

iExec PoCo Audit

- [1 Executive Summary](#)
- [2 Scope](#)
 - [2.1 Documentations](#)
 - [2.2 Objectives](#)
- [3 System Overview](#)
 - [3.1 PoCo Delegate](#)
 - [3.2 Actors](#)
- [4 Recommendations](#)
 - [4.1 Avoid memory manipulation routines in assembly](#)
 - [4.2 Avoid repeated code throughout the codebase](#)
 - [4.3 Consider replacing the ERC1538 standard](#)
 - [4.4 Simplify the inheritance and modularity of the system](#)
 - [4.5 Correct spelling mistakes present in variable names](#)
 - [4.6 Review the Code Quality recommendations in Appendix 1](#)
- [5 Security Specification](#)
 - [5.1 Trust Model](#)
 - [5.2 Funds](#)
 - [5.3 Important Security Properties](#)
- [6 Issues](#)
 - [6.1 Permissionless nature of proxy factory might cause confusion when parsing events](#)
Acknowledged
 - [6.2 System deployer is fully trusted in this version of the PoCo system](#) Medium
Acknowledged
 - [6.3 `importScore\(\)` in `IexecMaintenanceDelegate` can be used to wrongfully reset worker scores](#) Medium Acknowledged
 - [6.4 Outdated documentation](#) Medium Acknowledged
 - [6.5 Domain separator in `iExecMaintenanceDelegate` has a wrong version field](#) Medium
Acknowledged
 - [6.6 Limit the length of `task.contributors` to prevent reaching `gasBlockLimit`](#) Minor
Acknowledged
 - [6.7 The `updateContract\(\)` method in `ERC1538UpdateDelegate` is incorrectly implemented](#)
Minor
- [Appendix 1 - Code Quality Recommendations](#)
 - [A.1.1 Use hardcoded hash values instead of constants](#)

Date	March 2020
Lead Auditor	Gonçalo Sá
Co-auditors	Shayan Eskandari

- A.1.2 Use of error messages in require()
- A.1.3 Variable definitions on top of the contract
- A.1.4 Inline documentation increases the code readability
- Appendix 2 - Files in Scope
- Appendix 3 - Artifacts
 - A.3.1 MythX
 - A.3.2 Ethlint
 - A.3.3 Surya
 - A.3.4 Tests Suite
- Appendix 4 - Disclosure

1 Executive Summary

This report presents the results of our engagement with **iExec** to review their **PoCo (Proof of Contribution)** protocol.

The review was conducted over the course of two weeks, from **March 30, 2020** to **April 10, 2020** by Gonçalo Sá and Shayan Eskandari. A total of **15** person-days were spent.

During the first week, we focused our efforts on understanding the intention of the design (which is mostly provided through communication with the client and the resources provided in the README of the main repository under review, `poco-dev`), and defining the key risk factors and potential vulnerabilities requiring further investigation. We also initiated an isolated code review of the `iexec-solidity` repository, still not considering interactions with the `poco-dev` codebase.

During the second week we initiated the code review efforts for both repositories under review. Focusing on interactions between the two repositories and a standalone review of the ERC1538 delegates present in the `poco-dev` repository.

2 Scope

Our review focused on two repositories:

- <https://github.com/iExecBlockchainComputing/poco-dev.git> @ a4dfe7891ac60489809cdd4d9c491c8f2e107a82
- <https://github.com/iExecBlockchainComputing/iexec-solidity.git> @ a4dfe7891ac60489809cdd4d9c491c8f2e107a82

The list of files in scope can be found in the [Appendix](#).

They represent the big majority of files that comprise the iExec system (the only exception being the RLC token dependencies that remain unchanged throughout multiple versions for the PoCo system). Note that many of the checks and effects of the iExec platform are done off-chain and not in the scope of this audit.

The allotted time for the audit (three person-weeks over the span of two weeks time) was deemed insufficient from the start to do a full comprehensive review of the whole system. And, even reducing the amount of visual collateral being provided as part of the report, some compromises had to be made on the completeness of the audit.

As such, this audit is mostly **focused on the correctness of the code** in individual modules and less so on the adhesion to the specification of the business logic of the Proof of Contribution system. In addition, there are some mathematical models that have been modified to fit into solidity variables, such as the implementation of **trust** variable (e.g. floating point to integer, see [Trust in the PoCo](#)), the mathematics behind the conversion falls outside the scope of this audit and only the correctness of client's implementation was reviewed.

2.1 Documentations

The following documentations were provided to the audit team:

- [PoCo Series #1](#) — About Trust and Agents Incentives
- [PoCo Series #2](#) — On the use of staking to prevent attacks
- [PoCo Series #3](#) — Protocol update
- [PoCo Series #4](#) — Enclaves and Trusted Executions
- [PoCo Series #5](#) — Open decentralized brokering on the iExec platform
- [Proof of Contribution](#) - docs.iex.ec
- [iExec platform documentation: Trust in the PoCo](#)

2.2 Objectives

Through discussion with the **iExec** team, we identified the following priorities for our review

1. Ensure code correctness in each individual module in the system.
2. Identify known vulnerabilities particular to smart contract systems, as outlined in our [Smart Contract Best Practices](#), and the [Smart Contract Weakness Classification Registry](#).

3. Make sure each module is implemented consistently with the intended functionality and without unintended edge cases.

3 System Overview

The iExec platform uses blockchain technology to create a marketplace where people can rent computing power to run Applications provided by App developers and/or use Datasets provided Dataset providers.

The iExec platform requires two entities in order to work, and PoCo acts as a link between those two entities:

- A [marketplace](#) where agents propose their resources and where deals are made using the RLC token.
- A distributed computing infrastructure based on the middleware XtremWeb-HEP.

3.1 PoCo Delegate

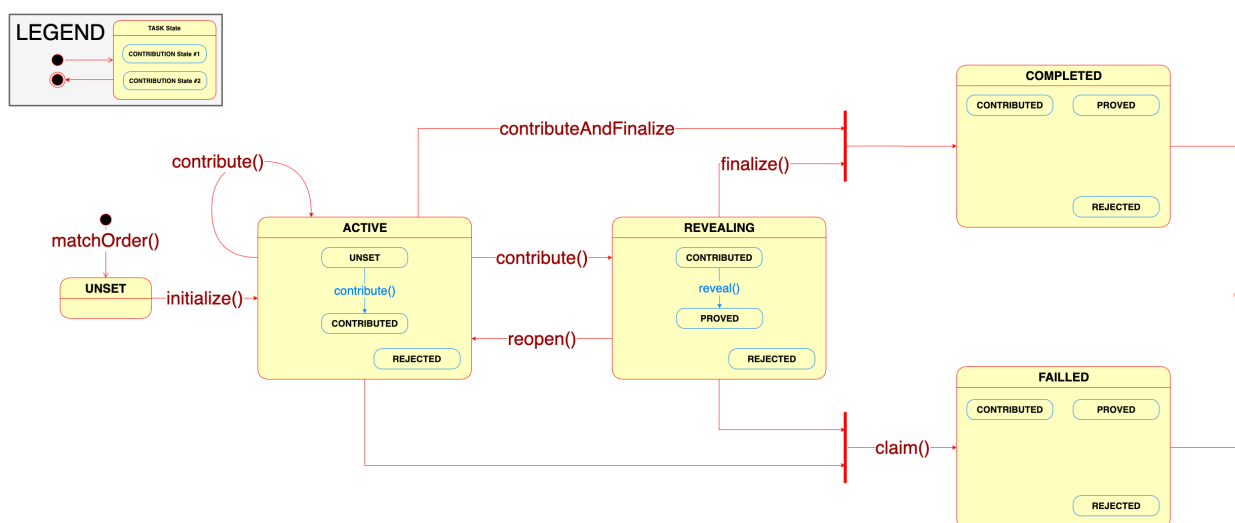
The core part of the PoCo system is the new `PoCoDelegate` smart contract. It replaces what used to be a combination of two smart contracts: the `IexecClerk` and the `IexecHub`.

The PoCo delegate (which, as the name indicates, is a delegate for the ERC1538 proxy acting as the entry for the system) implements almost all of the logic that rules over the success or failure of deals and, more specifically, tasks in the iExec system.

`IexecPoCoDelegate` is, undoubtedly, the most important smart contract of the PoCo architecture and its inception as a single smart contract is new to version 5 of the system.

The PoCo delegate handles both the token escrow and validation of the submitted computation results and handles the permissions (most of them through the checking of signatures from the relevant parties) of all the actors.

A PoCo delegate state diagram was generated to map out the state machines for both `Tasks` and `Contributions`, two important data structures for iExec's business logic, and guide the audit team through the review of the code.



The state machine, although complex, is clearly implemented in the code, with clear requirements enclosing the relevant functions.

3.2 Actors

In this platform, there are 4 main types of agents:

- **Application providers** provide applications running on the Ethereum/iExec platform and receive payments in RLC.
 - **Dataset providers** provide valuable datasets in a secure paradigm to protect their ownership.
- **Users** want to run applications and are therefore buying computing power to execute them.
- **Workers** execute applications required by the user and are therefore selling computing power. They receive payments in RLC for the computation power they provide. Workers can be pooled together in *worker pools*, and will be led by scheduler for work distribution.
- **Schedulers** organize workers into working pools and manage the execution of tasks: handling work distribution, assigning tasks to workers, transferring data, and handling failures. They do not do the actual computation, however they receive a fee for managing the infrastructure. Scheduler is also responsible for *random* worker selection.

iExec Hub & Market place: Smart contract without any privilege access to act as an *escrow* for the different agents' stake and provide transparency in the iExec ecosystem. Also *workers' reputation* is stored in this contract to enable workers to switch schedulers at will.

More on the permissions and ability of each actor can be found in [Security Specification](#) section.

4 Recommendations

4.1 Avoid memory manipulation routines in assembly

Even though the gas optimizations stemming from direct memory manipulation routines in assembly is commendable (these are mostly present in hashing-related functions in the `IexceLibCore_v5` library), the average saved gas per function is close to `600 gas` only. This means that, in average, a few thousand gas per user call will be saved at the expense of a big reduction in readability and auditability.

The audit team suggests that vanilla Solidity patterns are used in place of the more custom assembly blocks present in the code.

Update: iExec team agreed with this suggestion and implemented a fix in [PoCo-dev/pull/70/](#).

4.2 Avoid repeated code throughout the codebase

There are several instances of repeated contracts and code snippets throughout the two repositories under review. In some cases even differing slightly in the actual implementations. An effort should be made to reduce these duplicated instances to a minimum and, when possible, eliminate duplication at all.

Update: iExec team agreed with this suggestion and implemented a fix in [a74542102a1c4969eca8fefof947581f4f834a4c](#).

4.3 Consider replacing the ERC1538 standard

Consider using a more simplistic and auditable version of delegation than implementing the full ERC1538 standard. The two scenarios where delegation might be needed are covered below.

For size-constraint purposes, a simple fallback delegating to a following contract (this can, obviously, be a chain of multiple contracts in case the original contract is too big).

For purposes of gas optimization, external calls might still result in cheaper execution costs in the long run because of the additional cost of executing the pre-delegation piece of code in the proxy.

For modularity, the same architectural structure can be achieved with normal external calls and possibly a centralized registry that allows updates.

Update from the iExec team: The feature has been planned for almost 1 year, including communication about the advantages in terms of modularity and “future-proofness”. We would only consider removing the ERC1538 implementation if there was something fundamentally broken about it.

4.4 Simplify the inheritance and modularity of the system

Consider using less inheritance in similar classes for more audibility of the code. This is for overall the coding style of iExec code base. As an example discussed with the developer team, registries can be all

combined together and use types for each registers.

The current implementation has 3 main registries (and corresponding entities), **apps**, **dataset**, and **workerpools**. They share most of their logic in another file `Registry.sol`. All these registries can be combined in one registry, and by adding a type Enum (or other methods) they can be differentiated.

Update from the iExec team: We need the 3 registries to be different contracts in order for the 3 classes of assets to be independent ERC721 flavors. We would like to avoid any possible confusion between apps, datasets, and workerpools. And having all 3 be the same ERC721 family would create confusion.

4.5 Correct spelling mistakes present in variable names

Even though spelling mistakes are generally harmless when writing code, they can be harmful if not made consistently. There are two instances of spelling mistakes that are used in the PoCo codebase present in the codebase inconsistently.

On the task status Enum the value *FAILED* is spelled wrong but in the function in `PoCoDelegate` that makes sets this state is actually correctly named `failedWork()`. We recommend changing all instances of the Enum value to **FAILED**.

The other pervasive instance of a spelling mistake happens on the word *consensus* throughout the codebase. In this case, the inconsistency is only reflected in the difference from comments to the actual variable names. We recommend changing all the instances of *concensus* to **consensus** to prevent possible future errors.

Update: iExec team agreed with this suggestion and implemented a fix in [7bcbb54c8696664607a0135d02be5365abc584e2](#) and [a7fc84f2e72e5f4acdc147601d51234fb409907f](#).

4.6 Review the Code Quality recommendations in Appendix 1

Other comments related to readability and best practices are listed in [Appendix 1](#)

5 Security Specification

This section describes, **from a security perspective**, the expected behavior of the system under audit. It is not a substitute for documentation. The purpose of this section is to identify specific security properties that were validated by the audit team.

5.1 Trust Model

The relevant actors are listed below with their respective abilities:

System Deployer (iExec)

- Initially deploys and configures the iExec system, such as setting the address for the `baseToken`, all registries and iExec hub
- Upgrade and change the main contracts (registries):
 - App Registry
 - Dataset Registry
 - Worker Pool Registry
- Escrow Modifications
 - Recover funds and add to owner balance `recover()`
- Set callback gas limit `m_callbackgas`

Scheduler

- Manages Requests:
 - Reopen closed request `reopen()`
 - Finalize requests and contributions, which results in reward distribution to workers
- Manage Worker Pool Operation
- Create Worker pools, Set and Change policy of the worker pool, such as Stake ratio and Reward Ratio policies
- Sign PoolOrder for the work they are matching with

Worker (Computation Power Provider)

- Contribute work to tasks `contribute()`
- Reveal the contributed work `reveal()`

App Developer

- Create app `createApp()`
- Manage their submitted app `manageAppOrder()`
- Sign AppOrder for their app

Dataset Provider

- Create dataset `createDataset()`

- Manage their submitted dataset `manageDatasetOrder()`
- Sign DataOrder for their Datasets

Platform User (Computation Power Buyer)

- Request a task to be perform and stakes tokens for the requested computation
- Manage their submitted request `manageRequestOrder()`
- Sign the requestOrder

Note that App and Dataset signatures are assumed to be available publicly for users to use in their request orders. Workerpool and users signatures are gathered off-chain during the order request and bundled together with the App and Dataset signature to be sent to iExec hub (e.g. `matchOrder()`).

5.2 Funds

- All *actors* can deposit RLC on the iExec Hub.
- Funds deposited on the *iExec Hub* can be locked when staking. iExec Hub also holds all deposited rewards.
 - Funds that are not actively staked (locked) can be withdrawn at any time.
- *Worker's* stake in WorkerPool: This stake cannot be seized by anyone, and the worker can unlock it at anytime (by unsubscribing). Even If the worker is evicted by the scheduler (presumably because of a bad behavior) its stake will be unlocked.

It should be noted that the contracts that are named `Native` (such as `IexecEscrowNativeDelegate.sol`) are assumed to be deployed on iExec side chain and are not considered for mainnet deployment.

5.3 Important Security Properties

The following is a non-exhaustive list of security properties that were verified in this audit.

`iexec-solidity` Repository

- All the meant-to-be-internal, state-changing functions are correctly marked internal.
- All the external accessing functions accessing internal functions that can change the proxy's state (which functions it delegates to) are correctly permeated by `Ownable` -inherited modifiers.
- Delegates in the repository with state-changing methods (only the `Update` delegate) have correctly permeated functions with `onlyOwner` .
- The inheritance tree and delegation system of the ERC1538 architecture of the contract system are correctly implemented and do not create problems with shadowed elements or unimplemented methods.
- No unsigned integers in LibMap2 methods handling array indexes can underflow.
- No unsigned integers in LibSet methods handling arrays indexes can underflow.
- The compact signature recovery (EIP 2098) is correctly implemented (as per Nick Johnson's referral implementation).

`poco-dev` Repository

- The PoCo delegate state machine is implemented according to the intents stated in the documentation.
 - *Note:* The documentation refers only to previous versions' architecture with a *Clerk* and *Hub* instead of a `PocoDelegate`. The new specification that was validated is an extrapolation of the audit team.
- The signature checking methods are correctly implemented.
- No malicious actors can withdraw tokens from other agents' escrows.
- PoCo has its own implementation of ERC20, and it conforms with the ERC20 specification.
- PoCo delegate is inherently trusted, `owner` can upgrade the underlying contracts.
- Three registries exist that implement App, Dataset, and Workerpool. Note that they must be initialized to set proper values and only owner can change their policies.
- Management functionality for Requests, Apps, Datasets, and Workerpool scheduler are implemented as intended, with only the initial submitter being able to post the pre-signature or changing the task details.
- Structs meant for yet-to-be-implemented features are not accessible by any method in the current system.
- No problem arises from some of the *External* accessing functions being marked as *Public* (e.g., to prevent stack too deep compiler error).
- No unintended deadlock conditions arise in any part of the system from the use of `ExtendedSafeMath` methods.
- Incentives are correctly implemented for all of the actors in the PoCo system.

