IJS Technologies

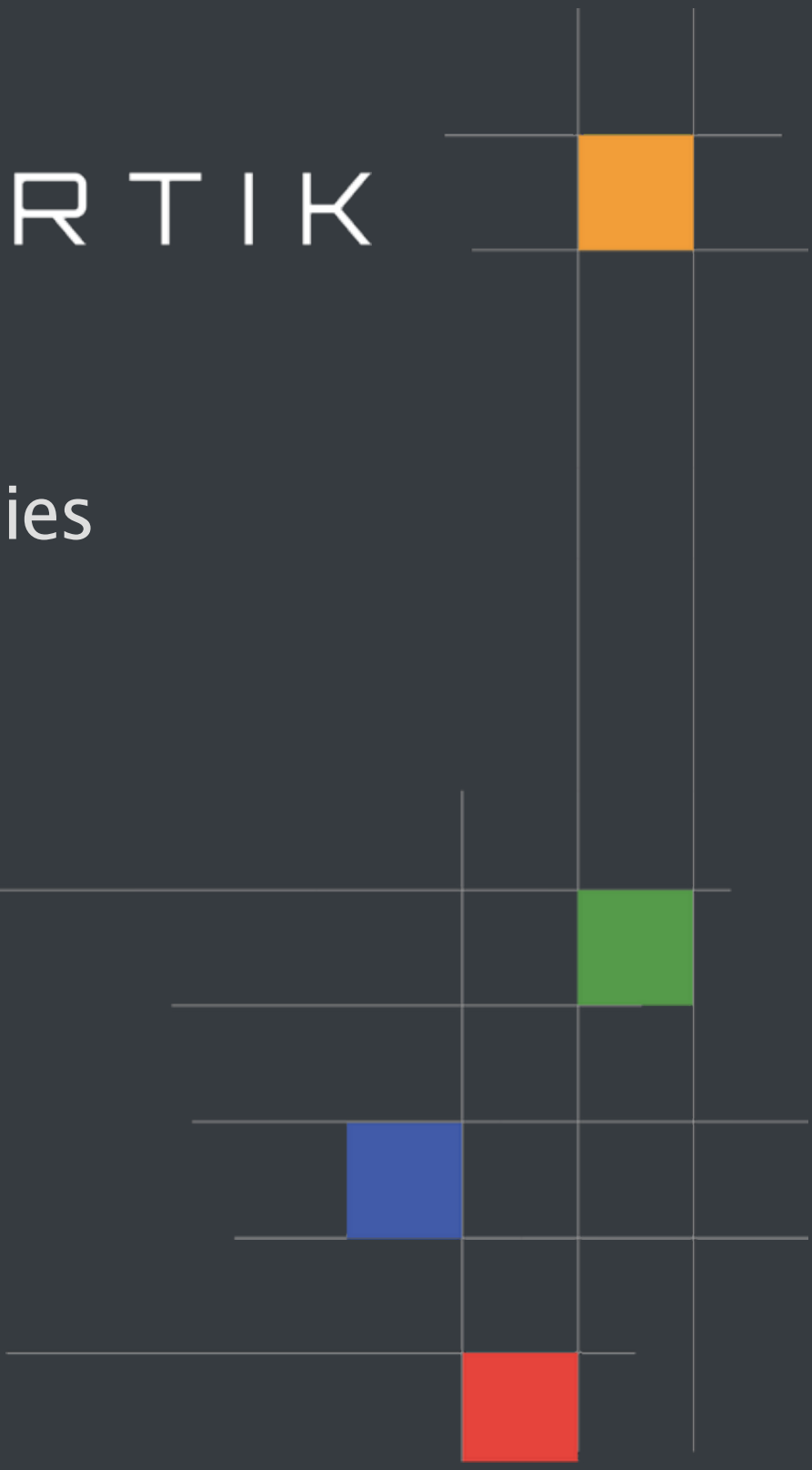
OpenSwap DEX

Security Assessment

March 25nd, 2021

[Preliminary Report]

Audited By:
Adrian Hetman @ CertiK
adrian.hetman@certik.org
Reviewed By:
Alex Papageorgiou @ CertiK
alex.papageorgiou@certik.org



Disclaimer

CertiK reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security review.

