixin.sol:325 - Line length must be no more than 100 but current length is 200.
- contracts/OrderMixin.sol:330 - Line length must be no more than 100 but current length is 111.
- contracts/OrderMixin.sol:333 - Line length must be no more than 100 but current length is 200.
- contracts/OrderMixin.sol:338 - Line length must be no more than 100 but current length is 111.
- contracts/OrderMixin.sol:341 - Line length must be no more than 100 but current length is 195.
- contracts/OrderMixin.sol:352 - Line length must be no more than 100 but current length is 128.
- contracts/OrderRFQLib.sol:30 - Line length must be no more than 100 but current length is 105.
- contracts/OrderRFQMixin.sol:47 - Line length must be no more than 100 but current length is 113.
- contracts/OrderRFQMixin.sol:52 - Line length must be no more than 100 but current length is 110.
- contracts/OrderRFQMixin.sol:82 - Line length must be no more than 100 but current length is 125.
- contracts/OrderRFQMixin.sol:106 - Line length must be no more than 100 but current length is 107.
- contracts/OrderRFQMixin.sol:116 - Line length must be no more than 100 but current length is 107.
- contracts/OrderRFQMixin.sol:120 - Line length must be no more than 100 but current length is 103.
- contracts/OrderRFQMixin.sol:122 - Line length must be no more than 100 but current length is 101.
- contracts/OrderRFQMixin.sol:125 - Line length must be no more than 100 but current length is 105.
- contracts/OrderRFQMixin.sol:128 - Line length must be no more than 100 but current length is 102.
- contracts/OrderRFQMixin.sol:140 - Line length must be no more than 100 but current length is 103.
- contracts/OrderRFQMixin.sol:152 - Line length must be no more than 100 but current length is 117.
- contracts/OrderRFQMixin.sol:158 - Line length must be no more than 100 but current length is 101.
- contracts/OrderRFQMixin.sol:172 - Line length must be no more than 100 but current length is 105.
- contracts/OrderRFQMixin.sol:175 - Line length must be no more than 100 but current length is 119.
- contracts/OrderRFQMixin.sol:176 - Line length must be no more than 100 but current length is 101.
- contracts/OrderRFQMixin.sol:178 - Line length must be no more than 100 but current length is 109.
- contracts/OrderRFQMixin.sol:194 - Line length must be no more than 100 but current length is 109.
- contracts/OrderRFQMixin.sol:200 - Line length must be no more than 100 but current length is 128.
- contracts/OrderRFQMixin.sol:232 - Line length must be no more than 100 but current length is 115.

Error/ordering

- contracts/helpers/NonceManager.sol:10 - Function order is incorrect, state variable declaration can not go after event definition (line 8)
- contracts/helpers/SeriesNonceManager.sol:21 - Function order is incorrect, state variable declaration can not go after event definition (line 8)
- contracts/interfaces/IOrderMixin.sol:48 - Function order is incorrect, external function can not go after external view function (line 41)

- contracts/mocks/EIP712Alien.sol:101 - Function order is incorrect, internal view function can not go after private view function (line 74)
- contracts/mocks/WhitelistRegistryMock.sol:19 - Function order is incorrect, external view function can not go after public function (line 15)
- contracts/OrderLib.sol:44 - Function order is incorrect, enum definition can not go after state variable declaration (line 29)

Error/code-complexity

- contracts/helpers/PredicateHelper.sol:107 - Function has cyclomatic complexity 6 but allowed no more than 5
- contracts/OrderMixin.sol:164 - Function has cyclomatic complexity 26 but allowed no more than 5
- contracts/OrderRFQMixin.sol:111 - Function has cyclomatic complexity 6 but allowed no more than 5
- contracts/OrderRFQMixin.sol:184 - Function has cyclomatic complexity 14 but allowed no more than 5