6 Issues

Each issue has an assigned severity:

- **Minor** issues are subjective in nature. They are typically suggestions around best practices or readability. Code maintainers should use their own judgment as to whether to address such issues.
- **Medium** issues are objective in nature but are not security vulnerabilities. These should be addressed unless there is a clear reason not to.
- **Major** issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- **Critical** issues are directly exploitable security vulnerabilities that need to be fixed.

6.1 Permissionless nature of proxy factory might cause confusion when parsing events **Acknowledged**

Resolution

Update from the iExec team:

The iExec offchain platform does not listen to GenericFactory. This factory is intended to be public and available to anyone and is just a tool used for deployment.

Description

The permissionless nature of the factory (the `GenericFactory` contract) meant to deploy the `ERC1538Proxy` and the instances of its several delegates might create confusion when parsing events.

Since there is no access control being enforced through the use of modifiers on said factory, any account can use its deployment public methods to deploy a contract. This means that the supporting off-chain infrastructure making use of the fired events to look for deployed instances of either the iExec proxies or its delegates might get hindered by an ill-intended actor that abuses its functions.

Recommendation

Use a modifier enforcing some sort of access control (easily done through the inherited `Ownable` contract) to make sure only iExec can deploy from the factory and, therefore, increase the readability of logged events.

This becomes more important as time goes by and updates to the architecture are performed or any past analysis needs to be done on deployed modules.

6.2 System deployer is fully trusted in this version of the PoCo system **Medium Acknowledged**

Resolution

Update from the iExec team:

After deployment, ownership is planned to be transferred to a multisig. This is just the first step towards a more decentralised governance on the protocol. We will consider adding an intermediary contract that enforces the lock period. This would however, prevent us from any kind of “emergency” update. The long term goal is it involve the community in the process, using a DAO or a similar solution.

Description

The introduction of ERC1538-compliant proxies to construct the PoCo system has many benefits. It heightens modularity, reduces the number of external calls between the system’s components and allows for easy expansion of the system’s capabilities without disruption of the service or need for off-chain infrastructure upgrade. However, the last enumerated benefit is in fact a double-edged sword.

Even though ERC1538 enables easy upgradeability it also completely strips the PoCo system of all of its prior trustless nature. In this version the iExec development team should be entirely trusted by **every** actor in the system not to change the deployed on-chain delegates for new ones.

Also the deployer, `owner`, has permission to change some of the system variables, such as `m_callbackgas` for Oracle callback gas limit. This indirectly can lock the system, for example it could result in `IexecPocoDelegate.executeCallback()` reverting which prevents the finalization of corresponding task.

Recommendation

The best, easiest solution for the trust issue would be to immediately revoke ownership of the proxy right after deployment. This way the modular deployment would still be possible but no power to change the deployed on-chain code would exist.

A second best solution would be to force a timespan period before any change to the proxy methods (and its delegates) is made effective. This way any actor in the system can still monitor for possible changes and “leave” the system before they are implemented.

In this last option the “lock” period should, obviously, be greater than the amount of time it takes to verify a `Task` of the bigger category but it is advisable to decide on it by anthropomorphic rules and use a longer, “human-friendly” time lock of, for example, 72 hours.

6.3 `importScore()` in `IexecMaintenanceDelegate` can be used to wrongfully reset worker scores **Medium** **Acknowledged**

Resolution

Update from the iExec team:

In order to perform this attack, one would first have to gain reputation on the new version, and lose it. They would then be able to restore its score from the old version.

We feel the risk is acceptable for a few reasons:

- It can only be done once per worker
- Considering the score dynamics discussed in the “Trust in the PoCo” document, it is more interesting for a worker to import its reputation in the beginning rather than creating a new one, since bad contributions only remove part of the reputation
- Only a handful of workers have reputation in the old system (180), and their score is low (average 7, max 22)

We might force the import all 180 workers with reputation >0. A script to identify the relevant addresses is already available.

Description

The import of worker scores from the previous PoCo system deployed on chain is made to be asynchronous. And, even though the pull pattern usually makes a system much more resilient, in this case, it opens up the possibility for an attack that undermines the trust-based game-theoretical balance the PoCo system relies on. As can be seen in the following function:

code/poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol:L51-L57

```
function importScore(address _worker)
external override
{
    require(!m_v3_scoreImported[_worker], "score-already-imported");
    m_workerScores[_worker] =
m_workerScores[_worker].max(m_v3_iexecHub.viewScore(_worker));
    m_v3_scoreImported[_worker] = true;
}
```

A motivated attacker could attack the system providing bogus results for computation tasks therefore reducing his own reputation (mirrored by the low worker score that would follow).

After the fact, the attacker could reset its score to the previous high value attained in the previously deployed PoCo system (v3) and undo all the wrongdoings he had done at no reputational cost.

Recommendation

Check that each worker interacting with the PoCo system has already imported his score. Otherwise import it synchronously with a call at the time of their first interaction.

6.4 Outdated documentation **Medium** **Acknowledged**

Resolution

Update from the iExec team: `Work in progress.`

Description

There are many changes within the system from the initial version that are not reflected in the documentation.

It is necessary to have updated documentation for the time of the audit, as the specification dictates the correct behaviour of the code base.

Examples

Entities such as `iExecClerk` are the main point of entry in the documentation, however they have been replaced by proxy implementation in the code base (V5).

Recommendation

Up date documentation to reflect the recent changes and design in the code base.

6.5 Domain separator in `iExecMaintenanceDelegate` has a wrong version field **Medium** **Acknowledged**

Resolution

Issue was fixed in [iExecBlockchainComputing/PoCo-dev@ ebee370](#)

Description

The domain separator used to comply with the EIP712 standard in `iExecMaintenanceDelegate` has a wrong version field.

code/poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol:L77-L86

```
function _domain()
internal view returns (IexecLibOrders_v5.EIP712Domain memory)
{
```



```
return IexecLibOrders_v5.EIP712Domain({
    name: "iExecODB"
, version: "3.0-alpha"
, chainId: _chainId()
, verifyingContract: address(this)
});
}
```

In the above snippet we can see the code is still using the version field from an old version of the PoCo protocol, "3.0-alpha" .

Recommendation

Change the version field to: "5.0-alpha"

6.6 Limit the length of `task.contributors` to prevent reaching `gasBlockLimit` **Minor** **Acknowledged**

Resolution

Update from the iExec team:

Any hardcoded lock would be a restriction in the future if the block size increases. In addition to that, workers are strongly incentivised to not contribute if it would result in a deadlocked task. Schedulers are incentivised to not authorise too many workers to contribute (they also lose stake if a task gets deadlocked). So the development team has assessed the risk as low.

In the unlikely event the described flaw still happens, the task will get in a deadlocked state, until at some point the block size limit is increased and a claim becomes possible. Because in a world where block size increases are possible, deadlocks are not eternal.

Description

It is recommended to limit the length of arrays that the contract iterates through to prevent system halts. `task.contributors` is used within `iExec` contract in many functions, and main functions such as `claim()`, `reOpen()`, and most importantly `contribute()` (through calling `checkConsensus()`) iterate through this list.

Given that contributions are not free and they could only block the task they are contributing to, this is a low impact issue.

Recommendation

The fix is trivial to implement and only requires to limit the number of items in `task.contributors` to the maximum imagined for the system (based on client communication this number could be 20, although further testing should be done to make sure with this number does not reach the `blockGasLimit`, possibly with future changes in the opcode pricing).

6.7 The `updateContract()` method in `ERC1538UpdateDelegate` is incorrectly implemented **Minor**

Resolution

Issue was fixed in [iExecBlockchainComputing/iexec-solidity@e6be083](#)

Description

The `updateContract()` method in `ERC1538UpdateDelegate` does not behave as intended for some specific streams of bytes (meant to be parsed as function signatures).

The mentioned function takes as input, among other things, a `string` (which is, canonically, a dynamically-sized `bytes` array) and tries to parse it as a conjunction of [function signatures](#).

As is evident in:

code/iexec-solidity/contracts/ERC1538/ERC1538Update.sol:L39

```
if (char == 0x3B) // 0x3B = ';' ;
```

Inside the function, `;` is being used as a “reserved” character, serving as a delimiter between each function signature.

However, if two semicolons are used in succession, the second one will not be checked and will be made part of the function signature being sent into the `_setFunc()` method.

Example of faulty input

```
someFunc;;someOtherFuncWithSemiColon;
```

Recommendation

Replace the line that increases the `pos` counter at the end of the function:

code/iexec-solidity/contracts/ERC1538/ERC1538Update.sol:L47

```
start = ++pos;
```

With this line of code:

```
start = pos + 1;
```

Appendix 1 - Code Quality Recommendations

A.1.1 Use hardcoded hash values instead of constants

Since the Solidity compiler does not yet compute constants which make use of EVM opcodes at compile-time (specifically important for the iExec codebase is the case of the `SHA3` opcode), the audit team recommends that the function signatures and Keccak256 hashes are substituted by hardcoded 4-byte and 32-byte hex values instead. This will result in less deployment and runtime costs overall, with close to no hinderance in auditability.

To create full trust in the hardcoded constants, the dev team may optionally want to verify that the hardcoded constant matches the result of the execution of said opcode by `require()` ing that both the constant and the runtime implementation of the `keccak256()` function with the right parameters match.

Update: iExec team agreed to this suggestion and implemented a fix in [PoCo-dev/pull/70/](#) and [d42593966b68524291715662154b1ba436af2be3](#).

A.1.2 Use of error messages in `require()`

Given the excessive amount of checks in the codebase (e.g. `matchOrder()` has 27 explicit `require` checks), it is suggested to use error messages to simplify debugging and future updates. The full text error messages might result in imploding size of the smart contract, hence it's suggested to add the error message to critical checks and use short error codes instead of (32+ bytes) strings.

Update: iExec team agreed to this suggestion and implemented a partial fix in [3f7f22712821bd5d8cfcf9b279d4af18boe56bf9](#). However, error messages increase immensely the deployment size of contracts, effectively rendering them “undeployable”. So the fix was only implemented partially.

A.1.3 Variable definitions on top of the contract

In order to have more readable code, it is recommended that all variables are defined on top of the contract code. As an example `Identities` struct is defined in the middle of `IexecPocoDelegate.sol`, and might not be obvious to the reader that there's such definition in that contract.

Update: iExec team agreed to this suggestion and implemented a fix in a number of commits to the repos between April 8, 2020 and April 17, 2020.

A.1.4 Inline documentation increases the code readability

Inline code documentation helps with the code review and most importantly with future code updates. The code base is lacking descriptive comments regarding the decisions of the development team on the implementation. It is suggested to leave the useful code comments when refactoring.

Update: iExec team agreed to this suggestion and implemented a fix in [fd91ee07a2bbe3b8eedd65f68ef8271a41960995](#).

Appendix 2 - Files in Scope

This audit covered the following files in the respective repositories:

iExecBlockchainComputing/poco-dev

File Name	SHA
poco-dev/contracts/IexecInterfaceNative.sol	438599f3acea91f811c71
poco-dev/contracts/IexecInterfaceNativeABILegacy.sol	28607ea20a6e91fcc5b9
poco-dev/contracts/IexecInterfaceToken.sol	2ea18304e61a6d88a39
poco-dev/contracts/IexecInterfaceTokenABILegacy.sol	e0541ee61d54d9034c5
poco-dev/contracts/Store.sol	b5edbo4dabdc5983a11
poco-dev/contracts/libs/IexecLibCore_v5.sol	359c785f15d6ac64197e
poco-dev/contracts/libs/IexecLibOrders_v5.sol	65d30c4d5069636495
poco-dev/contracts/modules/DelegateBase.sol	966321486cf7049912c1
poco-dev/contracts/modules/delegates/ENSIntegrationDelegate.sol	509ad5bda5fb7896699
poco-dev/contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol	257f318160dfd6a848c2
poco-dev/contracts/modules/delegates/IexecAccessorsDelegate.sol	8bbc143e3ea0e731c6c5
poco-dev/contracts/modules/delegates/IexecCategoryManagerDelegate.sol	b42cb5c07838d5eb8da
poco-dev/contracts/modules/delegates/IexecERC20Common.sol	54ecb31c576017c96fa7
poco-dev/contracts/modules/delegates/IexecERC20Delegate.sol	6b6e404844c727e57a1
poco-dev/contracts/modules/delegates/IexecEscrowNativeDelegate.sol	dof96ed32949a8d0726
poco-dev/contracts/modules/delegates/IexecEscrowTokenDelegate.sol	1c0177cff23a426fe40c2
poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol	1c1eef2430cc35ce3366
poco-dev/contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol	00b3b7ab05f2f790402
poco-dev/contracts/modules/delegates/IexecOrderManagementDelegate.sol	aa2f3dccf020d9c21f50
poco-dev/contracts/modules/delegates/IexecPocoDelegate.sol	a43fa6b7f4c088adfdfe

File Name	SHA
poco-dev/contracts/modules/delegates/IexecRelayDelegate.sol	096d24d4b15593ee1ce
poco-dev/contracts/modules/delegates/SignatureVerifier.sol	83160d2e5924055aa32
poco-dev/contracts/modules/interfaces/ENSIntegration.sol	foad54cfbc0f3f5dda20.
poco-dev/contracts/modules/interfaces/IOwnable.sol	b33a9ad33d580bb88e
poco-dev/contracts/modules/interfaces/IexecAccessors.sol	c2bff677eb8d606af569
poco-dev/contracts/modules/interfaces/IexecAccessorsABILegacy.sol	91f97256685b9101044
poco-dev/contracts/modules/interfaces/IexecCategoryManager.sol	2c0bc1c4f9e3261c4e1c
poco-dev/contracts/modules/interfaces/IexecERC20.sol	66841034833adca8c16
poco-dev/contracts/modules/interfaces/IexecEscrowNative.sol	d8847e54490a498845
poco-dev/contracts/modules/interfaces/IexecEscrowToken.sol	off3340f349dd50126d.
poco-dev/contracts/modules/interfaces/IexecMaintenance.sol	1822954ab2aa4f315f0c
poco-dev/contracts/modules/interfaces/IexecMaintenanceExtra.sol	47bdc786183681f4ba0
poco-dev/contracts/modules/interfaces/IexecOrderManagement.sol	bdc694d099bc20ca89c
poco-dev/contracts/modules/interfaces/IexecPoco.sol	f82e8e5e5aa70c35345c
poco-dev/contracts/modules/interfaces/IexecRelay.sol	be2ab578ba29627be46
poco-dev/contracts/modules/interfaces/IexecTokenSpender.sol	202b77df4de1fcdacd1a.
poco-dev/contracts/registries/IRegistry.sol	ffe3c15f48605d24c5b1.
poco-dev/contracts/registries/Registry.sol	a3837bdfa95c5024ad1:
poco-dev/contracts/registries/RegistryEntry.sol	b6864be405a056d6ef1
poco-dev/contracts/registries/apps/App.sol	cac8649f11ce8bc2c93b
poco-dev/contracts/registries/apps/AppRegistry.sol	e1d7c5744cbff24c80dc
poco-dev/contracts/registries/datasets/Dataset.sol	83257f5ac85d8da3460
poco-dev/contracts/registries/datasets/DatasetRegistry.sol	bf147967c07446dde52l
poco-dev/contracts/registries/workerpools/Workerpool.sol	16be9246eb5652d24a4
poco-dev/contracts/registries/workerpools/WorkerpoolRegistry.sol	cab0ee262cd9d5b42dc
poco-dev/contracts/tools/Migrations.sol	ab396f2c04aed69f6cde
poco-dev/contracts/tools/testing/TestClient.sol	obcf03e777105ce8d52c

File Name	SHA
poco-dev/contracts/tools/testing/TestReceiver.sol	5404782e56839826c5f

iExecBlockchainComputing/iexec-solidity

File Name	SHA-1
iexec-solidity/contracts/ENStools/ENSReverseRegistration.sol	20ea50fd7ba8fb5398281
iexec-solidity/contracts/ERC1154/IERC1154.sol	892b56dee343f68a984b
iexec-solidity/contracts/ERC1271/IERC1271.sol	4944fcc92d2ba5abf07a4
iexec-solidity/contracts/ERC1538/ERC1538.sol	c2ff06da81513e4f0a9143
iexec-solidity/contracts/ERC1538/ERC1538Proxy.sol	75e468f9819caace38123
iexec-solidity/contracts/ERC1538/ERC1538Query.sol	73f28de88815b08cdeae
iexec-solidity/contracts/ERC1538/ERC1538Store.sol	6f8bbfd330c5cbb78bc0c
iexec-solidity/contracts/ERC1538/ERC1538Update.sol	38a9d71ace70289423c57
iexec-solidity/contracts/ERC1538/IERC1538.sol	2a30f324d44b77a5dda16
iexec-solidity/contracts/ERC725/IERC725.sol	14e1265d58b916e92530c
iexec-solidity/contracts/ERC734/IERC734.sol	1648464843385275d20d
iexec-solidity/contracts/Factory/CounterfactualFactory.sol	822d7cfba1ca1f2a66304
iexec-solidity/contracts/Factory/GenericFactory.sol	45888956954bbb2c1a32
iexec-solidity/contracts/Libs/SafeMathExtended.sol	988444bcf4obe7af53d14
iexec-solidity/contracts/Migrations.sol	d6a9049b9ccf34341831c
iexec-solidity/contracts/TestContract.sol	44e98d4544boe414281a
iexec-solidity/contracts/Upgradeability/BaseUpgradeabilityProxy.sol	1d7fdce8663c7338ff9ca5
iexec-solidity/contracts/Upgradeability/InitializableUpgradeabilityProxy.sol	fae44f55f71595c17b7fc6a
iexec-solidity/contracts/Upgradeability/Proxy.sol	a6e3c5967eb838e4a79e7

Appendix 3 - Artifacts

This section contains some of the artifacts generated during our review by automated tools, the test suite, etc. If any issues or recommendations were identified by the output presented here, they have been addressed in the appropriate section above.