CertiK Reports do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

CertiK Reports should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

CertiK Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has completed a round of auditing with the intention to increase the quality of the company/product's IT infrastructure and or source code.

Overview

Project Summary

Project Name	IJS Technologies - OpenSwap DEX
Description	OpenSwapDEX is a community-driven project, supported by the OAX foundation to introduce a DEX experience that enables traders to participate in AMM (Automated Market Maker) swaps as well as oracle-priced swaps, under a decentralized community governance system that is transparent.
Platform	Ethereum; Solidity, Yul
Codebase	GitHub Repository
Commits	1. 9bdc742970ceb46a1a7a1adad712811716d93f80

Audit Summary

Delivery Date	March 25nd, 2021
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	1
Timeline	March 22nd, 2021 - March 22nd, 2021

Vulnerability Summary

Total Issues	0
Total Critical	0
Total Major	0
Total Medium	0
Total Minor	0
Total Informational	0

Executive Summary

We were tasked to check latest changes introduced by the team. Below is the list of major bug fixes and changes introduced in the code alongside.

1. Fixed a bug that cannot shutdown a oracle pair by admin (OAXDEX_OraclePair.sol)
2. Fixed a bug that cannot add admin up to the maxAdmin (OAXDEX_Administrator.sol)
3. Fixed typo (OAXDEX_Administrator.sol)
4. Added system parameters so that trade fee / protocol fee for AMM and Queues may be governed separately (OAXDEX_Factory.sol, OAXDEX_VotingExecutor.sol)
    1. OAXDEX_Factory.sol
    2. OAXDEX_Factory.sol
    3. OAXDEX_VotingExecutor.sol
5. Added an amount parameter so that Oracle Adapters is aware of trade sizes (OAXDEX_OraclePair.sol, oracles/*)
    1. `getRatio()` functions were introduced in OracleAdapters
    2. _getSwappedAmount was updated
    3. getAmountIn was updated
6. Set private replenish to true in queue by default
7. Fixed a bug where the on-going Polls were removed when adding new votes

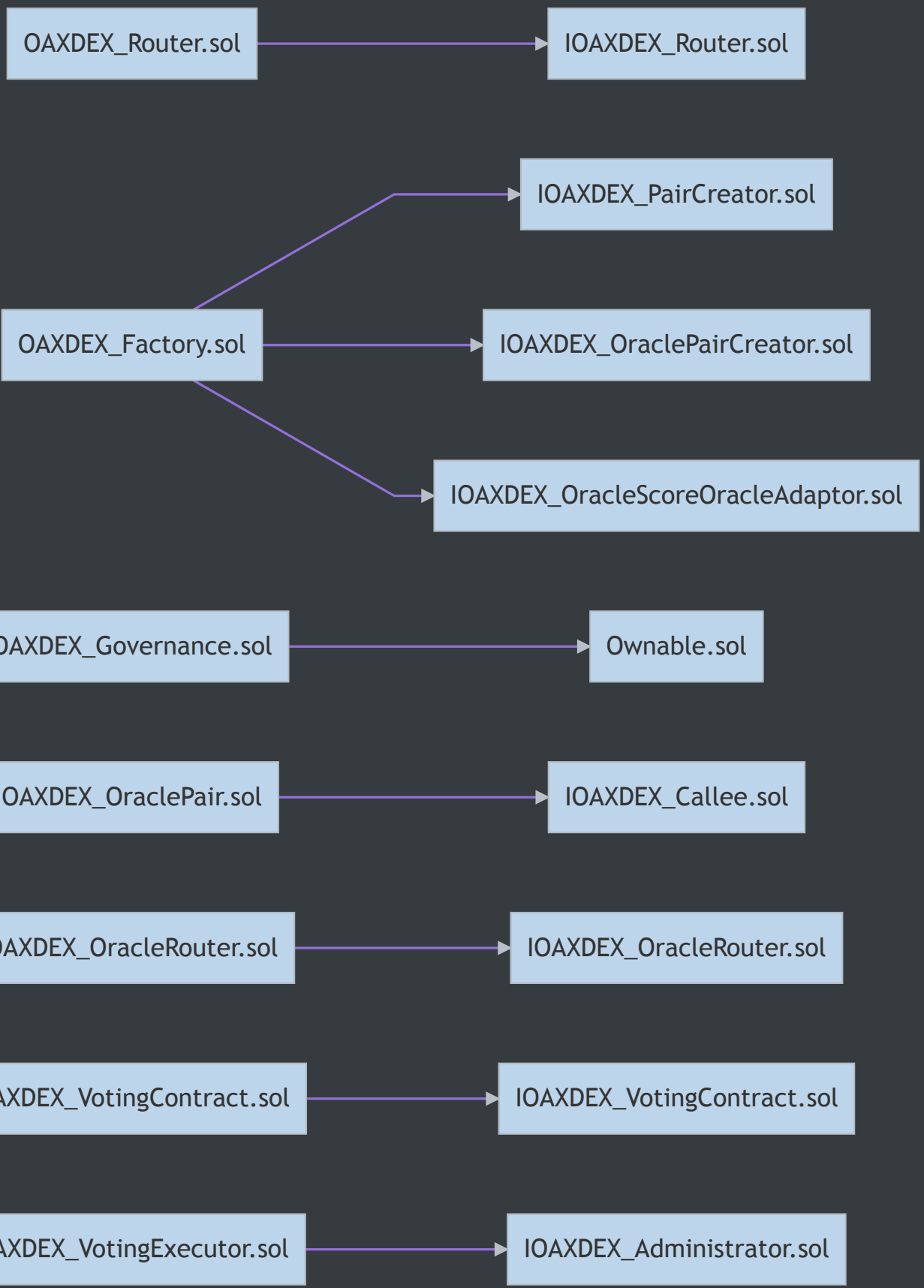
There were also some small changes that simplified operations like `_getLatestPrice` in OracleChainlink.sol. Overall, introduced changes fixed bugs and the team performed refactoring of the code. No bugs or vulnerabilities were introduced.