Error/function-max-lines

- contracts/OrderMixin.sol:164 - Function body contains 127 lines but allowed no more than 40 lines
- contracts/OrderRFQMixin.sol:184 - Function body contains 62 lines but allowed no more than 40 lines

solidity-utils

Error/max-line-length

- contracts/interfaces/IDaiLikePermit.sol:8 - Line length must be no more than 100 but current length is 138.
- contracts/libraries/AddressArray.sol:29 - Line length must be no more than 100 but current length is 102.
- contracts/libraries/AddressArray.sol:33 - Line length must be no more than 100 but current length is 126.
- contracts/libraries/ECDSA.sol:9 - Line length must be no more than 100 but current length is 105.
- contracts/libraries/ECDSA.sol:63 - Line length must be no more than 100 but current length is 114.
- contracts/libraries/ECDSA.sol:79 - Line length must be no more than 100 but current length is 132.
- contracts/libraries/ECDSA.sol:80 - Line length must be no more than 100 but current length is 103.
- contracts/libraries/ECDSA.sol:86 - Line length must be no more than 100 but current length is 137.
- contracts/libraries/ECDSA.sol:93 - Line length must be no more than 100 but current length is 129.
- contracts/libraries/ECDSA.sol:100 - Line length must be no more than 100 but current length is 131.
- contracts/libraries/ECDSA.sol:107 - Line length must be no more than 100 but current length is 123.
- contracts/libraries/ECDSA.sol:108 - Line length must be no more than 100 but current length is 142.
- contracts/libraries/ECDSA.sol:109 - Line length must be no more than 100 but current length is 114.
- contracts/libraries/ECDSA.sol:128 - Line length must be no more than 100 but current length is 128.
- contracts/libraries/ECDSA.sol:149 - Line length must be no more than 100 but current length is 120.
- contracts/libraries/ECDSA.sol:150 - Line length must be no more than 100 but current length is 156.
- contracts/libraries/ECDSA.sol:151 - Line length must be no more than 100 but current length is 114.
- contracts/libraries/ECDSA.sol:171 - Line length must be no more than 100 but current length is 122.
- contracts/libraries/ECDSA.sol:172 - Line length must be no more than 100 but current length is 195.
- contracts/libraries/ECDSA.sol:173 - Line length must be no more than 100 but current length is 114.
- contracts/libraries/ECDSA.sol:199 - Line length must be no more than 100 but current length is 127.
- contracts/libraries/ECDSA.sol:205 - Line length must be no more than 100 but current length is 111.
- contracts/libraries/ECDSA.sol:210 - Line length must be no more than 100 but current length is 105.
- contracts/libraries/RevertReasonParser.sol:10 - Line length must be no more than 100 but current length is 103.
- contracts/libraries/SafeERC20.sol:32 - Line length must be no more than 100 but current length is 112.
- contracts/libraries/SafeERC20.sol:86 - Line length must be no more than 100 but current length is 110.