A.3.1 MythX

MythX is a security analysis API for Ethereum smart contracts. It performs multiple types of analysis, including fuzzing and symbolic execution, to detect many common vulnerability types. The tool was used for automated vulnerability discovery for all audited contracts and libraries. More details on MythX can be found at mythx.io.

Below is the miniaturized output of the MythX vulnerability scan per repository. Please note that this does not include multi-contract, multi-transaction issues. Those can only be seen in the tool dashboard but have been analyzed extensively by the audit team.

MythX Output For `iexec-solidity` Repository

```
/iexec-solidity/contracts/upgradeability/baseupgradeabilityproxy.sol
  1:0  warning  A floating pragma is set  SWC-103
  8:1  error     integer overflow          SWC-101
  9:41 error     integer overflow          SWC-101

/iexec-solidity/contracts/upgradeability/proxy.sol
  1:0  warning  A floating pragma is set  SWC-103
 47:54 warning  requirement violation     SWC-123
 51:77 warning  requirement violation     SWC-123

/iexec-solidity/contracts/factory/counterfactualfactory.sol
 -1:0  warning  assertion violation       SWC-110
  1:0  warning  A floating pragma is set  SWC-103
 15:11 warning  requirement violation     SWC-123
 28:3  warning  Potentially unbounded data structure passed to builtin SWC-128

/iexec-solidity/contracts/libs/ecdsa.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity/contracts/libs/ecdsalib.sol
  1:0  warning  A floating pragma is set  SWC-103
 20:1  warning  The caller can jump to any point in the code SWC-127

/iexec-solidity/contracts/enstools/ensreverseregistration.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity@ensdomains/ens/contracts/ens.sol
  1:0  warning  A floating pragma is set  SWC-103
```

```
/iexec-solidity/contracts/erc1538/erc1538.sol
  1:0  warning  A floating pragma is set  SWC-103
  6:12 error    integer overflow           SWC-101

/iexec-solidity/contracts/erc1538/erc1538store.sol
  1:0  warning  A floating pragma is set      SWC-103
 10:1  warning  Unused state variable "m_funcs" SWC-131

/iexec-solidity/contracts/erc1538/ierc1538.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity@openzeppelin/contracts/gsn/context.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity@openzeppelin/contracts/access/ownable.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-soliditysolstruct/contracts/libs/libmap2.bytes4.address.bytes.sol
  1:0    warning  A floating pragma is set      SWC-103
 12:274 warning  Implicit loop over unbounded data structure SWC-128
 12:1176 warning  Implicit loop over unbounded data structure SWC-128
 12:1358 warning  Implicit loop over unbounded data structure SWC-128
 12:1507 warning  Loop over unbounded data structure SWC-128
 12:1588 warning  Implicit loop over unbounded data structure SWC-128
 23:15  error    integer overflow           SWC-101

/iexec-soliditysolstruct/contracts/libs/libset.bytes4.sol
  1:0    warning  A floating pragma is set      SWC-103
 12:29  warning  assertion violation          SWC-110
 12:378 warning  Implicit loop over unbounded data structure SWC-128
 12:1145 warning  Loop over unbounded data structure SWC-128
 12:1209 warning  Implicit loop over unbounded data structure SWC-128
 45:194 error    integer overflow           SWC-101

/iexec-solidity/contracts/erc1538/erc1538proxy.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity/contracts/erc1538/erc1538proxyv2.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity/contracts/erc1538/erc1538query.sol
  1:0    warning  A floating pragma is set      SWC-103
 45:1751 warning  Unused local variable "funcId" SWC-131

/iexec-solidity/contracts/erc1538/erc1538update.sol
  1:0  warning  A floating pragma is set  SWC-103

/iexec-solidity/contracts/erc1538/erc1538updatev2.sol
  1:0  warning  A floating pragma is set  SWC-103
  9:48 error    integer overflow           SWC-101

/iexec-solidity/contracts/factory/genericfactory.sol
```

```

1:0    warning  A floating pragma is set                               SWC-103
27:6   warning  Potentially unbounded data structure passed to builtin SWC-128
28:6   warning  Potentially unbounded data structure passed to builtin SWC-128
32:4   warning  The caller can jump to any point in the code           SWC-127
32:151 warning  Potentially unbounded data structure passed to builtin SWC-128
32:161 warning  Potentially unbounded data structure passed to builtin SWC-128

/iexec-solidity/contracts/erc1154/ierc1154.sol
1:0    warning  A floating pragma is set                               SWC-103

/iexec-solidity/contracts/erc725/ierc725.sol
1:0    warning  A floating pragma is set                               SWC-103

/iexec-solidity/contracts/erc734/ierc734.sol
1:0    warning  A floating pragma is set                               SWC-103

/iexec-solidity/contracts/upgradeability/initializableupgradeabilityproxy.sol
1:0    warning  A floating pragma is set                               SWC-103
28:34  warning  A reachable exception has been detected               SWC-110
33:4   warning  requirement violation                                 SWC-123

/iexec-solidity/contracts/libs/safemathextended.sol
1:0    warning  A floating pragma is set                               SWC-103

/iexec-solidity/contracts/libs/signatureverifier.sol
1:0    warning  A floating pragma is set                               SWC-103

/iexec-solidity/contracts/testcontract.sol
1:0    warning  A floating pragma is set                               SWC-103
7:1    warning  Implicit loop over unbounded data structure           SWC-128
28:2   warning  Implicit loop over unbounded data structure           SWC-128

× 59 problems (6 errors, 53 warnings)

```

MythX Output For `poco-dev` Repository

```

/poco-dev/contracts/registries/iregistry.sol
3:20   error    persistent state write after call                     SWC-107
3:42   warning  requirement violation                                 SWC-123
6:43   error    integer overflow                                     SWC-101
10:20  error    integer overflow                                     SWC-101

/poco-dev/contracts/registries/registry.sol
10:1090 warning  multiple external calls                               SWC-113
10:1090 warning  requirement violation                                 SWC-123
10:1159 error    persistent state read after call                     SWC-107
10:1673 warning  requirement violation                                 SWC-123

/poco-dev/contracts/registries/apps/app.sol
6:17   error    integer overflow                                     SWC-101

```

```

6:45 error integer overflow SWC-101
8:22 error integer overflow SWC-101
10:8 error integer overflow SWC-101

/poco-dev@iexec/solidity/contracts/enstools/ensreverseregistration.sol
10:387 warning Multiple calls are executed in the same transaction SWC-113
10:387 warning requirement violation SWC-123
16:35 warning requirement violation SWC-123

/poco-
dev@iexec/solidity/contracts/upgradeability/initializableupgradeabilityproxy.sol
10:719 warning A reachable exception has been detected SWC-110
10:883 warning requirement violation SWC-123

/poco-dev@iexec/solidity/contracts/upgradeability/proxy.sol
10:1253 warning requirement violation SWC-123
10:1471 warning requirement violation SWC-123

/poco-dev@openzeppelin/contracts/token/erc721/erc721.sol
10:9128 error persistent state read after call SWC-107
10:11878 error persistent state write after call SWC-107
10:11878 error persistent state read after call SWC-107
10:14333 warning Potentially unbounded data structure passed to builtin SWC-128
10:15790 warning Unused function parameter "from" SWC-131
10:15804 warning Unused function parameter "to" SWC-131
10:15816 warning Unused function parameter "tokenId" SWC-131
72:12641 warning Unused function parameter "from" SWC-131
72:12655 warning Unused function parameter "to" SWC-131
72:12667 warning Unused function parameter "tokenId" SWC-131

/poco-dev@openzeppelin/contracts/token/erc721/erc721enumerable.sol
10:3630 warning Incorrect function "_tokensOfOwner" state mutability SWC-000
10:3721 warning Implicit loop over unbounded data structure SWC-128
10:4132 error persistent state write after call SWC-107
10:4161 error persistent state read after call SWC-107
10:4194 error persistent state write after call SWC-107
10:4502 error persistent state write after call SWC-107
10:4529 error persistent state read after call SWC-107
10:4556 error persistent state write after call SWC-107
72:481 warning Incorrect function "_tokensOfOwner" state mutability SWC-000

/poco-dev@openzeppelin/contracts/token/erc721/erc721metadata.sol
10:1046 error integer overflow SWC-101
10:1249 error integer overflow SWC-101
10:2072 warning Potentially unbounded data structure passed to builtin SWC-128
10:3193 error integer overflow SWC-101

/poco-dev@openzeppelin/contracts/utils/counters.sol
10:1109 error persistent state read after call SWC-107
10:1109 error persistent state write after call SWC-107

/poco-dev/contracts/registries/datasets/dataset.sol

```

```
6:21 error integer overflow SWC-101
8:1 error integer overflow SWC-101
```

/poco-dev/contracts/store.sol

```
1:2 warning requirement violation SWC-123
27:1 warning Unused state variable "m_appregistry" SWC-131
28:1 warning Unused state variable "m_datasetregistry" SWC-131
29:1 warning Unused state variable "m_workerpoolregistry" SWC-131
32:1 warning Unused state variable "m_baseToken" SWC-131
33:1 warning Unused state variable "m_name" SWC-131
34:1 warning Unused state variable "m_symbol" SWC-131
35:1 warning Unused state variable "m_decimals" SWC-131
36:1 warning Unused state variable "m_totalSupply" SWC-131
37:1 warning Unused state variable "m_balances" SWC-131
38:1 warning Unused state variable "m_frozens" SWC-131
39:1 warning Unused state variable "m_allowances" SWC-131
50:1 warning Unused state variable "EIP712DOMAIN_SEPARATOR" SWC-131
53:1 warning Unused state variable "m_presigned" SWC-131
54:1 warning Unused state variable "m_consumed" SWC-131
55:1 warning Unused state variable "m_deals" SWC-131
56:1 warning Unused state variable "m_tasks" SWC-131
57:1 warning Unused state variable "m_consensus" SWC-131
58:1 warning Unused state variable "m_contributions" SWC-131
59:1 warning Unused state variable "m_workerScores" SWC-131
62:1 warning Unused state variable "m_teebroker" SWC-131
63:1 warning Unused state variable "m_callbackgas" SWC-131
66:1 warning Unused state variable "m_categories" SWC-131
69:1 warning Unused state variable "m_v3_iexecHub" SWC-131
70:1 warning Unused state variable "m_v3_scoreImported" SWC-131
72:40 error The binary subtraction can underflow SWC-101
72:3411 error integer overflow SWC-101
72:8887 error integer overflow SWC-101
72:10957 error integer overflow SWC-101
72:15134 error The binary addition can overflow SWC-101
72:15216 error The binary addition can overflow SWC-101
72:15305 error The binary addition can overflow SWC-101
72:15400 error The binary subtraction can underflow SWC-101
```

/poco-dev/contracts/libs/iexecliborders_v5.sol

```
140:24 warning Potentially unbounded data structure passed to builtin SWC-128
141:24 warning Potentially unbounded data structure passed to builtin SWC-128
287:29 warning Potentially unbounded data structure passed to builtin SWC-128
355:9 warning The caller can jump to any point in the code SWC-127
```

/poco-dev/contracts/registries/workerpools/workerpool.sol

```
6:27 error integer overflow SWC-101
```

/poco-dev@iexec/solidity/contracts/erc1538/erc1538store.sol

```
8:2 warning Unused state variable "m_funcs" SWC-131
```

/poco-devsolstruct/contracts/libs/libmap2.bytes4.address.bytes.sol

```
16:7 warning Implicit loop over unbounded data structure SWC-128
```

```

37:28 warning Implicit loop over unbounded data structure SWC-128
39:67 warning Implicit loop over unbounded data structure SWC-128
44:0 warning Loop over unbounded data structure SWC-128
45:20 warning Implicit loop over unbounded data structure SWC-128

/poco-devsolstruct/contracts/libs/libset.bytes4.sol
17:33 warning Implicit loop over unbounded data structure SWC-128
36:30 warning Loop over unbounded data structure SWC-128
37:61 warning Implicit loop over unbounded data structure SWC-128

/poco-dev/contracts/modules/delegates/iexecaccessorsabilegacydelegate.sol
11:43 error integer overflow SWC-101
19:34 error integer overflow SWC-101
24:39 error integer overflow SWC-101
43:16 error integer overflow SWC-101
56:12 warning assertion violation SWC-110

/poco-dev/contracts/modules/delegates/iexecaccessorsdelegate.sol
4:59 warning Incorrect ERC20 implementation SWC-000
8:15 error integer overflow SWC-101
10:30 error integer overflow SWC-101
32:20 error integer overflow SWC-101
42:1 error integer overflow SWC-101
53:56 warning assertion violation SWC-110

/poco-dev/contracts/modules/delegates/iexecerc20common.sol
19:55 warning Persistent state write after call SWC-107
19:71 warning Persistent state read after call SWC-107
20:23 warning Persistent state write after call SWC-107
20:45 warning Persistent state read after call SWC-107

/poco-dev/contracts/modules/delegates/iexecerc20delegate.sol
18:33 warning requirement violation SWC-123

/poco-dev/contracts/modules/delegates/iexecescrownativedelegate.sol
45:2 warning A call to a user-supplied address is executed SWC-107

/poco-dev/contracts/modules/delegates/iexecescrowtokenddelegate.sol
47:46 warning Persistent state read after call SWC-107

/poco-dev/contracts/modules/delegates/signatureverifier.sol
21:69 warning requirement violation SWC-123

/poco-dev/contracts/tools/testing/testclient.sol
11:1 warning Implicit loop over unbounded data structure SWC-128
21:2 warning Implicit loop over unbounded data structure SWC-128

✘ 114 problems (41 errors, 73 warnings)

```

A.3.2 Ethlint

[Ethlint](#) is an open source project for linting Solidity code. Only security-related issues were reviewed by the audit team.

Below is the raw output of the Ethlint vulnerability scan per repository.

Linting For `iexec-solidity` Repository

```
contracts/ENStools/ENSReverseRegistration.sol
  16:1  error    Only use indent of 4 spaces.  indentation
  18:1  error    Only use indent of 4 spaces.  indentation
  22:0  error    Only use indent of 4 spaces.  indentation

contracts/ERC1271/IERC1271.sol
  3:1   error    Syntax error: unexpected token a

contracts/ERC1538/ERC1538.sol
  8:1   error    Only use indent of 4 spaces.
indentation
  9:1   error    Only use indent of 4 spaces.
indentation
  11:1  error    Only use indent of 4 spaces.
indentation
  12:1  error    Only use indent of 4 spaces.
indentation
  14:1  error    Only use indent of 4 spaces.
indentation
  18:0  error    Only use indent of 4 spaces.
indentation
  20:1  error    Only use indent of 4 spaces.
indentation
  24:27 warning  There should be no whitespace or comments between the opening
brace '{' and first item.  whitespace
  24:56 warning  There should be no whitespace or comments between the last item
and closing brace '}'.  whitespace
  25:27 warning  There should be no whitespace or comments between the opening
brace '{' and first item.  whitespace
  25:56 warning  There should be no whitespace or comments between the last item
and closing brace '}'.  whitespace
  43:0  error    Only use indent of 4 spaces.
indentation

contracts/ERC1538/ERC1538Proxy.sol
  9:1   error    Only use indent of 4 spaces.  indentation
  10:1  error    Only use indent of 4 spaces.  indentation
  12:1  error    Only use indent of 4 spaces.  indentation
  18:0  error    Only use indent of 4 spaces.  indentation
  20:1  error    Only use indent of 4 spaces.  indentation
  25:0  error    Only use indent of 4 spaces.  indentation

contracts/ERC1538/ERC1538ProxyV2.sol
  9:1   error    Only use indent of 4 spaces.  indentation
```


