Major changes in the repository from the last external audit [tag v1.0.0]

tag v1.0.1

From the last audit tag v1.0.0, no code was changed in the solidity files. More tests were added and the documentation was frequently refreshed to keep it up-to-date.

tag v1.0.2-pre-internal-audit

From the last tag v1.0.1, the wveOLAS contract has been added.

Wapper for the veOLAS contract (wveOLAS)

This contract has been added to address issues regarding the functions `getPastVotes`, `balanceOfAt`, `totalSupplyLockedAtT` on the veOLAS contract (cf. Vulnerabilities_list#1.pdf for more details). These are view functions and their issues affect voting but do not affect veOLAS contract storage. In summary, this wrapper contract serves the purpose of fixing view functions with issues and forwarding all other view functions to the original veOLAS contract. All the write-to-storage functions must be called directly by the veOLAS contract. The default fallback reverts with the statement mentioning the original veOLAS address. See Specs of governance contracts_v1.1.0.pdf for full specifications of this contract.

PRs summary

PR #47 This PR allows us to provide evidence that there are issues with the above veOLAS view functions (cf. Vulnerabilities_list#1.pdf) that affect voting but do not affect veOLAS contract storage. Specifically, here we forked the original Curve VotingEscrow contract and compared all the functions that modify the contract storage with our original veOLAS contract executions. This showed that storage changes matched in both contracts with exact precision.

PR #48 This PR provides a partial implementation of the wveOLAS contract. Specifically:

- View functions `getPastVotes(address account, uint256 blockNumber)` and `balanceOfAt(address account, uint256 blockNumber)` with issues described in Vulnerabilities_list#1.pdf are wrapped and fixed. There is a check that the input `blockNumber` is not smaller than the block number written in the very first user point. Then the veOLAS original function is called. Zero is returned otherwise. (cf. Specs of governance contracts_v1.1.0.pdf for more details).

- The view function `totalSupplyLockedAtT(uint256 ts)` with the issue described in Vulnerabilities_list#1.pdf is wrapped and fixed. There is a check that the input `ts` is not smaller than the timestamp written in the very last supply point. Then call the original function, or revert otherwise (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- The view function `getUserPoint(address account, uint256 idx)` is wrapped and modified in such a way that if the `account` has at least one point it is returned the point structure of its i`dx` point. Otherwise, the empty structure is returned (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- The view function `getPastTotalSupply(uint256 blockNumber)` is wrapped and modified in such a way if the input `blockNumber` is lower than the block number when the contract was deployed it is returned zero instead of the original Curve Voting Escrow plain revert (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- The view function `totalSupplyAt` is wrapped and not modified. E.g. it is directly called the corresponding original veOLAS method (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- The `fallback` method is added and this reverts with the statement mentioning the original veOLAS address (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- the view functions `totalNumPoints` and `mapSupplyPoints` are added (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- Tests are added to have full coverage.

PR #49 This PR updates hardhat packages and changes reverts in tests due to the Hardhat 2.10+ different management of reverts.

PR #50 This PR provides the complete implementation of the wveOLAS contract.

Specifically, the rest of the view functions are added:

- External view functions are wrapped but not modified `getLastUserPoint, getNumUserPoints, lockedEnd, allowance, delegates`. E.g. the corresponding original veOLAS methods are called (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- Functions `getVotes, totalSupply, supportsInterface, balanceOf, totalSupplyLocked` are wrapped and the corresponding veOLAS original

methods are called. Moreover, their veOLAS original *public* visibility is modified to *external*. (cf. Specs of governance contracts_v1.1.0.pdf for more details).
- Tests are added to have full coverage.

PR #51 This PR provides new deployment scripts, deprecates the Sale contract, and updates tests. Specifically:
- New deployment scripts and corresponding tests for integrating wveOLAS to the Autonolas protocol are added;
- The Sale contract (only initially used by the protocol and then stopped) and any mention of it are deprecated
- Tests showing the different behavior of `getPastVotes()` method in veOLAS and wveOLAS are added (veOLAS.js#L442-L444 & wveOLAS.js#L300-L302)

PR #52 This PR refines deployment script names, makes a small refactor to the wveOLAS contract and updates the vulnerabilities list. Specifically:
- Deployment script names are changed to make them more readable, and workflow to be more sequential;
- The function `getPastTotalSupply()` is rolled back to its exact original behavior as implemented in the Curve Voting Escrow contract to save on gas;
- The Vulnerabilities_list#1.pdf was updated in such a way it is clear that for us a revert in `getPastTotalSupply(uint256)` is something unexpected (must return zero), but we follow the original Curve Voting Escrow implementation.

tag v1.1.0-pre-audit

From the last audit tag v1.0.2-pre-internal-audit, the wveOLAS contract has been updated for internal audit suggestions.

PRs summary

PR #53 This PR contains an updated internal audit with a focus on the wveOLAS contract.

PR #54 In this PR we reacted to some suggestions from the internal audit. Specifically:
- The following parameters have been added: OLAS token address, name, symbol, and decimals.
- Constructor has been updated to also point to the OLAS token.
- Functions `totalNumPoints, mapSupplyPoints` have been updated by pointing to the corresponding original veOLAS state variables.

- The function `mapSlopeChanges` has been added by pointing to the corresponding original veOLAS state variable.
- The function `balanceOfAt` has been updated to save on gas when the user does not have any points.
- Functions `transfer, approve, transferFrom, delegate, delegatebySing` have been added to pass the ERC20 checks.
- Functions `allowance, delegates` have been updated to directly implement reverts.
- The deployment scripts have been updated to correctly point also to the OLAS token.
- Tests have been updated to full coverage.

PR #55 This PR prepares the repository for the external audit by adding and updating the documentation.