- contracts/libraries/SafeERC20.sol:105 - Line length must be no more than 100 but current length is 111.
- contracts/libraries/StringUtil.sol:22 - Line length must be no more than 100 but current length is 107.
- contracts/libraries/StringUtil.sol:26 - Line length must be no more than 100 but current length is 108.
- contracts/libraries/StringUtil.sol:30 - Line length must be no more than 100 but current length is 108.
- contracts/libraries/StringUtil.sol:34 - Line length must be no more than 100 but current length is 107.
- contracts/libraries/StringUtil.sol:37 - Line length must be no more than 100 but current length is 108.
- contracts/libraries/StringUtil.sol:38 - Line length must be no more than 100 but current length is 107.
- contracts/libraries/StringUtil.sol:44 - Line length must be no more than 100 but current length is 116.
- contracts/libraries/StringUtil.sol:58 - Line length must be no more than 100 but current length is 123.
- contracts/libraries/UniERC20.sol:45 - Line length must be no more than 100 but current length is 103.
- contracts/libraries/UniERC20.sol:75 - Line length must be no more than 100 but current length is 143.
- contracts/mocks/DaiLikePermitMock.sol:8 - Line length must be no more than 100 but current length is 143.
- contracts/mocks/DaiLikePermitMock.sol:9 - Line length must be no more than 100 but current length is 113.
- contracts/mocks/DaiLikePermitMock.sol:20 - Line length must be no more than 100 but current length is 137.
- contracts/mocks/ERC1271WalletMock.sol:14 - Line length must be no more than 100 but current length is 120.
- contracts/mocks/ERC1271WalletMock.sol:15 - Line length must be no more than 100 but current length is 102.
- contracts/mocks/SafeERC20Helper.sol:13 - Line length must be no more than 100 but current length is 118.
- contracts/mocks/SafeERC20Helper.sol:37 - Line length must be no more than 100 but current length is 103.
- contracts/mocks/SafeERC20Helper.sol:45 - Line length must be no more than 100 but current length is 118.
- contracts/mocks/SafeERC20Helper.sol:80 - Line length must be no more than 100 but current length is 118.
- contracts/mocks/SafeERC20Helper.sol:138 - Line length must be no more than 100 but current length is 120.
- contracts/tests/ECDSATest.sol:9 - Line length must be no more than 100 but current length is 111.
- contracts/tests/ECDSATest.sol:14 - Line length must be no more than 100 but current length is 102.
- contracts/tests/ECDSATest.sol:22 - Line length must be no more than 100 but current length is 132.
- contracts/tests/ECDSATest.sol:27 - Line length must be no more than 100 but current length is 143.
- contracts/tests/ECDSATest.sol:32 - Line length must be no more than 100 but current length is 134.
- contracts/tests/ECDSATest.sol:36 - Line length must be no more than 100 but current length is 131.
- contracts/tests/ECDSATest.sol:40 - Line length must be no more than 100 but current length is 123.
- contracts/tests/ECDSATest.sol:45 - Line length must be no more than 100 but current length is 134.
- contracts/tests/ECDSATest.sol:50 - Line length must be no more than 100 but current length is 125.
- contracts/tests/ECDSATest.sol:54 - Line length must be no more than 100 but current length is 122.
- contracts/tests/ECDSATest.sol:62 - Line length must be no more than 100 but current length is 111.
- contracts/tests/RevertReasonParserTest.sol:29 - Line length must be no more than 100 but current length is 101.
- contracts/tests/RevertReasonParserTest.sol:49 - Line length must be no more than 100 but current length is 107.
- contracts/tests/RevertReasonParserTest.sol:53 - Line length must be no more than 100 but current length is 130.
- contracts/tests/RevertReasonParserTest.sol:71 - Line length must be no more than 100 but current length is 102.
- contracts/tests/RevertReasonParserTest.sol:77 - Line length must be no more than 100 but current length is 105.
- contracts/tests/RevertReasonParserTest.sol:78 - Line length must be no more than 100 but current length is 109.
- contracts/tests/StringUtilTest.sol:11 - Line length must be no more than 100 but current length is 128.
- contracts/tests/StringUtilTest.sol:15 - Line length must be no more than 100 but current length is 137.
- contracts/tests/StringUtilTest.sol:19 - Line length must be no more than 100 but current length is 133.
- contracts/tests/StringUtilTest.sol:23 - Line length must be no more than 100 but current length is 142.

Error/ordering

- contracts/libraries/AddressSet.sol:28 - Function order is incorrect, internal function can not go after internal view function (line 24)
- contracts/mocks/AddressArrayMock.sol:25 - Function order is incorrect, external function can not go after external view function (line 21)
- contracts/mocks/AddressSetMock.sol:25 - Function order is incorrect, external function can not go after external view function (line 21)
- contracts/mocks/SafeERC20Helper.sol:175 - Function order is incorrect, external function can not go after public function (line 171)

Error/function-max-lines

- contracts/libraries/StringUtil.sol:16 - Function body contains 59 lines but allowed no more than 40 lines

Error/code-complexity

- contracts/libraries/UniERC20.sol:45 - Function has cyclomatic complexity 7 but allowed no more than 5
- contracts/libraries/UniERC20.sol:75 - Function has cyclomatic complexity 8 but allowed no more than 5