10:1	error	Only use indent of 4 spaces.	indentation
12:1	error	Only use indent of 4 spaces.	indentation
18:0	error	Only use indent of 4 spaces.	indentation
20:1	error	Only use indent of 4 spaces.	indentation
25:0	error	Only use indent of 4 spaces.	indentation

contracts/ERC1538/ERC1538Query.sol

20:1	error	Only use indent of 4 spaces.	indentation
24:0	error	Only use indent of 4 spaces.	indentation
26:1	error	Only use indent of 4 spaces.	indentation
31:0	error	Only use indent of 4 spaces.	indentation
33:1	error	Only use indent of 4 spaces.	indentation
37:0	error	Only use indent of 4 spaces.	indentation
39:1	error	Only use indent of 4 spaces.	indentation
43:0	error	Only use indent of 4 spaces.	indentation
45:1	error	Only use indent of 4 spaces.	indentation
49:0	error	Only use indent of 4 spaces.	indentation
51:1	error	Only use indent of 4 spaces.	indentation
75:0	error	Only use indent of 4 spaces.	indentation
77:1	error	Only use indent of 4 spaces.	indentation
86:4	error	Variable 'funcId' is declared but never used.	no-unused-vars
110:0	error	Only use indent of 4 spaces.	indentation
112:1	error	Only use indent of 4 spaces.	indentation
143:0	error	Only use indent of 4 spaces.	indentation

contracts/ERC1538/ERC1538Store.sol

8:1	error	Only use indent of 4 spaces.	indentation
10:1	error	Only use indent of 4 spaces.	indentation

contracts/ERC1538/ERC1538Update.sol

13:1	error	Only use indent of 4 spaces.	indentation
27:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
30:2	error	Avoid using Inline Assembly.	security/no-inline-assembly
38:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
42:4	error	Avoid using Inline Assembly.	security/no-inline-assembly
46:4	error	Avoid using Inline Assembly.	security/no-inline-assembly
51:0	error	Only use indent of 4 spaces.	indentation

contracts/ERC1538/ERC1538UpdateV2.sol

14:1	error	Only use indent of 4 spaces.	indentation
24:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
32:0	error	Only use indent of 4 spaces.	indentation

contracts/ERC734/IERC734.sol

3:1	error	Syntax error: unexpected token a	
-----	-------	----------------------------------	--

contracts/Factory/CounterfactualFactory.sol

6:1	error	Only use indent of 4 spaces.	indentation
19:0	error	Only use indent of 4 spaces.	indentation
21:1	error	Only use indent of 4 spaces.	indentation
30:0	error	Only use indent of 4 spaces.	indentation

contracts/Factory/GenericFactory.sol

8:1	error	Only use indent of 4 spaces.	indentation
10:1	error	Only use indent of 4 spaces.	indentation
14:0	error	Only use indent of 4 spaces.	indentation
16:1	error	Only use indent of 4 spaces.	indentation
20:0	error	Only use indent of 4 spaces.	indentation
22:1	error	Only use indent of 4 spaces.	indentation
26:0	error	Only use indent of 4 spaces.	indentation
28:1	error	Only use indent of 4 spaces.	indentation
40:0	error	Only use indent of 4 spaces.	indentation

contracts/Libs/ECDSA.sol

6:1	error	Only use indent of 4 spaces.	indentation
11:0	error	Only use indent of 4 spaces.	indentation
13:1	error	Only use indent of 4 spaces.	indentation
16:2	warning	Provide an error message for require()	error-reason
18:0	error	Only use indent of 4 spaces.	indentation
20:1	error	Only use indent of 4 spaces.	indentation
29:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
38:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
51:2	warning	Provide an error message for require()	error-reason
53:0	error	Only use indent of 4 spaces.	indentation
55:1	error	Only use indent of 4 spaces.	indentation
59:0	error	Only use indent of 4 spaces.	indentation
61:1	error	Only use indent of 4 spaces.	indentation
65:0	error	Only use indent of 4 spaces.	indentation

contracts/Libs/ECDSALib.sol

6:1	error	Only use indent of 4 spaces.	indentation
11:0	error	Only use indent of 4 spaces.	indentation
13:1	error	Only use indent of 4 spaces.	indentation
16:2	warning	Provide an error message for require()	error-reason
18:0	error	Only use indent of 4 spaces.	indentation
20:1	error	Only use indent of 4 spaces.	indentation
29:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
38:3	error	Avoid using Inline Assembly.	security/no-inline-assembly
51:2	warning	Provide an error message for require()	error-reason
53:0	error	Only use indent of 4 spaces.	indentation
55:1	error	Only use indent of 4 spaces.	indentation
59:0	error	Only use indent of 4 spaces.	indentation
61:1	error	Only use indent of 4 spaces.	indentation
65:0	error	Only use indent of 4 spaces.	indentation

contracts/Libs/SafeMathExtended.sol

12:1	error	Only use indent of 4 spaces.	indentation
15:2	warning	Provide an error message for require()	error-reason
17:0	error	Only use indent of 4 spaces.	indentation
22:1	error	Only use indent of 4 spaces.	indentation

24:2	warning	Provide an error message for require()	error-reason
27:0	error	Only use indent of 4 spaces.	indentation
32:1	error	Only use indent of 4 spaces.	indentation
42:2	warning	Provide an error message for require()	error-reason
44:0	error	Only use indent of 4 spaces.	indentation
49:1	error	Only use indent of 4 spaces.	indentation
52:3	warning	Provide an error message for require()	error-reason
56:0	error	Only use indent of 4 spaces.	indentation
62:1	error	Only use indent of 4 spaces.	indentation
64:2	warning	Provide an error message for require()	error-reason
66:0	error	Only use indent of 4 spaces.	indentation
71:1	error	Only use indent of 4 spaces.	indentation
74:0	error	Only use indent of 4 spaces.	indentation
79:1	error	Only use indent of 4 spaces.	indentation
82:0	error	Only use indent of 4 spaces.	indentation
87:1	error	Only use indent of 4 spaces.	indentation
90:0	error	Only use indent of 4 spaces.	indentation
95:1	error	Only use indent of 4 spaces.	indentation
98:0	error	Only use indent of 4 spaces.	indentation
104:1	error	Only use indent of 4 spaces.	indentation
106:2	error	Avoid using Inline Assembly.	security/no-inline-assembly
135:0	error	Only use indent of 4 spaces.	indentation
contracts/Libs/SignatureVerifier.sol			
10:1	error	Only use indent of 4 spaces.	indentation
12:1	error	Only use indent of 4 spaces.	indentation
16:2	error	Avoid using Inline Assembly.	security/no-inline-assembly
18:0	error	Only use indent of 4 spaces.	indentation
20:1	error	Only use indent of 4 spaces.	indentation
24:0	error	Only use indent of 4 spaces.	indentation
26:1	error	Only use indent of 4 spaces.	indentation
29:2	warning	Line exceeds the limit of 145 characters	max-len
30:0	error	Only use indent of 4 spaces.	indentation
32:1	error	Only use indent of 4 spaces.	indentation
43:0	error	Only use indent of 4 spaces.	indentation
contracts/TestContract.sol			
12:9	error	Syntax error: unexpected token (
contracts/Upgradeability/BaseUpgradeabilityProxy.sol			
3:7	error	"@openzeppelin/contracts/Utils/Address.sol": Import statements must use double quotes only.	quotes
4:7	error	"./Proxy.sol": Import statements must use double quotes only.	quotes
17:2	error	Only use indent of 4 spaces.	indentation
24:2	error	Only use indent of 4 spaces.	indentation
30:2	error	Only use indent of 4 spaces.	indentation

```

32:4    error    Avoid using Inline Assembly.
security/no-inline-assembly
35:0    error    Only use indent of 4 spaces.
indentation
41:2    error    Only use indent of 4 spaces.
indentation
44:0    error    Only use indent of 4 spaces.
indentation
50:2    error    Only use indent of 4 spaces.
indentation
55:4    error    Avoid using Inline Assembly.
security/no-inline-assembly
58:0    error    Only use indent of 4 spaces.
indentation

contracts/Upgradeability/InitializableUpgradeabilityProxy.sol
3:7     error    "./BaseUpgradeabilityProxy.sol": Import statements must use
double quotes only.    quotes
19:2    error    Only use indent of 4 spaces.
indentation
20:4    warning   Provide an error message for require()
error-reason
24:6    error    Only use indent of 8 spaces.
indentation
24:31   warning   Avoid using low-level function 'delegatecall'.
security/no-low-level-calls
25:6    error    Only use indent of 8 spaces.
indentation
25:6    warning   Provide an error message for require()
error-reason
27:0    error    Only use indent of 4 spaces.
indentation

contracts/Upgradeability/Proxy.sol
10:1    error    Syntax error: unexpected token a

✘ 141 errors, 17 warnings found.

```

Linting For `poco-dev` Repository

```

contracts/IexecInterfaceNative.sol
17:32   error    Syntax error: unexpected token i

contracts/IexecInterfaceNativeABILegacy.sol
18:41   error    Syntax error: unexpected token i

contracts/IexecInterfaceToken.sol
17:31   error    Syntax error: unexpected token i

contracts/IexecInterfaceTokenABILegacy.sol

```

18:40 error Syntax error: unexpected token i

contracts/Store.sol

24:1 error Syntax error: unexpected token a

contracts/libs/IexecLibCore_v5.sol

9:1 error Only use indent of 4 spaces. indentation

13:0 error Only use indent of 4 spaces. indentation

14:1 error Only use indent of 4 spaces. indentation

19:0 error Only use indent of 4 spaces. indentation

24:1 error Only use indent of 4 spaces. indentation

29:0 error Only use indent of 4 spaces. indentation

30:1 error Only use indent of 4 spaces. indentation

51:0 error Only use indent of 4 spaces. indentation

56:1 error Only use indent of 4 spaces. indentation

63:0 error Only use indent of 4 spaces. indentation

64:1 error Only use indent of 4 spaces. indentation

80:0 error Only use indent of 4 spaces. indentation

85:1 error Only use indent of 4 spaces. indentation

89:0 error Only use indent of 4 spaces. indentation

94:1 error Only use indent of 4 spaces. indentation

100:0 error Only use indent of 4 spaces. indentation

101:1 error Only use indent of 4 spaces. indentation

108:0 error Only use indent of 4 spaces. indentation

contracts/libs/IexecLibOrders_v5.sol

7:1 warning Line exceeds the limit of 145 characters
max-len

7:1 error Only use indent of 4 spaces.
indentation

8:1 error Only use indent of 4 spaces.
indentation

8:1 warning Line exceeds the limit of 145 characters
max-len

9:1 warning Line exceeds the limit of 145 characters
max-len

9:1 error Only use indent of 4 spaces.
indentation

10:1 warning Line exceeds the limit of 145 characters
max-len

10:1 error Only use indent of 4 spaces.
indentation

11:1 error Only use indent of 4 spaces.
indentation

11:1 warning Line exceeds the limit of 145 characters
max-len

12:1 warning Line exceeds the limit of 145 characters
max-len

12:1 error Only use indent of 4 spaces.
indentation

13:1 error Only use indent of 4 spaces.
indentation

13:1	warning	Line exceeds the limit of 145 characters
max-len		
14:1	warning	Line exceeds the limit of 145 characters
max-len		
14:1	error	Only use indent of 4 spaces.
indentation		
15:1	error	Only use indent of 4 spaces.
indentation		
15:1	warning	Line exceeds the limit of 145 characters
max-len		
17:1	error	Only use indent of 4 spaces.
indentation		
21:0	error	Only use indent of 4 spaces.
indentation		
23:1	error	Only use indent of 4 spaces.
indentation		
29:0	error	Only use indent of 4 spaces.
indentation		
31:1	error	Only use indent of 4 spaces.
indentation		
43:0	error	Only use indent of 4 spaces.
indentation		
45:1	error	Only use indent of 4 spaces.
indentation		
57:0	error	Only use indent of 4 spaces.
indentation		
59:1	error	Only use indent of 4 spaces.
indentation		
73:0	error	Only use indent of 4 spaces.
indentation		
75:1	error	Only use indent of 4 spaces.
indentation		
94:0	error	Only use indent of 4 spaces.
indentation		
96:1	error	Only use indent of 4 spaces.
indentation		
101:0	error	Only use indent of 4 spaces.
indentation		
103:1	error	Only use indent of 4 spaces.
indentation		
108:0	error	Only use indent of 4 spaces.
indentation		
110:1	error	Only use indent of 4 spaces.
indentation		
115:0	error	Only use indent of 4 spaces.
indentation		
117:1	error	Only use indent of 4 spaces.
indentation		
122:0	error	Only use indent of 4 spaces.
indentation		
124:1	error	Only use indent of 4 spaces.
indentation		

139:2 warning Assignment operator must have exactly single space on both sides of it. operator-whitespace

140:2 warning Assignment operator must have exactly single space on both sides of it. operator-whitespace

142:2 error Avoid using Inline Assembly. security/no-inline-assembly

158:0 error Only use indent of 4 spaces. indentation

160:1 error Only use indent of 4 spaces. indentation

180:2 error Avoid using Inline Assembly. security/no-inline-assembly

190:0 error Only use indent of 4 spaces. indentation

192:1 error Only use indent of 4 spaces. indentation

212:2 error Avoid using Inline Assembly. security/no-inline-assembly

222:0 error Only use indent of 4 spaces. indentation

224:1 error Only use indent of 4 spaces. indentation

246:2 error Avoid using Inline Assembly. security/no-inline-assembly

256:0 error Only use indent of 4 spaces. indentation

258:1 error Only use indent of 4 spaces. indentation

288:2 error Avoid using Inline Assembly. security/no-inline-assembly

301:0 error Only use indent of 4 spaces. indentation

303:1 error Only use indent of 4 spaces. indentation

311:0 error Only use indent of 4 spaces. indentation

313:1 error Only use indent of 4 spaces. indentation

321:0 error Only use indent of 4 spaces. indentation

323:1 error Only use indent of 4 spaces. indentation

331:0 error Only use indent of 4 spaces. indentation

333:1 error Only use indent of 4 spaces. indentation

341:0 error Only use indent of 4 spaces. indentation

343:1 error Only use indent of 4 spaces. indentation

347:0 error Only use indent of 4 spaces. indentation

```
349:1 error Only use indent of 4 spaces.
indentation
353:0 error Only use indent of 4 spaces.
indentation
355:1 error Only use indent of 4 spaces.
indentation
364:3 error Avoid using Inline Assembly.
security/no-inline-assembly
373:3 error Avoid using Inline Assembly.
security/no-inline-assembly
388:0 error Only use indent of 4 spaces.
indentation
```

contracts/modules/DelegateBase.sol

```
6:1 error Syntax error: unexpected token a
```

contracts/modules/delegates/ENSIntegrationDelegate.sol

```
11:1 error Only use indent of 4 spaces. indentation
15:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol

```
10:1 error Only use indent of 4 spaces. indentation
35:0 error Only use indent of 4 spaces. indentation
37:1 error Only use indent of 4 spaces. indentation
56:0 error Only use indent of 4 spaces. indentation
58:1 error Only use indent of 4 spaces. indentation
77:0 error Only use indent of 4 spaces. indentation
79:1 error Only use indent of 4 spaces. indentation
83:0 error Only use indent of 4 spaces. indentation
85:1 error Only use indent of 4 spaces. indentation
116:0 error Only use indent of 4 spaces. indentation
118:1 error Only use indent of 4 spaces. indentation
133:0 error Only use indent of 4 spaces. indentation
135:1 error Only use indent of 4 spaces. indentation
140:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecAccessorsDelegate.sol

```
11:1 error Only use indent of 4 spaces. indentation
15:0 error Only use indent of 4 spaces. indentation
17:1 error Only use indent of 4 spaces. indentation
21:0 error Only use indent of 4 spaces. indentation
23:1 error Only use indent of 4 spaces. indentation
27:0 error Only use indent of 4 spaces. indentation
29:1 error Only use indent of 4 spaces. indentation
33:0 error Only use indent of 4 spaces. indentation
35:1 error Only use indent of 4 spaces. indentation
39:0 error Only use indent of 4 spaces. indentation
41:1 error Only use indent of 4 spaces. indentation
45:0 error Only use indent of 4 spaces. indentation
47:1 error Only use indent of 4 spaces. indentation
51:0 error Only use indent of 4 spaces. indentation
53:1 error Only use indent of 4 spaces. indentation
```

57:0	error	Only use indent of 4 spaces.	indentation
59:1	error	Only use indent of 4 spaces.	indentation
63:0	error	Only use indent of 4 spaces.	indentation
65:1	error	Only use indent of 4 spaces.	indentation
69:0	error	Only use indent of 4 spaces.	indentation
71:1	error	Only use indent of 4 spaces.	indentation
75:0	error	Only use indent of 4 spaces.	indentation
77:1	error	Only use indent of 4 spaces.	indentation
81:0	error	Only use indent of 4 spaces.	indentation
83:1	error	Only use indent of 4 spaces.	indentation
87:0	error	Only use indent of 4 spaces.	indentation
89:1	error	Only use indent of 4 spaces.	indentation
93:0	error	Only use indent of 4 spaces.	indentation
95:1	error	Only use indent of 4 spaces.	indentation
99:0	error	Only use indent of 4 spaces.	indentation
101:1	error	Only use indent of 4 spaces.	indentation
105:2	warning	Provide an error message for require()	error-reason
107:0	error	Only use indent of 4 spaces.	indentation
109:1	error	Only use indent of 4 spaces.	indentation
113:0	error	Only use indent of 4 spaces.	indentation
115:1	error	Only use indent of 4 spaces.	indentation
119:0	error	Only use indent of 4 spaces.	indentation
122:1	error	Only use indent of 4 spaces.	indentation
126:0	error	Only use indent of 4 spaces.	indentation
128:1	error	Only use indent of 4 spaces.	indentation
132:0	error	Only use indent of 4 spaces.	indentation
134:1	error	Only use indent of 4 spaces.	indentation
138:0	error	Only use indent of 4 spaces.	indentation
140:1	error	Only use indent of 4 spaces.	indentation
144:0	error	Only use indent of 4 spaces.	indentation
146:1	error	Only use indent of 4 spaces.	indentation
150:0	error	Only use indent of 4 spaces.	indentation
152:1	error	Only use indent of 4 spaces.	indentation
156:0	error	Only use indent of 4 spaces.	indentation
158:1	error	Only use indent of 4 spaces.	indentation
162:0	error	Only use indent of 4 spaces.	indentation
164:1	error	Only use indent of 4 spaces.	indentation
168:0	error	Only use indent of 4 spaces.	indentation
170:1	error	Only use indent of 4 spaces.	indentation
174:0	error	Only use indent of 4 spaces.	indentation
176:1	error	Only use indent of 4 spaces.	indentation
180:0	error	Only use indent of 4 spaces.	indentation
182:1	error	Only use indent of 4 spaces.	indentation
186:0	error	Only use indent of 4 spaces.	indentation
188:1	error	Only use indent of 4 spaces.	indentation
192:0	error	Only use indent of 4 spaces.	indentation
194:1	error	Only use indent of 4 spaces.	indentation
198:0	error	Only use indent of 4 spaces.	indentation
200:1	error	Only use indent of 4 spaces.	indentation
204:0	error	Only use indent of 4 spaces.	indentation


```
13:1 error Only use indent of 4 spaces. indentation
34:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecERC20Common.sol