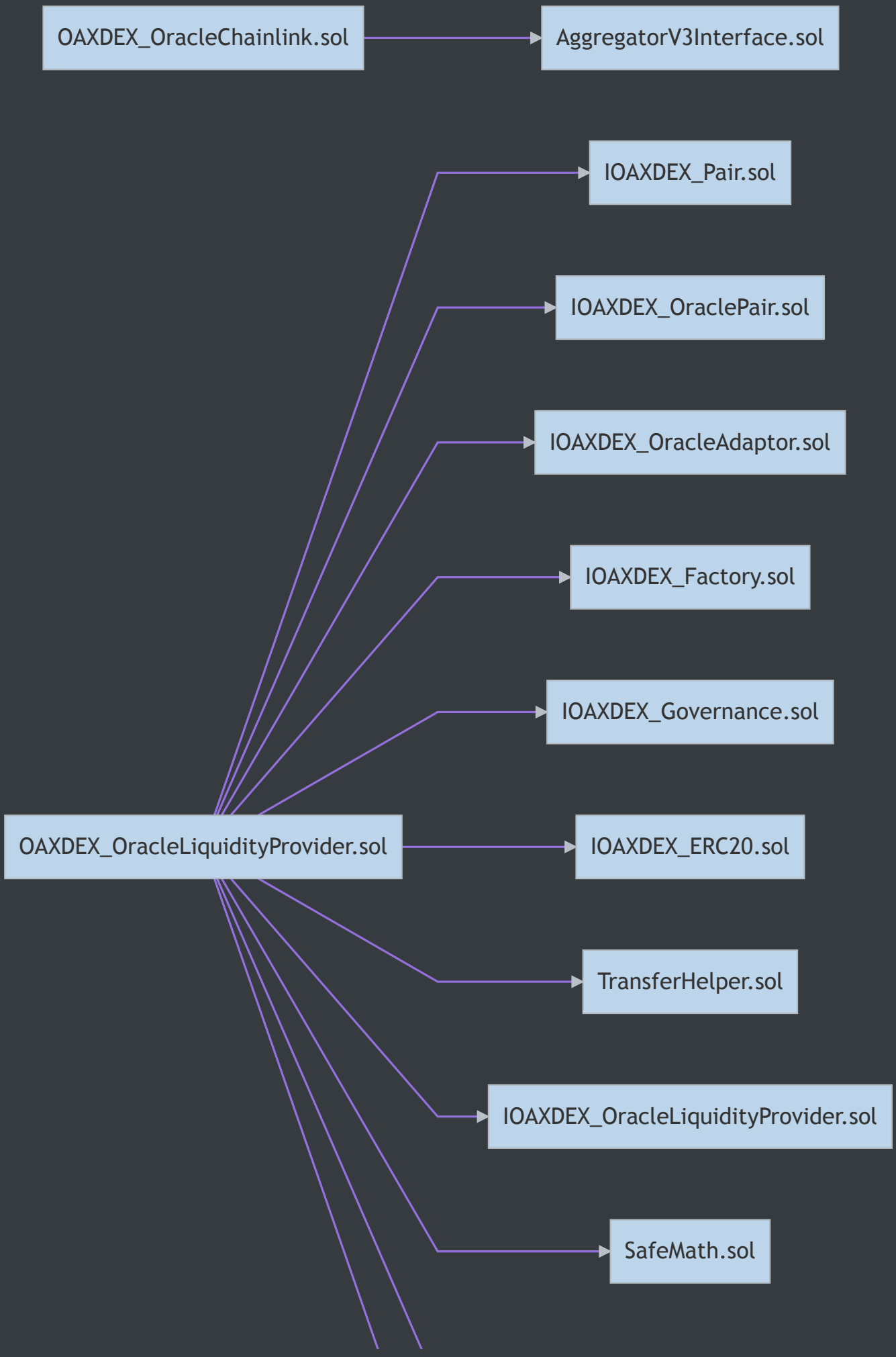
List of all changes can be found here.