7. Appendix B. Slither

Informational/High/assembly

SafeERC20.safeTransferFrom(IERC20,address,address,uint256) uses assembly - INLINE ASM

ECDSA.toTypedDataHash(bytes32,bytes32) uses assembly - INLINE ASM

UniERC20._uniDecode(IERC20,string,string) uses assembly - INLINE ASM

ECDSA.isValidSignature(address,bytes32,bytes) uses assembly - INLINE ASM

RevertReasonParser.parse(bytes,string) uses assembly - INLINE ASM - INLINE ASM - INLINE ASM

ECDSA.isValidSignature(address,bytes32,bytes32,bytes32) uses assembly - INLINE ASM

RevertReasonForwarder.reRevert() uses assembly - INLINE ASM

ECDSA.toEthSignedMessageHash(bytes32) uses assembly - INLINE ASM

SafeERC20._makeCalldataCall(IERC20,bytes4,bytes) uses assembly - INLINE ASM

ECDSA.isValidSignature65(address,bytes32,bytes32,bytes32) uses assembly - INLINE ASM

ECDSA.recover(bytes32,uint8,bytes32,bytes32) uses assembly - INLINE ASM

ECDSA.recover(bytes32,bytes32,bytes32) uses assembly - INLINE ASM

ECDSA.isValidSignature(address,bytes32,uint8,bytes32,bytes32) uses assembly - INLINE ASM

ECDSA.recover(bytes32,bytes) uses assembly - INLINE ASM

RevertReasonParserTest.testParseWithThrow() uses assembly - INLINE ASM

SafeERC20._makeCall(IERC20,bytes4,address,uint256) uses assembly - INLINE ASM

StringUtil.toHex(bytes) uses assembly - INLINE ASM

StringUtil.toHex.asm_0._toHex16() uses assembly - INLINE ASM

Informational/High/low-level-calls

Low level call in UniERC20._uniDecode(IERC20,string,string): - (success,data) = address(token).staticcall{gas: 20000}(abi.encodeWithSignature(lowerCaseSignature)) - (success,data) = address(token).staticcall{gas: 20000}(abi.encodeWithSignature(upperCaseSignature))

Informational/High/missing-inheritance

DaiLikePermitMock should inherit from IDaiLikePermit

Informational/High/naming-convention

Function ECDSATest.isValidSignature_v_r_s(address,bytes32,uint8,bytes32,bytes32) is not in mixedCase

Function ECDSATest.isValidSignature_r_vs(address,bytes32,bytes32,bytes32) is not in mixedCase

Function ECDSATest.recoverOrIsValidSignature_v_r_s(address,bytes32,uint8,bytes32,bytes32) is not in mixedCase

Function ECDSATest.recover_r_vs(bytes32,bytes32,bytes32) is not in mixedCase

Function ECDSATest.recoverOrIsValidSignature_r_vs(address,bytes32,bytes32,bytes32) is not in mixedCase

Function ECDSATest.recover_v_r_s(bytes32,uint8,bytes32,bytes32) is not in mixedCase

Variable OnlyWethReceiver._WETH is not in mixedCase

Informational/High/unused-state

ERC20ReturnFalseMock._allowance is never used in ERC20ReturnFalseMock

Informational/Medium/dead-code

UniERC20.uniTransfer(IERC20,address,uint256) is never used and should be removed

UniERC20.uniSymbol(IERC20) is never used and should be removed

UniERC20.uniBalanceOf(IERC20,address) is never used and should be removed

StringUtil.toHex(address) is never used and should be removed

UniERC20.uniApprove(IERC20,address,uint256) is never used and should be removed

UniERC20.uniName(IERC20) is never used and should be removed

UniERC20.uniTransferFrom(IERC20,address,address,uint256) is never used and should be removed

UniERC20.isETH(IERC20) is never used and should be removed

UniERC20._uniDecode(IERC20,string,string) is never used and should be removed

AddressArray.get(AddressArray.Data,address[]) is never used and should be removed