```
9:1 error Only use indent of 4 spaces. indentation
11:1 error Only use indent of 4 spaces. indentation
12:1 error Only use indent of 4 spaces. indentation
14:1 error Only use indent of 4 spaces. indentation
23:0 error Only use indent of 4 spaces. indentation
25:1 error Only use indent of 4 spaces. indentation
33:0 error Only use indent of 4 spaces. indentation
35:1 error Only use indent of 4 spaces. indentation
43:0 error Only use indent of 4 spaces. indentation
45:1 error Only use indent of 4 spaces. indentation
53:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecERC20Delegate.sol

```
12:1 error Only use indent of 4 spaces. indentation
17:0 error Only use indent of 4 spaces. indentation
19:1 error Only use indent of 4 spaces. indentation
24:0 error Only use indent of 4 spaces. indentation
26:1 error Only use indent of 4 spaces. indentation
30:102 error String literal must be quoted with double quotes. quotes
32:0 error Only use indent of 4 spaces. indentation
34:1 error Only use indent of 4 spaces. indentation
40:0 error Only use indent of 4 spaces. indentation
42:1 error Only use indent of 4 spaces. indentation
47:0 error Only use indent of 4 spaces. indentation
50:1 error Only use indent of 4 spaces. indentation
55:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecEscrowNativeDelegate.sol

```
17:9 error Syntax error: unexpected token (
```

contracts/modules/delegates/IexecEscrowTokenDelegate.sol

```
17:9 error Syntax error: unexpected token (
```

contracts/modules/delegates/IexecMaintenanceDelegate.sol

```
10:1 error Only use indent of 4 spaces.
indentation
11:1 error Only use indent of 4 spaces.
indentation
13:1 error Only use indent of 4 spaces.
indentation
27:2 warning Assignment operator must have exactly single space on both
sides of it. operator-whitespace
28:2 warning Assignment operator must have exactly single space on both
sides of it. operator-whitespace
29:2 warning Assignment operator must have exactly single space on both
sides of it. operator-whitespace
30:2 warning Assignment operator must have exactly single space on both
sides of it. operator-whitespace
```

31:2	warning	Assignment operator must have exactly single space on both sides of it.	operator-whitespace
32:2	warning	Assignment operator must have exactly single space on both sides of it.	operator-whitespace
34:2	warning	Assignment operator must have exactly single space on both sides of it.	operator-whitespace
35:2	warning	Assignment operator must have exactly single space on both sides of it.	operator-whitespace
36:0	error	Only use indent of 4 spaces.	
		indentation	
38:1	error	Only use indent of 4 spaces.	
		indentation	
42:0	error	Only use indent of 4 spaces.	
		indentation	
44:1	error	Only use indent of 4 spaces.	
		indentation	
49:0	error	Only use indent of 4 spaces.	
		indentation	
51:1	error	Only use indent of 4 spaces.	
		indentation	
57:0	error	Only use indent of 4 spaces.	
		indentation	
59:1	error	Only use indent of 4 spaces.	
		indentation	
63:0	error	Only use indent of 4 spaces.	
		indentation	
65:1	error	Only use indent of 4 spaces.	
		indentation	
69:0	error	Only use indent of 4 spaces.	
		indentation	
71:1	error	Only use indent of 4 spaces.	
		indentation	
74:2	error	Avoid using Inline Assembly.	
		security/no-inline-assembly	
75:0	error	Only use indent of 4 spaces.	
		indentation	
77:1	error	Only use indent of 4 spaces.	
		indentation	
81:4	warning	Name 'name': Only "N: V", "N : V" or "N:V" spacing style should be used in Name-Value Mapping.	whitespace
81:32	warning	"iExecODB" should be immediately followed by a comma, then an optional space.	whitespace
82:5	warning	Name 'version': Only "N: V", "N : V" or "N:V" spacing style should be used in Name-Value Mapping.	whitespace
82:34	warning	"3.0-alpha" should be immediately followed by a comma, then an optional space.	whitespace
83:5	warning	Name 'chainId': Only "N: V", "N : V" or "N:V" spacing style should be used in Name-Value Mapping.	whitespace
83:33	warning	"_chainId()" should be immediately followed by a comma, then an optional space.	whitespace
86:0	error	Only use indent of 4 spaces.	
		indentation	

contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol

```
10:1 error Only use indent of 4 spaces.
indentation
16:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
17:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
19:0 error Only use indent of 4 spaces.
indentation
```

contracts/modules/delegates/IexecOrderManagementDelegate.sol

```
10:1 error Only use indent of 4 spaces. indentation
11:1 error Only use indent of 4 spaces. indentation
12:1 error Only use indent of 4 spaces. indentation
13:1 error Only use indent of 4 spaces. indentation
14:1 error Only use indent of 4 spaces. indentation
15:1 error Only use indent of 4 spaces. indentation
16:1 error Only use indent of 4 spaces. indentation
17:1 error Only use indent of 4 spaces. indentation
18:1 error Only use indent of 4 spaces. indentation
23:1 error Only use indent of 4 spaces. indentation
27:2 warning Provide an error message for require() error-reason
27:2 warning Line exceeds the limit of 145 characters max-len
40:0 error Only use indent of 4 spaces. indentation
42:1 error Only use indent of 4 spaces. indentation
46:2 warning Line exceeds the limit of 145 characters max-len
46:2 warning Provide an error message for require() error-reason
59:0 error Only use indent of 4 spaces. indentation
61:1 error Only use indent of 4 spaces. indentation
65:2 warning Provide an error message for require() error-reason
65:2 warning Line exceeds the limit of 145 characters max-len
78:0 error Only use indent of 4 spaces. indentation
80:1 error Only use indent of 4 spaces. indentation
84:2 warning Line exceeds the limit of 145 characters max-len
84:2 warning Provide an error message for require() error-reason
97:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/delegates/IexecPocoDelegate.sol

```
773:23 error Syntax error: unexpected token (
```

contracts/modules/delegates/IexecRelayDelegate.sol

```
10:1 warning Line exceeds the limit of 145 characters
max-len
10:1 error Only use indent of 4 spaces.
indentation
10:155 warning 'BroadcastAppOrder': The last argument must not be succeeded
by any whitespace or comments (only ' '). function-whitespace
11:1 warning Line exceeds the limit of 145 characters
max-len
11:1 error Only use indent of 4 spaces.
indentation
```

```
11:159 warning 'BroadcastDatasetOrder': The last argument must not be
succeeded by any whitespace or comments (only ' '). function-whitespace
12:1 error Only use indent of 4 spaces.
indentation
12:1 warning Line exceeds the limit of 145 characters
max-len
13:1 warning Line exceeds the limit of 145 characters
max-len
13:1 error Only use indent of 4 spaces.
indentation
13:159 warning 'BroadcastRequestOrder': The last argument must not be
succeeded by any whitespace or comments (only ' '). function-whitespace
```

contracts/modules/delegates/SignatureVerifier.sol

```
11:1 error Only use indent of 4 spaces. indentation
13:1 error Only use indent of 4 spaces. indentation
15:1 error Only use indent of 4 spaces. indentation
19:2 error Avoid using Inline Assembly. security/no-inline-
assembly
21:0 error Only use indent of 4 spaces. indentation
23:1 error Only use indent of 4 spaces. indentation
27:0 error Only use indent of 4 spaces. indentation
29:1 error Only use indent of 4 spaces. indentation
32:2 warning Line exceeds the limit of 145 characters max-len
33:0 error Only use indent of 4 spaces. indentation
35:1 error Only use indent of 4 spaces. indentation
46:0 error Only use indent of 4 spaces. indentation
48:1 error Only use indent of 4 spaces. indentation
52:0 error Only use indent of 4 spaces. indentation
54:1 error Only use indent of 4 spaces. indentation
58:0 error Only use indent of 4 spaces. indentation
```

contracts/modules/interfaces/IexecAccessors.sol

```
8:26 error Syntax error: unexpected token i
```

contracts/modules/interfaces/IexecEscrowNative.sol

```
7:9 error Syntax error: unexpected token (
```

contracts/modules/interfaces/IexecEscrowToken.sol

```
7:9 error Syntax error: unexpected token (
```

contracts/modules/interfaces/IexecPoco.sol

```
31:1 warning Line exceeds the limit of 145 characters max-len
```

contracts/registries/IRegistry.sol

```
6:1 error Syntax error: unexpected token a
```

contracts/registries/Registry.sol

```
13:1 error Only use indent of 4 spaces.
indentation
14:1 error Only use indent of 4 spaces.
indentation
```

```
15:1 error Only use indent of 4 spaces.
indentation
16:1 error Only use indent of 4 spaces.
indentation
17:1 error Only use indent of 4 spaces.
indentation
19:1 error Only use indent of 4 spaces.
indentation
22:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
23:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
25:0 error Only use indent of 4 spaces.
indentation
27:1 error Only use indent of 4 spaces.
indentation
30:2 warning Provide an error message for require()
error-reason
32:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
33:0 error Only use indent of 4 spaces.
indentation
36:1 error Only use indent of 4 spaces.
indentation
48:0 error Only use indent of 4 spaces.
indentation
50:1 error Only use indent of 4 spaces.
indentation
57:0 error Only use indent of 4 spaces.
indentation
60:1 error Only use indent of 4 spaces.
indentation
64:0 error Only use indent of 4 spaces.
indentation
66:1 error Only use indent of 4 spaces.
indentation
70:0 error Only use indent of 4 spaces.
indentation
72:1 error Only use indent of 4 spaces.
indentation
77:0 error Only use indent of 4 spaces.
indentation
```

contracts/registries/RegistryEntry.sol

```
7:1 error Syntax error: unexpected token a
```

contracts/registries/apps/App.sol

```
11:1 error Only use indent of 4 spaces.
indentation
```

```
12:1 error Only use indent of 4 spaces.
indentation
```

```
13:1 error Only use indent of 4 spaces.
```

```
indentation
  14:1    error    Only use indent of 4 spaces.
indentation
  15:1    error    Only use indent of 4 spaces.
indentation
  20:1    error    Only use indent of 4 spaces.
indentation
  29:2    warning   Assignment operator must have exactly single space on both sides
of it.   operator-whitespace
  30:2    warning   Assignment operator must have exactly single space on both sides
of it.   operator-whitespace
  32:2    warning   Assignment operator must have exactly single space on both sides
of it.   operator-whitespace
  34:0    error    Only use indent of 4 spaces.
indentation

contracts/registries/apps/AppRegistry.sol
  3:7    error    "../Registry.sol": Import statements must use double quotes only.
quotes
  4:7    error    "../App.sol": Import statements must use double quotes only.
quotes
  12:1   error    Only use indent of 4 spaces.
indentation
  18:0   error    Only use indent of 4 spaces.
indentation
  23:1   error    Only use indent of 4 spaces.
indentation
  39:0   error    Only use indent of 4 spaces.
indentation
  41:1   error    Only use indent of 4 spaces.
indentation
  51:0   error    Only use indent of 4 spaces.
indentation
  53:1   error    Only use indent of 4 spaces.
indentation
  63:0   error    Only use indent of 4 spaces.
indentation

contracts/registries/datasets/Dataset.sol
  11:1   error    Only use indent of 4 spaces.
indentation
  12:1   error    Only use indent of 4 spaces.
indentation
  13:1   error    Only use indent of 4 spaces.
indentation
  18:1   error    Only use indent of 4 spaces.
indentation
  25:2   warning   Assignment operator must have exactly single space on both sides
of it.   operator-whitespace
  27:2   warning   Assignment operator must have exactly single space on both sides
of it.   operator-whitespace
  28:0   error    Only use indent of 4 spaces.
```

indentation

contracts/registries/datasets/DatasetRegistry.sol

3:7 error `"../Registry.sol"`: Import statements must use double quotes only.
quotes

4:7 error `"../Dataset.sol"`: Import statements must use double quotes only.
quotes

12:1 error Only use indent of 4 spaces.

indentation

18:0 error Only use indent of 4 spaces.

indentation

23:1 error Only use indent of 4 spaces.

indentation

35:0 error Only use indent of 4 spaces.

indentation

37:1 error Only use indent of 4 spaces.

indentation

45:0 error Only use indent of 4 spaces.

indentation

47:1 error Only use indent of 4 spaces.

indentation

55:0 error Only use indent of 4 spaces.

indentation

contracts/registries/workerpools/Workerpool.sol

11:1 error Only use indent of 4 spaces.

indentation

12:1 error Only use indent of 4 spaces.

indentation

13:1 error Only use indent of 4 spaces.

indentation

18:1 error Only use indent of 4 spaces.

indentation

20:0 error Only use indent of 4 spaces.

indentation

25:1 error Only use indent of 4 spaces.

indentation

30:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace

31:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace

33:0 error Only use indent of 4 spaces.

indentation

35:1 error Only use indent of 4 spaces.

indentation

40:2 warning Provide an error message for `require()`

error-reason

47:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace

49:0 error Only use indent of 4 spaces.

indentation

contracts/registries/workerpools/WorkerpoolRegistry.sol

3:7 error "../Registry.sol": Import statements must use double quotes only.
quotes
4:7 error "../Workerpool.sol": Import statements must use double quotes only.
quotes
12:1 error Only use indent of 4 spaces.
indentation
18:0 error Only use indent of 4 spaces.
indentation
23:1 error Only use indent of 4 spaces.
indentation
31:0 error Only use indent of 4 spaces.
indentation
33:1 error Only use indent of 4 spaces.
indentation
39:0 error Only use indent of 4 spaces.
indentation
41:1 error Only use indent of 4 spaces.
indentation
47:0 error Only use indent of 4 spaces.
indentation

contracts/tools/Migrations.sol

8:1 error Only use indent of 4 spaces. indentation
10:1 error Only use indent of 4 spaces. indentation
12:1 warning Code contains empty block no-empty-blocks
13:0 error Only use indent of 4 spaces. indentation
15:1 error Only use indent of 4 spaces. indentation
18:0 error Only use indent of 4 spaces. indentation
20:1 error Only use indent of 4 spaces. indentation
24:0 error Only use indent of 4 spaces. indentation

contracts/tools/testing/TestClient.sol

8:1 error Only use indent of 4 spaces.
indentation
10:1 error Only use indent of 4 spaces.
indentation
11:1 error Only use indent of 4 spaces.
indentation
13:1 error Only use indent of 4 spaces.
indentation
15:1 warning Code contains empty block
no-empty-blocks
16:0 error Only use indent of 4 spaces.
indentation
18:1 error Only use indent of 4 spaces.
indentation
21:2 warning Assignment operator must have exactly single space on both sides
of it. operator-whitespace
23:0 error Only use indent of 4 spaces.
indentation


```

contracts/tools/testing/TestReceiver.sol
  8:1      error      Only use indent of 4 spaces.      indentation
 10:1      error      Only use indent of 4 spaces.      indentation
 12:1      warning     Code contains empty block        no-empty-blocks
 13:0      error      Only use indent of 4 spaces.      indentation
 15:1      error      Only use indent of 4 spaces.      indentation
 31:0      error      Only use indent of 4 spaces.      indentation

✘ 344 errors, 62 warnings found.

```

A.3.3 Surya

Surya is a utility tool for smart contract systems. It provides a number of visual outputs and information about the structure of smart contracts. It also supports querying the function call graph in multiple ways to aid in the manual inspection and control flow analysis of contracts.

Below is the tool output per repository.