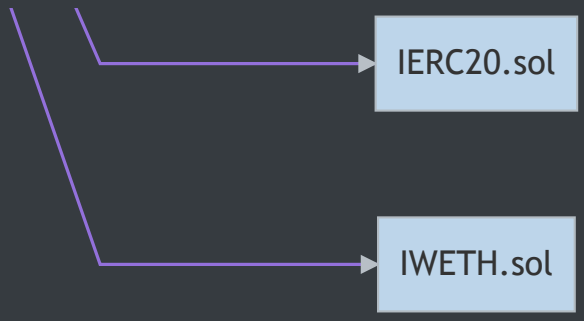
Files In Scope

ID	Contract	Location
OAA	OAXDEX_Administrator.sol	OAXDEX_Administrator.sol
OAX	OAXDEX_ERC20.sol	OAXDEX_ERC20.sol
OAE	OAXDEX_Factory.sol	OAXDEX_Factory.sol
OAG	OAXDEX_Governance.sol	OAXDEX_Governance.sol
OAL	OAXDEX_OracleLiquidityProvider.sol	OAXDEX_OracleLiquidityProvider.sol
OAO	OAXDEX_OraclePair.sol	OAXDEX_OraclePair.sol
OAR	OAXDEX_OracleRouter.sol	OAXDEX_OracleRouter.sol
OAD	OAXDEX_Router.sol	OAXDEX_Router.sol
OAV	OAXDEX_VotingContract.sol	OAXDEX_VotingContract.sol
OXD	OAXDEX_VotingExecutor.sol	OAXDEX_VotingExecutor.sol
IOX	IOAXDEX_Administrator.sol	interfaces/IOAXDEX_Administrator.sol
IOA	IOAXDEX_Factory.sol	interfaces/IOAXDEX_Factory.sol
IOD	IOAXDEX_OracleAdaptor.sol	interfaces/IOAXDEX_OracleAdaptor.sol
OXE	OAXDEX_OracleChainlink.sol	oracles/OAXDEX_OracleChainlink.sol
OAC	OAXDEX_OracleConstant.sol	oracles/OAXDEX_OracleConstant.sol
OAS	OAXDEX_OracleSigned.sol	oracles/OAXDEX_OracleSigned.sol
OAU	OAXDEX_OracleUnity.sol	oracles/OAXDEX_OracleUnity.sol

File Dependency Graph




OAXDEX_OracleChainlink.sol
AggregatorV3Interface.sol
IOAXDEX_Pair.sol
IOAXDEX_OraclePair.sol
IOAXDEX_OracleAdaptor.sol
IOAXDEX_Factory.sol
IOAXDEX_Governance.sol
OAXDEX_OracleLiquidityProvider.sol
IOAXDEX_ERC20.sol
TransferHelper.sol
IOAXDEX_OracleLiquidityProvider.sol
SafeMath.sol


IERC20.sol
IWETH.sol