Informational/Medium/too-many-digits

StringUtil.toHex.asm_0._toHex16() uses literals with too many digits: - output_toHex_asm_0__toHex16 = output_toHex_asm_0__toHex16 & 0xFFFFFFFF000000000000000000000000FFFFFFFF000000000000000000000000 | output_toHex_asm_0__toHex16 & 0x00000000FFFFFFFF000000000000000000000000FFFFFFFF000000000000000000000000 >> 32

StringUtil.toHex.asm_0._toHex16() uses literals with too many digits: - output_toHex_asm_0__toHex16 = input_toHex_asm_0__toHex16 & 0xFFFFFFFFFFFFFFFF000000000000000000000000000000000000000000000000 | input_toHex_asm_0__toHex16 & 0x0000000000000000FFFFFFFFFFFFFFFF000000000000000000000000000000000000000000000000 >> 64

StringUtil.toHex(bytes) uses literals with too many digits: - mstore(uint256,uint256)(toPtr_toHex_asm_0,0x3078000000000000000000000000000000000000000000000000000000000000)

StringUtil.toHex.asm_0._toHex16() uses literals with too many digits: - output_toHex_asm_0__toHex16 = output_toHex_asm_0__toHex16 & 0xFF00000000FF00000000FF00000000FF00000000FF00000000FF00000000FF000000 | output_toHex_asm_0__toHex16 & 0x00FF00000000FF00000000FF00000000FF00000000FF00000000FF00000000FF0000 >> 8

ECDSA.toTypedDataHash(bytes32,bytes32) uses literals with too many digits: - mstore(uint256,uint256)(ptr_toTypedDataHash_asm_0,0x1901000000000000000000000000000000000000000000000000000000000000)

RevertReasonParserTest.testAssertion() uses literals with too many digits: - _test(this.assertion,Panic(0x0000000000000000000000000000000000000000000000000000000000000001))

StringUtil.toHex.asm_0._toHex16() uses literals with too many digits: - output_toHex_asm_0__toHex16 = output_toHex_asm_0__toHex16 & 0xFFFF0000000000000000FFFF0000000000000000FFFF0000000000000000 | output_toHex_asm_0__toHex16 & 0x0000FFFF0000000000000000FFFF0000000000000000FFFF0000000000000000 >> 16

ECDSA.toEthSignedMessageHash(bytes32) uses literals with too many digits: - mstore(uint256,uint256)(0,0x19457468657265756d205369676e6564204d6573736167653a0a333200000000)

Low/High/variable-scope

Variable 'RevertReasonParserTest._test(function(),string).reason' in RevertReasonParserTest._test(function(),string) potentially used before declaration: parsedReason = RevertReasonParser.parse(reason,)

Variable 'RevertReasonParserTest.testParseWithThrow().reason' in RevertReasonParserTest.testParseWithThrow() potentially used before declaration: RevertReasonParser.parse(reason,)

Variable 'RevertReasonParserTest.testParseWithThrow().reason' in RevertReasonParserTest.testParseWithThrow() potentially used before declaration: mstore(uint256,uint256)(reason,mload(uint256)(reason) - 0x20)

Variable 'UniERC20._uniDecode(IERC20,string,string).len' in UniERC20._uniDecode(IERC20,string,string) potentially used before declaration: mstore(uint256,uint256)(data,len)

Low/Medium/timestamp

DaiLikePermitMock.permit(address,address,uint256,uint256,bool,uint8,bytes32,bytes32) uses timestamp for comparisons Dangerous comparisons: - require(bool,string)(expiry == 0 || block.timestamp <= expiry,Dai/permit-expired)

Medium/High/erc20-interface

ERC20NoReturnMock has incorrect ERC20 function interface:ERC20NoReturnMock.approve(address,uint256)

ERC20NoReturnMock has incorrect ERC20 function interface:ERC20NoReturnMock.transferFrom(address,address,uint256)

ERC20NoReturnMock has incorrect ERC20 function interface:ERC20NoReturnMock.transfer(address,uint256)

Medium/High/locked-ether

Contract locking ether found: Contract EthReceiver has payable functions: - EthReceiver.receive() But does not have a function to withdraw the ether