Sūrya's Description Report For The `iexec-solidity` Repository

Files Description Table

File Name	SHA-1
<code>iexec-solidity/contracts/ENStools/ENSReverseRegistration.sol</code>	<code>20ea50fd7ba8fb5398281</code>
<code>iexec-solidity/contracts/ERC1154/IERC1154.sol</code>	<code>892b56dee343f68a984b</code>
<code>iexec-solidity/contracts/ERC1271/IERC1271.sol</code>	<code>4944fcc92d2ba5abf07a4</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538.sol</code>	<code>c2ff06da81513e4f0a9143</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538Proxy.sol</code>	<code>75e468f9819caace38123</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538ProxyV2.sol</code>	<code>05a295a9c62eda7d6c106</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538Query.sol</code>	<code>73f28de88815b08cdeae</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538Store.sol</code>	<code>6f8bbfd330c5cbb78bc0c</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538Update.sol</code>	<code>38a9d71ace70289423c57</code>
<code>iexec-solidity/contracts/ERC1538/ERC1538UpdateV2.sol</code>	<code>6830163504f53c40271a7</code>
<code>iexec-solidity/contracts/ERC1538/IERC1538.sol</code>	<code>2a30f324d44b77a5dda16</code>
<code>iexec-solidity/contracts/ERC725/IERC725.sol</code>	<code>14e1265d58b916e92530c</code>
<code>iexec-solidity/contracts/ERC734/IERC734.sol</code>	<code>1648464843385275d20d</code>
<code>iexec-solidity/contracts/Factory/CounterfactualFactory.sol</code>	<code>822d7cfba1ca1f2a663044</code>

File Name	SHA-1
iexec-solidity/contracts/Factory/GenericFactory.sol	45888956954bbb2c1a32
iexec-solidity/contracts/Libs/ECDSA.sol	3fa8517670e83c2219c5c
iexec-solidity/contracts/Libs/ECDSALib.sol	ea8e62fa6f1f489ecc26f15
iexec-solidity/contracts/Libs/SafeMathExtended.sol	988444bcf40be7af53d14
iexec-solidity/contracts/Libs/SignatureVerifier.sol	54f3d4406e3998d6effe3
iexec-solidity/contracts/Migrations.sol	d6a9049b9ccf34341831c
iexec-solidity/contracts/TestContract.sol	44e98d4544b0e414281a
iexec-solidity/contracts/Upgradeability/BaseUpgradeabilityProxy.sol	1d7fdce8663c7338ff9ca5
iexec-solidity/contracts/Upgradeability/InitializableUpgradeabilityProxy.sol	fae44f55f71595c17b7fc6a
iexec-solidity/contracts/Upgradeability/Proxy.sol	a6e3c5967eb838e4a79e7

Contracts Description Table

Contract	Type	Bases
L	Function Name	Visibility
IReverseRegistrar	Interface	
L	claim	External !
L	claimWithResolver	External !
L	setName	External !
L	node	External !
ENSReverseRegistration	Implementation	
L	_setName	Internal 
IOracleConsumer	Interface	
L	receiveResult	External !
IOracle	Interface	
L	resultFor	External !

Contract	Type	Bases
IERC1271	Implementation	
L	isValidSignature	Public !
ERC1538	Implementation	IERC1538, ERC1538Store
L		Public !
L	_setFunc	Internal 🔒
ERC1538Proxy	Implementation	ERC1538, Proxy
L		Public !
L	_implementation	Internal 🔒
ERC1538ProxyV2	Implementation	ERC1538, Proxy
L		Public !
L	_implementation	Internal 🔒
ERC1538Query	Interface	
L	totalFunctions	External !
L	functionByIndex	External !
L	functionById	External !
L	functionExists	External !
L	functionSignatures	External !
L	delegateFunctionSignatures	External !
L	delegateAddress	External !
L	delegateAddresses	External !
ERC1538QueryDelegate	Implementation	ERC1538Query, ERC1538
L	totalFunctions	External !
L	functionByIndex	External !
L	functionById	External !



Contract	Type	Bases
L	functionExists	External !
L	delegateAddress	External !
L	functionSignatures	External !
L	delegateFunctionSignatures	External !
L	delegateAddresses	External !
ERC1538Store	Implementation	Ownable
ERC1538Update	Interface	
L	updateContract	External !
ERC1538UpdateDelegate	Implementation	ERC1538Update, ERC1538
L	updateContract	External !
ERC1538UpdateV2	Interface	
L	updateContract	External !
ERC1538UpdateV2Delegate	Implementation	ERC1538UpdateV2, ERC1538
L	updateContract	External !
IERC1538	Interface	
IERC725	Interface	
L	getData	External !
L	setData	External !
L	execute	External !
IERC734	Implementation	
L	getKey	External !
L	keyHasPurpose	External !
L	getKeysByPurpose	External !

Contract	Type	Bases
L	addKey	External !
L	removeKey	External !
L	execute	External !
L	approve	External !
CounterfactualFactory		
	Implementation	
L	_create2	Internal 🔒
L	_predictAddress	Internal 🔒
GenericFactory		
	Implementation	CounterfactualFactory
L	predictAddress	Public !
L	createContract	Public !
L	predictAddressWithCall	Public !
L	createContractAndCall	Public !
ECDSA		
	Implementation	
L	recover	Internal 🔒
L	recover	Internal 🔒
L	toEthSignedMessageHash	Internal 🔒
L	toEthTypedStructHash	Internal 🔒
ECDSALib		
	Library	
L	recover	Public !
L	recover	Public !
L	toEthSignedMessageHash	Public !
L	toEthTypedStructHash	Public !
SafeMathExtended		
	Library	
L	add	Internal 🔒
L	sub	Internal 🔒

Contract	Type	Bases
L	mul	Internal 🔒
L	div	Internal 🔒
L	mod	Internal 🔒
L	max	Internal 🔒
L	min	Internal 🔒
L	mulByFraction	Internal 🔒
L	percentage	Internal 🔒
L	log	Internal 🔒
SignatureVerifier	Implementation	ECDSA
L	_isContract	Internal 🔒
L	_addrToKey	Internal 🔒
L	_checkIdentity	Internal 🔒
L	_checkSignature	Internal 🔒
Migrations	Implementation	
L		Public !
L	setCompleted	Public !
L	upgrade	Public !
TestContract	Implementation	
L		External !
L		External !
L	set	External !
BaseUpgradeabilityProxy	Implementation	Proxy
L	_implementation	Internal 🔒
L	_upgradeTo	Internal 🔒
L	_setImplementation	Internal 🔒

Contract	Type	Bases
InitializableUpgradeabilityProxy	Implementation	BaseUpgradeabilityProxy
L	initialize	Public !
Proxy	Implementation	
L		External !
L		External !
L	_implementation	Internal 🔒
L	_delegate	Internal 🔒
L	_willFallback	Internal 🔒
L	_fallback	Internal 🔒

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Sūrya's Description Report For The `poco-dev` Repository

Files Description Table

File Name	SHA
poco-dev/contracts/IexecInterfaceNative.sol	438599f3ace91f811c7f
poco-dev/contracts/IexecInterfaceNativeABILegacy.sol	28607ea20a6e91fcc5b9
poco-dev/contracts/IexecInterfaceToken.sol	2ea18304e61a6d88a39
poco-dev/contracts/IexecInterfaceTokenABILegacy.sol	e0541ee61d54d9034c5
poco-dev/contracts/Store.sol	b5edbo4dabdc5983a11
poco-dev/contracts/libs/IexecLibCore_v5.sol	359c785f15d6ac64197e
poco-dev/contracts/libs/IexecLibOrders_v5.sol	65d30c4d5069636495f
poco-dev/contracts/modules/DelegateBase.sol	966321486cf7049912cf
poco-dev/contracts/modules/delegates/ENSIntegrationDelegate.sol	509ad5bda5fb7896699

File Name	SHA
poco-dev/contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol	257f31816odfd6a848c4
poco-dev/contracts/modules/delegates/IexecAccessorsDelegate.sol	8bbc143e3ea0e731c6c5
poco-dev/contracts/modules/delegates/IexecCategoryManagerDelegate.sol	b42cb5c07838d5eb8d8
poco-dev/contracts/modules/delegates/IexecERC20Common.sol	54ecb31c576017c96fa7
poco-dev/contracts/modules/delegates/IexecERC20Delegate.sol	6b6e404844c727e57a1
poco-dev/contracts/modules/delegates/IexecEscrowNativeDelegate.sol	dof96ed32949a8d0726
poco-dev/contracts/modules/delegates/IexecEscrowTokenDelegate.sol	1c0177cff23a426fe40c2
poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol	1c1eef2430cc35ce3366
poco-dev/contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol	00b3b7ab05f2f790402
poco-dev/contracts/modules/delegates/IexecOrderManagementDelegate.sol	aa2f3dccf020d9c21f50
poco-dev/contracts/modules/delegates/IexecPocoDelegate.sol	a43fa6b7f4c088adfdfe
poco-dev/contracts/modules/delegates/IexecRelayDelegate.sol	096d24d4b15593ee1ce
poco-dev/contracts/modules/delegates/SignatureVerifier.sol	83160d2e5924055aa32
poco-dev/contracts/modules/interfaces/ENSIntegration.sol	f0ad54cfbc0f3f5dda20.
poco-dev/contracts/modules/interfaces/IOwnable.sol	b33a9ad33d58obb88e
poco-dev/contracts/modules/interfaces/IexecAccessors.sol	c2bff677eb8d606af569
poco-dev/contracts/modules/interfaces/IexecAccessorsABILegacy.sol	91f97256685b9101044
poco-dev/contracts/modules/interfaces/IexecCategoryManager.sol	2c0bc1c4f9e3261c4e1c
poco-dev/contracts/modules/interfaces/IexecERC20.sol	66841034833adca8c16
poco-dev/contracts/modules/interfaces/IexecEscrowNative.sol	d8847e54490a498845
poco-dev/contracts/modules/interfaces/IexecEscrowToken.sol	off3340f349dd50126d.
poco-dev/contracts/modules/interfaces/IexecMaintenance.sol	1822954ab2aa4f315f0c
poco-dev/contracts/modules/interfaces/IexecMaintenanceExtra.sol	47bdc786183681f4ba0
poco-dev/contracts/modules/interfaces/IexecOrderManagement.sol	bdc694d099bc20ca89c

File Name	SHA
poco-dev/contracts/modules/interfaces/IexecPoco.sol	f82e8e5e5aa70c35345c
poco-dev/contracts/modules/interfaces/IexecRelay.sol	be2ab578ba29627be46
poco-dev/contracts/modules/interfaces/IexecTokenSpender.sol	202b77df4de1fcdacd1a
poco-dev/contracts/registries/IRegistry.sol	ffe3c15f48605d24c5b1
poco-dev/contracts/registries/Registry.sol	a3837bdfa95c5024ad1
poco-dev/contracts/registries/RegistryEntry.sol	b6864be405a056d6ef1
poco-dev/contracts/registries/apps/App.sol	cac8649f11ce8bc2c93b
poco-dev/contracts/registries/apps/AppRegistry.sol	e1d7c5744cbff24c80dc
poco-dev/contracts/registries/datasets/Dataset.sol	83257f5ac85d8da3460
poco-dev/contracts/registries/datasets/DatasetRegistry.sol	bf147967c07446dde52l
poco-dev/contracts/registries/workerpools/Workerpool.sol	16be9246eb5652d24a4
poco-dev/contracts/registries/workerpools/WorkerpoolRegistry.sol	cab0ee262cd9d5b42dc
poco-dev/contracts/tools/Migrations.sol	ab396f2c04aed69f6cdc
poco-dev/contracts/tools/testing/TestClient.sol	0bcf03e777105ce8d52c
poco-dev/contracts/tools/testing/TestReceiver.sol	5404782e56839826c5f

Contracts Description Table

Contract	Type	Bases
L	Function Name	Visibility
IexecInterfaceNative	Interface	IOwnable, IexecAc IexecCategoryMa IexecERC2c IexecEscrowNa IexecMaintena IexecOrderManag IexecPoco, Iexecl IexecTokenSper ENSIntegrati





















Contract	Type	Bases
IexecInterfaceNativeABILegacy	Interface	IOwnable, IexecAc IexecAccessorsABI IexecCategoryMa IexecERC2c IexecEscrowNa IexecMaintena IexecOrderManag IexecPoco, Iexecl IexecTokenSpe ENSIntegrati
IexecInterfaceToken	Interface	IOwnable, IexecAc IexecCategoryMa IexecERC2c IexecEscrowTo IexecMaintena IexecOrderManag IexecPoco, Iexecl IexecTokenSpe ENSIntegrati
IexecInterfaceTokenABILegacy	Interface	IOwnable, IexecAc IexecAccessorsABI IexecCategoryMa IexecERC2c IexecEscrowTo IexecMaintena IexecOrderManag IexecPoco, Iexecl IexecTokenSpe ENSIntegrati
Store	Implementation	ERC1538Sto:
IexecLibCore_v5	Library	
IexecLibOrders_v5	Library	
L	hash	Public !
L	hash	Public !

Contract	Type	Bases
L	hash	Public !
L	hash	Public !
L	hash	Public !
L	hash	Public !
L	hash	Public !
L	hash	Public !
L	hash	Public !
L	toEthSignedMessageHash	Public !
L	toEthTypedStructHash	Public !
L	recover	Public !
DelegateBase	Implementation	Store
L		Internal 🔒
ENSIntegrationDelegate	Implementation	ENSIntegratio ENSReverseRegist DelegateBas
L	setName	External !
IexecAccessorsABILegacyDelegate	Implementation	IexecAccessorsABI DelegateBas
L	viewDealABILegacy_pt1	External !
L	viewDealABILegacy_pt2	External !
L	viewConfigABILegacy	External !
L	viewAccountABILegacy	External !
L	viewTaskABILegacy	External !
L	viewContributionABILegacy	External !
L	viewCategoryABILegacy	External !
IexecAccessorsDelegate	Implementation	IexecAccesso: DelegateBas
























Contract	Type	Bases
L	name	External !
L	symbol	External !
L	decimals	External !
L	totalSupply	External !
L	balanceOf	External !
L	frozenOf	External !
L	allowance	External !
L	viewAccount	External !
L	token	External !
L	viewDeal	External !
L	viewConsumed	External !
L	viewPresigned	External !
L	viewTask	External !
L	viewContribution	External !
L	viewScore	External !
L	resultFor	External !
L	viewCategory	External !
L	countCategory	External !
L	appregistry	External !
L	datasetregistry	External !
L	workerpoolregistry	External !
L	teebroker	External !
L	callbackgas	External !
L	contribution_deadline_ratio	External !
L	reveal_deadline_ratio	External !
L	final_deadline_ratio	External !
L	workerpool_stake_ratio	External !

Contract	Type	Bases
L	kitty_ratio	External !
L	kitty_min	External !
L	kitty_address	External !
L	groupmember_purpose	External !
L	eip712domain_separator	External !
IexecCategoryManagerDelegate	Implementation	IexecCategoryMa DelegateBas
L	createCategory	External !
IexecERC20Common	Implementation	DelegateBas
L	_transfer	Internal 🔒
L	_mint	Internal 🔒
L	_burn	Internal 🔒
L	_approve	Internal 🔒
IexecERC20Delegate	Implementation	IexecERC20 DelegateBas IexecERC20Con
L	transfer	External !
L	approve	External !
L	approveAndCall	External !
L	transferFrom	External !
L	increaseAllowance	External !
L	decreaseAllowance	External !
IexecEscrowNativeDelegate	Implementation	IexecEscrowNa DelegateBas IexecERC20Con
L		External !
L	deposit	External !

Contract	Type	Bases
L	depositFor	External !
L	depositForArray	External !
L	withdraw	External !
L	recover	External !
L	_deposit	Internal 🗝️
L	_withdraw	Internal 🗝️
IexecEscrowTokenDelegate	Implementation	IexecEscrowTo IexecTokenSpe DelegateBas IexecERC2oCon
L		External !
L	deposit	External !
L	depositFor	External !
L	depositForArray	External !
L	withdraw	External !
L	recover	External !
L	receiveApproval	External !
L	_deposit	Internal 🗝️
L	_withdraw	Internal 🗝️
IexecMaintenanceDelegate	Implementation	IexecMaintena DelegateBas
L	configure	External !
L	domain	External !
L	updateDomainSeparator	External !
L	importScore	External !
L	setTeeBroker	External !
L	setCallbackGas	External !

Contract	Type	Bases
L	_chainId	Internal 
L	_domain	Internal 
IexecMaintenanceExtraDelegate	Implementation	IexecMaintenance DelegateBas
L	changeRegistries	External 
IexecOrderManagementDelegate	Implementation	IexecOrderManag DelegateBas
L	manageAppOrder	Public 
L	manageDatasetOrder	Public 
L	manageWorkerpoolOrder	Public 
L	manageRequestOrder	Public 
IexecPocoDelegate	Implementation	IexecPoco, Delega IexecERC20Com SignatureVeri
L	reward	Internal 
L	seize	Internal 
L	lock	Internal 
L	unlock	Internal 
L	lockContribution	Internal 
L	unlockContribution	Internal 
L	rewardForContribution	Internal 
L	seizeContribution	Internal 
L	rewardForScheduling	Internal 
L	successWork	Internal 
L	failedWork	Internal 
L	verifySignature	External 
L	verifyPresignature	External 

Contract	Type	Bases
L	verifyPresignatureOrSignature	External !
L	matchOrders	Public !
L	initialize	Public !
L	contribute	Public !
L	reveal	External !
L	reopen	External !
L	finalize	External !
L	claim	Public !
L	contributeAndFinalize	Public !
L	checkConsensus	Internal 🔒
L	distributeRewards	Internal 🔒
L	executeCallback	Internal 🔒
L	initializeArray	External !
L	claimArray	External !
L	initializeAndClaimArray	External !
IexecRelayDelegate	Implementation	IexecRelay, Delegate
L	broadcastAppOrder	External !
L	broadcastDatasetOrder	External !
L	broadcastWorkerpoolOrder	External !
L	broadcastRequestOrder	External !
SignatureVerifier	Implementation	DelegateBase
L	_isContract	Internal 🔒
L	_addrToKey	Internal 🔒
L	_checkIdentity	Internal 🔒
L	_checkSignature	Internal 🔒
L	_checkPresignature	Internal 🔒

Contract	Type	Bases
L	_checkPresignatureOrSignature	Internal 
ENSIntegration	Interface	
L	setName	External 
IOwnable	Interface	
L	owner	External 
L	renounceOwnership	External 
L	transferOwnership	External 
IexecAccessors	Interface	IOracle
L	name	External 
L	symbol	External 
L	decimals	External 
L	totalSupply	External 
L	balanceOf	External 
L	frozenOf	External 
L	allowance	External 
L	viewAccount	External 
L	token	External 
L	viewDeal	External 
L	viewConsumed	External 
L	viewPresigned	External 
L	viewTask	External 
L	viewContribution	External 
L	viewScore	External 
L	viewCategory	External 
L	countCategory	External 
L	appregistry	External 

Contract	Type	Bases
L	datasetregistry	External !
L	workerpoolregistry	External !
L	teebroker	External !
L	callbackgas	External !
L	contribution_deadline_ratio	External !
L	reveal_deadline_ratio	External !
L	final_deadline_ratio	External !
L	workerpool_stake_ratio	External !
L	kitty_ratio	External !
L	kitty_min	External !
L	kitty_address	External !
L	groupmember_purpose	External !
L	eip712domain_separator	External !
IexecAccessorsABILegacy	Interface	
L	viewAccountABILegacy	External !
L	viewDealABILegacy_pt1	External !
L	viewDealABILegacy_pt2	External !
L	viewTaskABILegacy	External !
L	viewContributionABILegacy	External !
L	viewCategoryABILegacy	External !
L	viewConfigABILegacy	External !
IexecCategoryManager	Interface	
L	createCategory	External !
IexecERC20	Interface	
L	transfer	External !
L	approve	External !

Contract	Type	Bases
L	transferFrom	External !
L	increaseAllowance	External !
L	decreaseAllowance	External !
L	approveAndCall	External !
IexecEscrowNative	Interface	
L		External !
L	deposit	External !
L	depositFor	External !
L	depositForArray	External !
L	withdraw	External !
L	recover	External !
IexecEscrowToken	Interface	
L		External !
L	deposit	External !
L	depositFor	External !
L	depositForArray	External !
L	withdraw	External !
L	recover	External !
IexecMaintenance	Interface	
L	configure	External !
L	domain	External !
L	updateDomainSeparator	External !
L	importScore	External !
L	setTeeBroker	External !
L	setCallbackGas	External !



Contract	Type	Bases
IexecMaintenanceExtra	Interface	
L	changeRegistries	External !
IexecOrderManagement	Interface	
L	manageAppOrder	External !
L	manageDatasetOrder	External !
L	manageWorkerpoolOrder	External !
L	manageRequestOrder	External !
IexecPoco	Interface	
L	verifySignature	External !
L	verifyPresignature	External !
L	verifyPresignatureOrSignature	External !
L	matchOrders	External !
L	initialize	External !
L	contribute	External !
L	reveal	External !
L	reopen	External !
L	finalize	External !
L	claim	External !
L	contributeAndFinalize	External !
L	initializeArray	External !
L	claimArray	External !
L	initializeAndClaimArray	External !
IexecRelay	Interface	
L	broadcastAppOrder	External !
L	broadcastDatasetOrder	External !
L	broadcastWorkerpoolOrder	External !

Contract	Type	Bases
L	broadcastRequestOrder	External !
IexecTokenSpender	Interface	
L	receiveApproval	External !
IRegistry	Implementation	IERC721Enume
L	isRegistered	External !
Registry	Implementation	IRegistry, ERC72 ENSReverseRegist Ownable
L		Public !
L	initialize	External !
L	_mintCreate	Internal 🔒
L	_mintPredict	Internal 🔒
L	isRegistered	External !
L	setName	External !
L	setTokenURI	External !
RegistryEntry	Implementation	ENSReverseRegis
L	_initialize	Internal 🔒
L	owner	Public !
L	setName	External !
App	Implementation	RegistryEntri
L	initialize	Public !
AppRegistry	Implementation	Registry
L		Public !
L	encodeInitializer	Internal 🔒
L	createApp	External !

Contract	Type	Bases
L	predictApp	External !
Dataset	Implementation	RegistryEntry
L	initialize	Public !
DatasetRegistry	Implementation	Registry
L		Public !
L	encodeInitializer	Internal 🔒
L	createDataset	External !
L	predictDataset	External !
Workerpool	Implementation	RegistryEntry
L	initialize	Public !
L	changePolicy	External !
WorkerpoolRegistry	Implementation	Registry
L		Public !
L	encodeInitializer	Internal 🔒
L	createWorkerpool	External !
L	predictWorkerpool	External !
Migrations	Implementation	Ownable
L		Public !
L	setCompleted	Public !
L	upgrade	Public !
TestClient	Implementation	IOracleConsumer
L		Public !
L	receiveResult	External !
TestReceiver	Implementation	IexecTokenSpec

Contract	Type	Bases
L		Public !
L	receiveApproval	External !

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

A.3.4 Tests Suite

Below is the output generated by running the test suite per repository.

Tests For `iexec-solidity` Repository

```

Compiling your contracts...
=====
> Everything is up to date, there is nothing to compile.

# web3 version: 1.2.1
Chainid is: 1585608428903
Chaintype is: private

Contract: ERC1538
  ✓ Ownership (101ms)
  ✓ ERC1538Query - totalFunctions
  ✓ ERC1538Query - functionByIndex (362ms)
  ✓ ERC1538Query - functionById (367ms)
  ✓ ERC1538Query - functionExists (290ms)
  ✓ ERC1538Query - functionSignatures (293ms)
  ✓ ERC1538Query - delegateFunctionSignatures (506ms)
  ✓ ERC1538Query - delegateAddress (292ms)
  ✓ ERC1538Query - delegateAddresses (77ms)
  ✓ ERC1538 - receive (111ms)
  ✓ ERC1538 - fallback (91ms)
  ✓ ERC1538 - no update (45ms)
  ✓ ERC1538 - remove fallback (73ms)

Contract: ERC1538
  ✓ Ownership (86ms)
  ✓ ERC1538Query - totalFunctions
  ✓ ERC1538Query - functionByIndex (336ms)
  ✓ ERC1538Query - functionById (331ms)

```

- ✓ ERC1538Query - functionExists (347ms)
- ✓ ERC1538Query - functionSignatures (327ms)
- ✓ ERC1538Query - delegateFunctionSignatures (487ms)
- ✓ ERC1538Query - delegateAddress (277ms)
- ✓ ERC1538Query - delegateAddresses (69ms)
- ✓ ERC1538 - receive (114ms)
- ✓ ERC1538 - fallback (102ms)
- ✓ ERC1538 - no update (47ms)
- ✓ ERC1538 - remove fallback (62ms)

Contract: GenericFactory

createContract

- ✓ select random salt
- ✓ predict address
- ✓ success (first) (63ms)
- ✓ failure (duplicate) (61ms)
- ✓ post check (88ms)

createContractAndCall

- ✓ select random salt and value
- ✓ predict address
- ✓ success (first) (70ms)
- ✓ failure (duplicate) (64ms)
- ✓ post check (81ms)

36 passing (8s)

Tests For `poco-dev` Repository

Compiling your contracts...

=====

> Everything is up to date, there is nothing to compile.

web3 version: 1.2.1

Chainid is: 1585608428903

Chaintype is: private

Contract: ERC1538

- ✓ Ownership (101ms)
- ✓ ERC1538Query - totalFunctions
- ✓ ERC1538Query - functionByIndex (362ms)
- ✓ ERC1538Query - functionById (367ms)
- ✓ ERC1538Query - functionExists (290ms)
- ✓ ERC1538Query - functionSignatures (293ms)
- ✓ ERC1538Query - delegateFunctionSignatures (506ms)
- ✓ ERC1538Query - delegateAddress (292ms)
- ✓ ERC1538Query - delegateAddresses (77ms)
- ✓ ERC1538 - receive (111ms)
- ✓ ERC1538 - fallback (91ms)

- ✓ ERC1538 - no update (45ms)
- ✓ ERC1538 - remove fallback (73ms)

Contract: ERC1538

- ✓ Ownership (86ms)
- ✓ ERC1538Query - totalFunctions
- ✓ ERC1538Query - functionByIndex (336ms)
- ✓ ERC1538Query - functionById (331ms)
- ✓ ERC1538Query - functionExists (347ms)
- ✓ ERC1538Query - functionSignatures (327ms)
- ✓ ERC1538Query - delegateFunctionSignatures (487ms)
- ✓ ERC1538Query - delegateAddress (277ms)
- ✓ ERC1538Query - delegateAddresses (69ms)
- ✓ ERC1538 - receive (114ms)
- ✓ ERC1538 - fallback (102ms)
- ✓ ERC1538 - no update (47ms)
- ✓ ERC1538 - remove fallback (62ms)

Contract: GenericFactory

createContract

- ✓ select random salt
- ✓ predict address
- ✓ success (first) (63ms)
- ✓ failure (duplicate) (61ms)
- ✓ post check (88ms)

createContractAndCall

- ✓ select random salt and value
- ✓ predict address
- ✓ success (first) (70ms)
- ✓ failure (duplicate) (64ms)
- ✓ post check (81ms)

36 passing (8s)

```
iexec-poco-audit-2020-03/code/iexec-solidity on  master [!?] is 📦 v0.1.0-beta.9  
via 🎛️ v8.10.0 took 17s  
> cd ../poco-dev
```

```
iexec-poco-audit-2020-03/code/poco-dev on  master [!?] is 📦 v3.0.35 via 🎛️ v8.10.0  
> truffle etst  
You can improve web3's performance when running Node.js versions older than 10.5.0 by  
installing the (deprecated) scrypt package in your project  
^C
```

```
iexec-poco-audit-2020-03/code/poco-dev on  master [!?] is 📦 v3.0.35 via 🎛️ v8.10.0  
took 2s  
> truffle test  
You can improve web3's performance when running Node.js versions older than 10.5.0 by  
installing the (deprecated) scrypt package in your project  
Using network 'development'.
```

Compiling your contracts...

=====

```
> Compiling ./contracts/IexecInterfaceNative.sol
> Compiling ./contracts/IexecInterfaceNativeABILegacy.sol
> Compiling ./contracts/IexecInterfaceToken.sol
> Compiling ./contracts/IexecInterfaceTokenABILegacy.sol
> Compiling ./contracts/Store.sol
> Compiling ./contracts/libs/IexecLibCore_v5.sol
> Compiling ./contracts/libs/IexecLibOrders_v5.sol
> Compiling ./contracts/modules/DelegateBase.sol
> Compiling ./contracts/modules/delegates/ENSIntegrationDelegate.sol
> Compiling ./contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol
> Compiling ./contracts/modules/delegates/IexecAccessorsDelegate.sol
> Compiling ./contracts/modules/delegates/IexecCategoryManagerDelegate.sol
> Compiling ./contracts/modules/delegates/IexecERC20Common.sol
> Compiling ./contracts/modules/delegates/IexecERC20Delegate.sol
> Compiling ./contracts/modules/delegates/IexecEscrowNativeDelegate.sol
> Compiling ./contracts/modules/delegates/IexecEscrowTokenDelegate.sol
> Compiling ./contracts/modules/delegates/IexecMaintenanceDelegate.sol
> Compiling ./contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol
> Compiling ./contracts/modules/delegates/IexecOrderManagementDelegate.sol
> Compiling ./contracts/modules/delegates/IexecPocoDelegate.sol
> Compiling ./contracts/modules/delegates/IexecRelayDelegate.sol
> Compiling ./contracts/modules/delegates/SignatureVerifier.sol
> Compiling ./contracts/modules/interfaces/ENSIntegration.sol
> Compiling ./contracts/modules/interfaces/IOwnable.sol
> Compiling ./contracts/modules/interfaces/IexecAccessors.sol
> Compiling ./contracts/modules/interfaces/IexecAccessorsABILegacy.sol
> Compiling ./contracts/modules/interfaces/IexecCategoryManager.sol
> Compiling ./contracts/modules/interfaces/IexecERC20.sol
> Compiling ./contracts/modules/interfaces/IexecEscrowNative.sol
> Compiling ./contracts/modules/interfaces/IexecEscrowToken.sol
> Compiling ./contracts/modules/interfaces/IexecMaintenance.sol
> Compiling ./contracts/modules/interfaces/IexecMaintenanceExtra.sol
> Compiling ./contracts/modules/interfaces/IexecOrderManagement.sol
> Compiling ./contracts/modules/interfaces/IexecPoco.sol
> Compiling ./contracts/modules/interfaces/IexecRelay.sol
> Compiling ./contracts/modules/interfaces/IexecTokenSpender.sol
> Compiling ./contracts/registries/IRegistry.sol
> Compiling ./contracts/registries/Registry.sol
> Compiling ./contracts/registries/RegistryEntry.sol
> Compiling ./contracts/registries/apps/App.sol
> Compiling ./contracts/registries/apps/AppRegistry.sol
> Compiling ./contracts/registries/datasets/Dataset.sol
> Compiling ./contracts/registries/datasets/DatasetRegistry.sol
> Compiling ./contracts/registries/workerpools/Workerpool.sol
> Compiling ./contracts/registries/workerpools/WorkerpoolRegistry.sol
> Compiling ./contracts/tools/Migrations.sol
> Compiling ./contracts/tools/testing/TestClient.sol
> Compiling ./contracts/tools/testing/TestReceiver.sol
```

```

> Compiling @ensdomains/ens/contracts/ENS.sol
> Compiling @iexec/interface/contracts/IexecClerk.sol
> Compiling @iexec/interface/contracts/IexecHub.sol
> Compiling @iexec/interface/contracts/IexecRegistries.sol
> Compiling @iexec/interface/contracts/libs/IexecODBLibCore.sol
> Compiling @iexec/interface/contracts/libs/IexecODBLibOrders.sol
> Compiling @iexec/solidity/contracts/ENSStools/ENSReverseRegistration.sol
> Compiling @iexec/solidity/contracts/ERC1154/IERC1154.sol
> Compiling @iexec/solidity/contracts/ERC1271/IERC1271.sol
> Compiling @iexec/solidity/contracts/ERC1538/ERC1538Store.sol
> Compiling @iexec/solidity/contracts/ERC734/IERC734.sol
> Compiling @iexec/solidity/contracts/Libs/SafeMathExtended.sol
> Compiling @iexec/solidity/contracts/Upgradeability/BaseUpgradeabilityProxy.sol
> Compiling
@iexec/solidity/contracts/Upgradeability/InitializableUpgradeabilityProxy.sol
> Compiling @iexec/solidity/contracts/Upgradeability/Proxy.sol
> Compiling @openzeppelin/contracts/GSN/Context.sol
> Compiling @openzeppelin/contracts/access/Ownable.sol
> Compiling @openzeppelin/contracts/introspection/ERC165.sol
> Compiling @openzeppelin/contracts/introspection/IERC165.sol
> Compiling @openzeppelin/contracts/math/SafeMath.sol
> Compiling @openzeppelin/contracts/token/ERC20/IERC20.sol
> Compiling @openzeppelin/contracts/token/ERC721/ERC721.sol
> Compiling @openzeppelin/contracts/token/ERC721/ERC721Enumerable.sol
> Compiling @openzeppelin/contracts/token/ERC721/ERC721Full.sol
> Compiling @openzeppelin/contracts/token/ERC721/ERC721Metadata.sol
> Compiling @openzeppelin/contracts/token/ERC721/IERC721.sol
> Compiling @openzeppelin/contracts/token/ERC721/IERC721Enumerable.sol
> Compiling @openzeppelin/contracts/token/ERC721/IERC721Metadata.sol
> Compiling @openzeppelin/contracts/token/ERC721/IERC721Receiver.sol
> Compiling @openzeppelin/contracts/utils/Address.sol
> Compiling @openzeppelin/contracts/utils/Counters.sol
> Compiling @openzeppelin/contracts/utils/Create2.sol
> Compiling solstruct/contracts/libs/LibMap2.bytes4.address.bytes.sol
> Compiling solstruct/contracts/libs/LibSet.bytes4.sol
> Compilation warnings encountered:

```

```

    @ensdomains/ens/contracts/ENS.sol:31:31: Warning: This declaration shadows an
existing declaration.

```

```

    function isApprovedForAll(address owner, address operator) external view returns
(bool);

```

```

          ^-----^

```

```

@ensdomains/ens/contracts/ENS.sol:27:5: The shadowed declaration is here:

```

```

    function owner(bytes32 node) external view returns (address);

```

```

    ^-----^

```

```

,@iexec/solidity/contracts/Libs/SafeMathExtended.sol:12:2: Warning: Variable is
shadowed in inline assembly by an instruction of the same name

```

```

    function add(uint256 a, uint256 b) internal pure returns (uint256)

```

```

    ^ (Relevant source part starts here and spans across multiple lines).