Contract locking ether found: Contract ERC20PermitMock has payable functions: - ERC20PermitMock.constructor(string,string,address,uint256) But does not have a function to withdraw the ether

Contract locking ether found: Contract DaiLikePermitMock has payable functions: - DaiLikePermitMock.constructor(string,string,address,uint256) But does not have a function to withdraw the ether

Contract locking ether found: Contract OnlyWethReceiver has payable functions: - OnlyWethReceiver.receive() But does not have a function to withdraw the ether

Medium/Medium/uninitialized-local

RevertReasonParserTest._test(function(),string).reason is a local variable never initialized

SafeERC20.safePermit(IERC20,bytes).success is a local variable never initialized

Medium/Medium/unused-return

RevertReasonParserTest.testParseWithThrow() ignores return value by RevertReasonParser.parse(reason,)

Optimization/High/constable-states

ERC20ReturnFalseMock._allowance should be constant

Optimization/High/external-function

allowance(address,address) should be declared external: - ERC20ReturnTrueMock.allowance(address,address)

allowance(address,address) should be declared external: - ERC20ReturnFalseMock.allowance(address,address)

decreaseAllowance(uint256) should be declared external: - SafeERC20Wrapper.decreaseAllowance(uint256)

transferFrom(address,address,uint256) should be declared external: - ERC20NoReturnMock.transferFrom(address,address,uint256)

transfer(address,uint256) should be declared external: - ERC20NoReturnMock.transfer(address,uint256)

allowance() should be declared external: - SafeERC20Wrapper.allowance()

transferFrom(address,address,uint256) should be declared external: - ERC20ReturnFalseMock.transferFrom(address,address,uint256)

approve(address,uint256) should be declared external: - ERC20ReturnTrueMock.approve(address,uint256)

increaseAllowance(uint256) should be declared external: - SafeERC20Wrapper.increaseAllowance(uint256)

isValidSignature(bytes32,bytes) should be declared external: - ERC1271WalletMock.isValidSignature(bytes32,bytes)

setAllowance(uint256) should be declared external: - ERC20ReturnTrueMock.setAllowance(uint256)

approve(address,uint256) should be declared external: - ERC20ReturnFalseMock.approve(address,uint256)

permitThatMayRevert(address,address,uint256,uint256,uint8,bytes32,bytes32) should be declared external: - ERC20PermitNoRevertMock.permitThatMayRevert(address,address,uint256,uint256,uint8,bytes32,bytes32)

approve(address,uint256) should be declared external: - ERC20NoReturnMock.approve(address,uint256)

allowance(address,address) should be declared external: - ERC20NoReturnMock.allowance(address,address)

transfer() should be declared external: - SafeERC20Wrapper.transfer()

approve(uint256) should be declared external: - SafeERC20Wrapper.approve(uint256)

setAllowance(uint256) should be declared external: - ERC20NoReturnMock.setAllowance(uint256)

transfer(address,uint256) should be declared external: - ERC20ReturnTrueMock.transfer(address,uint256)

transferFrom() should be declared external: - SafeERC20Wrapper.transferFrom()

setAllowance(uint256) should be declared external: - SafeERC20Wrapper.setAllowance(uint256)

transfer(address,uint256) should be declared external: - ERC20ReturnFalseMock.transfer(address,uint256)

transferFrom(address,address,uint256) should be declared external: - ERC20ReturnTrueMock.transferFrom(address,address,uint256)

8. Appendix C. Tests

1inch-contract

Tests result

```
70 passing (2m)
6 pending
```

Tests coverage

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\	8.33	16.67	14.29	8.33	
AggregationRouterV5.sol	33.33	50	33.33	33.33	32,36
WhitelistRegistrySimple.sol	0	0	0	0	... 32,33,34,38
contracts\executors\	69.23	50	71.43	68.75	
AggregationExecutorBase.sol	100	100	100	100	
AggregationExecutorProtected.sol	100	100	100	100	
AggregationExecutorSimple.sol	100	100	100	100	
AggregationExecutorWhitelist.sol	0	0	0	0	15,21,22,25,26
contracts\extensions\	69.44	47.92	65.79	69.38	
DodoExtension.sol	52.38	41.67	62.5	50	... 176,177,178
FlashbotsExtension.sol	11.11	0	25	11.11	... 58,59,60,61
KyberDMMExtension.sol	78.57	50	100	78.57	35,36,46
LeftoversExtension.sol	100	87.5	100	100	
LimitedAmountExtension.sol	0	0	0	0	... 26,27,28,29
PatcherExtension.sol	90.91	40	87.5	89.74	15,55,56,85
RouteWrapperExtension.sol	100	100	100	100	

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
SafeERC20Extension.sol	60	100	66.67	60	17,18
UniswapV2Extension.sol	100	100	100	100	
UniswapV3Extension.sol	71.43	100	60	77.78	79,84
contracts\helpers\	100	100	100	100	
Errors.sol	100	100	100	100	
contracts\helpers\dodo\	73.68	60	77.78	74.47	
DecimalMath.sol	88.89	100	80	85.71	22,23
DodoMath.sol	68.97	50	66.67	68.75	... 74,75,92,98
Sqrt.sol	100	100	100	100	
contracts\libs\	100	100	100	100	
CallDescription.sol	100	100	100	100	
contracts\routers\	66.3	48.15	76.47	66.34	
ClipperRouter.sol	6.45	0	25	5.88	... 231,233,256
GenericRouter.sol	96.15	59.09	100	96.55	59
UnoswapRouter.sol	80	50	75	83.33	68
UnoswapV3Router.sol	100	85.71	100	100	
All files	66.56	47.54	65.82	67.06	

limit-order-protocol

Tests result

```
100 passing (1m)
```

Tests coverage

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\	89.08	72.03	85.37	88.46	
LimitOrderProtocol.sol	100	100	100	100	
LimitOrderProtocolPro.sol	0	100	0	0	17
OrderLib.sol	100	100	100	100	
OrderMixin.sol	86.96	80	80	85.57	... 264,346,348
OrderRFQLib.sol	100	100	100	100	
OrderRFQMixin.sol	90.16	58.7	90	90.32	... 122,175,176
contracts\helpers\	86.81	62.5	84.85	86.02	
AmountCalculator.sol	100	100	100	100	
ChainlinkCalculator.sol	78.57	50	100	76.92	33,44,46
ERC1155Proxy.sol	0	0	0	0	18,24
ERC721Proxy.sol	100	50	100	100	
ERC721ProxySafe.sol	0	0	0	0	18,25
ImmutableOwner.sol	100	50	100	100	
NonceManager.sol	100	100	100	100	
PredicateHelper.sol	93.88	83.33	90.91	92.16	28,66,67,119
SeriesNonceManager.sol	100	100	100	100	
WethUnwrapper.sol	100	50	100	100	
WhitelistChecker.sol	60	75	100	60	33,35
contracts\libraries\	100	100	100	100	
ArgumentsDecoder.sol	100	100	100	100	
Callib.sol	100	100	100	100	
Errors.sol	100	100	100	100	
All files	88.48	71.08	86.08	88.03	

solidity-utils

Tests result

```
196 passing (44s)
6 pending
```

Tests coverage

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\	75	16.67	50	57.14	
EthReceiver.sol	100	0	100	0	11
GasChecker.sol	100	50	100	100	
OnlyWethReceiver.sol	0	0	0	0	14,19
contracts\libraries\	71.32	59.3	78.72	74.84	
AddressArray.sol	96.77	92.86	87.5	97.06	30
AddressSet.sol	100	100	100	100	
ECDSA.sol	100	100	100	100	
RevertReasonForwarder.sol	100	100	100	100	
RevertReasonParser.sol	100	100	100	100	
SafeERC20.sol	100	88.89	100	100	
StringUtil.sol	50	100	66.67	66.67	13
UniERC20.sol	0	0	0	0	... 103,106,110
All files	71.43	56.52	77.55	74.07	

STATE
MIND