```

```

,@iexec/solidity/contracts/Libs/SafeMathExtended.sol:49:2: Warning: Variable is
shadowed in inline assembly by an instruction of the same name

```

```

    function div(uint256 a, uint256 b) internal pure returns (uint256)

```

```

^ (Relevant source part starts here and spans across multiple lines).
,@iexec/solidity/contracts/Libs/SafeMathExtended.sol:62:2: Warning: Variable is
shadowed in inline assembly by an instruction of the same name
    function mod(uint256 a, uint256 b) internal pure returns (uint256)
^ (Relevant source part starts here and spans across multiple lines).
,@iexec/solidity/contracts/Libs/SafeMathExtended.sol:32:2: Warning: Variable is
shadowed in inline assembly by an instruction of the same name
    function mul(uint256 a, uint256 b) internal pure returns (uint256)
^ (Relevant source part starts here and spans across multiple lines).
,@iexec/solidity/contracts/Libs/SafeMathExtended.sol:22:2: Warning: Variable is
shadowed in inline assembly by an instruction of the same name
    function sub(uint256 a, uint256 b) internal pure returns (uint256)
^ (Relevant source part starts here and spans across multiple lines).
,@openzeppelin/contracts/utils/Address.sol:55:28: Warning: Using ".value(...)" is
deprecated. Use "{value: ...}" instead.
    (bool success, ) = recipient.call.value(amount)("");
        ^-----^
, /Users/gnsps/iexec-poco-audit-2020-03/code/poco-
dev/contracts/modules/delegates/IexecEscrowNativeDelegate.sol:77:22: Warning: Using
"value(...)" is deprecated. Use "{value: ...}" instead.
    (bool success, ) = to.call.value(value>(');
        ^-----^
, /Users/gnsps/iexec-poco-audit-2020-03/code/poco-
dev/contracts/modules/delegates/IexecPocoDelegate.sol:773:8: Warning: Using
".gas(...)" is deprecated. Use "{gas: ...}" instead.
    try IOracleConsumer(target).receiveResult.gas(m_callbackgas)
(_taskid, _results)
        ^-----^

> Artifacts written to /var/folders/4_/wjzjgx7x6z94bcp_1ftykp080000gn/T/test-2020230-
92625-pbhk3v.o0xp
> Compiled successfully using:
  - solc: 0.6.4+commit.1dca32f3.Emscripten.clang

# web3 version: 1.2.1
Chainid is: 1585608428903
Chaintype is: private
Checking factory availability
→ Factory is not yet deployed on private (1585608428903)
→ Factory deployed at address: 0xfAC000a12dA42B871c0AaD5F25391aAe62958Db1
# web3 version: 1.2.1
Chainid is: 1585608428903
Chaintype is: private
[factoryDeployer] IexecLibOrders_v5
[factory] Preparing to deploy IexecLibOrders_v5 ...
[factory] IexecLibOrders_v5 successfully deployed at
0x0B16A066Cf937093AB351F88C3d405a8DB80F294
[factoryDeployer] ERC1538UpdateDelegate
[factory] Preparing to deploy ERC1538UpdateDelegate ...
[factory] ERC1538UpdateDelegate successfully deployed at
0x628c08D4d3ef38e113d49953A1B2C055692d682b
[factoryDeployer] ERC1538Proxy

```

```
[factory] Preparing to deploy ERC1538Proxy ...
[factory] ERC1538Proxy successfully deployed at
0x0B2A28f6AfC16016cc31279071ccCfB9a47693a4
IexecInstance deployed at address: 0x0B2A28f6AfC16016cc31279071ccCfB9a47693a4
Linking smart contracts to proxy
[0] ERC1538 link: ERC1538QueryDelegate
[factoryDeployer] ERC1538QueryDelegate
[factory] Preparing to deploy ERC1538QueryDelegate ...
[factory] ERC1538QueryDelegate successfully deployed at
0x9F383d022EA370162e26a001f2AbF853399e6565
[1] ERC1538 link: IexecAccessorsDelegate
[factoryDeployer] IexecAccessorsDelegate
[factory] Preparing to deploy IexecAccessorsDelegate ...
[factory] IexecAccessorsDelegate successfully deployed at
0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5
[2] ERC1538 link: IexecAccessorsABILegacyDelegate
[factoryDeployer] IexecAccessorsABILegacyDelegate
[factory] Preparing to deploy IexecAccessorsABILegacyDelegate ...
[factory] IexecAccessorsABILegacyDelegate successfully deployed at
0x01DbeAb239851895618b503B3d46fFEcB9298137
[3] ERC1538 link: IexecCategoryManagerDelegate
[factoryDeployer] IexecCategoryManagerDelegate
[factory] Preparing to deploy IexecCategoryManagerDelegate ...
[factory] IexecCategoryManagerDelegate successfully deployed at
0x712d4904b6E6943b1A3050607B1042679C62736A
[4] ERC1538 link: IexecERC20Delegate
[factoryDeployer] IexecERC20Delegate
[factory] Preparing to deploy IexecERC20Delegate ...
[factory] IexecERC20Delegate successfully deployed at
0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774
[5] ERC1538 link: IexecEscrowNativeDelegate
[factoryDeployer] IexecEscrowNativeDelegate
[factory] Preparing to deploy IexecEscrowNativeDelegate ...
[factory] IexecEscrowNativeDelegate successfully deployed at
0xB1850a6d4c36FE10F2A0467DA7358666db94b865
[6] ERC1538 link: IexecMaintenanceDelegate
[factoryDeployer] IexecMaintenanceDelegate
[factory] Preparing to deploy IexecMaintenanceDelegate ...
[factory] IexecMaintenanceDelegate successfully deployed at
0xbb87aB66F32129444970565C90B30E45E1bA2240
[7] ERC1538 link: IexecOrderManagementDelegate
[factoryDeployer] IexecOrderManagementDelegate
[factory] Preparing to deploy IexecOrderManagementDelegate ...
[factory] IexecOrderManagementDelegate successfully deployed at
0x91314edb4aCdA897978DA9FD4Ed26cE1f2356B43
[8] ERC1538 link: IexecPocoDelegate
[factoryDeployer] IexecPocoDelegate
[factory] Preparing to deploy IexecPocoDelegate ...
[factory] IexecPocoDelegate successfully deployed at
0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
[9] ERC1538 link: IexecRelayDelegate
[factoryDeployer] IexecRelayDelegate
```

```
[factory] Preparing to deploy IexecRelayDelegate ...
[factory] IexecRelayDelegate successfully deployed at
0x54a4823Eb855ECD96d90f19411C31a1af1163561
[10] ERC1538 link: ENSIntegrationDelegate
[factoryDeployer] ENSIntegrationDelegate
[factory] Preparing to deploy ENSIntegrationDelegate ...
[factory] ENSIntegrationDelegate successfully deployed at
0x7df84dc31810188707069bC42f1b217804Dd2f56
[11] ERC1538 link: IexecMaintenanceExtraDelegate
[factoryDeployer] IexecMaintenanceExtraDelegate
[factory] Preparing to deploy IexecMaintenanceExtraDelegate ...
[factory] IexecMaintenanceExtraDelegate successfully deployed at
0xe2827536292acCb5AcC793920254771211887401
[factoryDeployer] AppRegistry
[factory] Preparing to deploy AppRegistry ...
[factory] AppRegistry successfully deployed at
0x9eBe2123c362FAF7797469769b70F4A8332896CF
[factoryDeployer] DatasetRegistry
[factory] Preparing to deploy DatasetRegistry ...
[factory] DatasetRegistry successfully deployed at
0x2aCb7F08b4002d9D2179A30b2c576146A6c4c47B
[factoryDeployer] WorkerpoolRegistry
[factory] Preparing to deploy WorkerpoolRegistry ...
[factory] WorkerpoolRegistry successfully deployed at
0x3a28BC1009e937d40bBd13220C77Ad42360e6430
AppRegistry      deployed at address: 0x9eBe2123c362FAF7797469769b70F4A8332896CF
DatasetRegistry  deployed at address: 0x2aCb7F08b4002d9D2179A30b2c576146A6c4c47B
WorkerpoolRegistry deployed at address: 0x3a28BC1009e937d40bBd13220C77Ad42360e6430
create category: XS
create category: S
create category: M
create category: L
create category: XL
countCategory is now: 5
category 0 : XS {} 300
category 1 : S {} 1200
category 2 : M {} 3600
category 3 : L {} 10800
category 4 : XL {} 36000
ENSRegistry deployed at address: 0xdc3597552448C3BBf2FB8d7c22D1cFCd4633fCc8
PublicResolver deployed at address: 0x13E7aD6e1750b849F252B51E2fc1255A47eA6A1b
The deployed ERC1538Proxy supports 95 functions:
[0] 0x628c08D4d3ef38e113d49953A1B2C055692d682b updateContract(address,string,string)
[1] 0x9F383d022EA370162e26a001f2AbF853399e6565 isOwner()
[2] 0xe2827536292acCb5AcC793920254771211887401 owner()
[3] 0xe2827536292acCb5AcC793920254771211887401 renounceOwnership()
[4] 0xe2827536292acCb5AcC793920254771211887401 transferOwnership(address)
[5] 0x9F383d022EA370162e26a001f2AbF853399e6565 totalFunctions()
[6] 0x9F383d022EA370162e26a001f2AbF853399e6565 functionByIndex(uint256)
[7] 0x9F383d022EA370162e26a001f2AbF853399e6565 functionById(bytes4)
[8] 0x9F383d022EA370162e26a001f2AbF853399e6565 functionExists(string)
[9] 0x9F383d022EA370162e26a001f2AbF853399e6565 delegateAddress(string)
```


[10] 0x9F383d022EA370162e26a001f2AbF853399e6565 functionSignatures()
[11] 0x9F383d022EA370162e26a001f2AbF853399e6565 delegateFunctionSignatures(address)
[12] 0x9F383d022EA370162e26a001f2AbF853399e6565 delegateAddresses()
[13] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 name()
[14] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 symbol()
[15] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 decimals()
[16] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 totalSupply()
[17] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 balanceOf(address)
[18] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 frozenOf(address)
[19] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 allowance(address, address)
[20] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewAccount(address)
[21] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 token()
[22] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewDeal(bytes32)
[23] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewConsumed(bytes32)
[24] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewPresigned(bytes32)
[25] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewTask(bytes32)
[26] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewContribution(bytes32, address)
[27] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewScore(address)
[28] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 resultFor(bytes32)
[29] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 viewCategory(uint256)
[30] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 countCategory()
[31] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 appregistry()
[32] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 datasetregistry()
[33] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 workerpoolregistry()
[34] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 teebroker()
[35] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 callbackgas()
[36] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 contribution_deadline_ratio()
[37] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 reveal_deadline_ratio()
[38] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 final_deadline_ratio()
[39] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 workerpool_stake_ratio()
[40] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 kitty_ratio()
[41] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 kitty_min()
[42] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 kitty_address()
[43] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 groupmember_purpose()
[44] 0x2Df67Ff64bCBa590bBb26A3D07f1D6b0D26e0bB5 eip712domain_separator()
[45] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewDealABILegacy_pt1(bytes32)
[46] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewDealABILegacy_pt2(bytes32)
[47] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewConfigABILegacy(bytes32)
[48] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewAccountABILegacy(address)
[49] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewTaskABILegacy(bytes32)
[50] 0x01DbeAb239851895618b503B3d46fFEcB9298137
viewContributionABILegacy(bytes32, address)
[51] 0x01DbeAb239851895618b503B3d46fFEcB9298137 viewCategoryABILegacy(uint256)
[52] 0x712d4904b6E6943b1A3050607B1042679C62736A createCategory(string, string, uint256)
[53] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 transfer(address, uint256)
[54] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 approve(address, uint256)
[55] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 approveAndCall(address, uint256, bytes)
[56] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 transferFrom(address, address, uint256)
[57] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 increaseAllowance(address, uint256)
[58] 0xBf8808eFb32dED4D9F3dcedEE21DFe776088c774 decreaseAllowance(address, uint256)
[59] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 deposit()
[60] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 depositFor(address)

[61] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 depositForArray(uint256[],address[])
[62] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 withdraw(uint256)
[63] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 recover()
[64] 0xB1850a6d4c36FE10F2A0467DA7358666db94b865 receive
[65] 0xbb87aB66F32129444970565C90B30E45E1bA2240
configure(address,string,string,uint8,address,address,address,address)
[66] 0xbb87aB66F32129444970565C90B30E45E1bA2240 domain()
[67] 0xbb87aB66F32129444970565C90B30E45E1bA2240 updateDomainSeparator()
[68] 0xbb87aB66F32129444970565C90B30E45E1bA2240 importScore(address)
[69] 0xbb87aB66F32129444970565C90B30E45E1bA2240 setTeeBroker(address)
[70] 0xbb87aB66F32129444970565C90B30E45E1bA2240 setCallbackGas(uint256)
[71] 0x91314edb4aCdA897978DA9FD4Ed26cE1f2356B43
manageAppOrder(((address,uint256,uint256,bytes32,address,address,address,bytes32,bytes),

[72] 0x91314edb4aCdA897978DA9FD4Ed26cE1f2356B43
manageDatasetOrder(((address,uint256,uint256,bytes32,address,address,address,bytes32,byt

[73] 0x91314edb4aCdA897978DA9FD4Ed26cE1f2356B43
manageWorkerpoolOrder(((address,uint256,uint256,bytes32,uint256,uint256,address,address,

[74] 0x91314edb4aCdA897978DA9FD4Ed26cE1f2356B43
manageRequestOrder(((address,uint256,address,uint256,address,uint256,address,uint256,byt

[75] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
verifySignature(address,bytes32,bytes)
[76] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 verifyPresignature(address,bytes32)
[77] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
verifyPresignatureOrSignature(address,bytes32,bytes)
[78] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
matchOrders((address,uint256,uint256,bytes32,address,address,address,bytes32,bytes),
(address,uint256,uint256,bytes32,address,address,address,bytes32,bytes),
(address,uint256,uint256,bytes32,uint256,uint256,address,address,address,bytes32,bytes),
(address,uint256,address,uint256,address,uint256,address,uint256,bytes32,uint256,uint256

[79] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 initialize(bytes32,uint256)
[80] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
contribute(bytes32,bytes32,bytes32,address,bytes,bytes)
[81] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 reveal(bytes32,bytes32)
[82] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 reopen(bytes32)
[83] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 finalize(bytes32,bytes)
[84] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 claim(bytes32)
[85] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
contributeAndFinalize(bytes32,bytes32,bytes,address,bytes,bytes)
[86] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 initializeArray(bytes32[],uint256[])
[87] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92 claimArray(bytes32[])
[88] 0x76dcfb1Fd45b8bC734E7ee3fdb8283D6b465ad92
initializeAndClaimArray(bytes32[],uint256[])
[89] 0x54a4823Eb855ECD96d90f19411C31a1af1163561
broadcastAppOrder((address,uint256,uint256,bytes32,address,address,address,bytes32,bytes

[90] 0x54a4823Eb855ECD96d90f19411C31a1af1163561
broadcastDatasetOrder((address,uint256,uint256,bytes32,address,address,address,bytes32,b


```
[91] 0x54a4823Eb855ECD96d90f19411C31a1af1163561  
broadcastWorkerpoolOrder((address,uint256,uint256,bytes32,uint256,uint256,address,adres  
  
[92] 0x54a4823Eb855ECD96d90f19411C31a1af1163561  
broadcastRequestOrder((address,uint256,address,uint256,address,uint256,address,uint256,b  
  
[93] 0x7df84dc31810188707069bC42f1b217804Dd2f56 setName(address,string)  
[94] 0xe2827536292acCb5AcC793920254771211887401  
changeRegistries(address,address,address)
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
1) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
2) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
3) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
4) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
5) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
6) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
7) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
8) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
9) "before all" hook: configure
```

```
Contract: Fullchain  
# web3 version: 1.2.1  
10) "before all" hook: configure
```

```
Contract: Fullchain
# web3 version: 1.2.1
  11) "before all" hook: configure
```

```
Contract: ENSIntegration
# web3 version: 1.2.1
  12) "before all" hook: configure
```

```
Contract: Accessors
# web3 version: 1.2.1
  13) "before all" hook: configure
```

```
Contract: CategoryManager
# web3 version: 1.2.1
  14) "before all" hook: configure
```

```
Contract: ERC20
# web3 version: 1.2.1
  total supply
    ✓ returns the total amount of tokens
  balanceOf
    when the requested account has no tokens
      ✓ returns zero
    when the requested account has some tokens
      ✓ returns the total amount of tokens
  transfer
    when the recipient is not the zero address
      when the sender does not have enough balance
        ✓ reverts (54ms)
      when the sender transfers all balance
        ✓ transfers the requested amount (91ms)
        ✓ emits a transfer event (48ms)
      when the sender transfers zero tokens
        ✓ transfers the requested amount (90ms)
        ✓ emits a transfer event (43ms)
    when the recipient is the zero address
      ✓ reverts (46ms)
  transfer from
    when the token owner is not the zero address
      when the recipient is not the zero address
        when the spender has enough approved balance
          when the token owner has enough balance
            ✓ transfers the requested amount (92ms)
            ✓ decreases the spender allowance (67ms)
            ✓ emits a transfer event (50ms)
            ✓ emits an approval event (73ms)
          when the token owner does not have enough balance
            ✓ reverts (48ms)
        when the spender does not have enough approved balance
          when the token owner has enough balance
            ✓ reverts (51ms)
          when the token owner does not have enough balance
```

- ✓ reverts (40ms)
- when the recipient is the zero address
 - ✓ reverts (42ms)
- when the token owner is the zero address
 - ✓ reverts (47ms)
- approve
 - when the spender is not the zero address
 - when the sender has enough balance
 - ✓ emits an approval event (40ms)
 - when there was no approved amount before
 - ✓ approves the requested amount (67ms)
 - when the spender had an approved amount
 - ✓ approves the requested amount and replaces the previous one (63ms)
 - when the sender does not have enough balance
 - ✓ emits an approval event
 - when there was no approved amount before
 - ✓ approves the requested amount (62ms)
 - when the spender had an approved amount
 - ✓ approves the requested amount and replaces the previous one (82ms)
 - when the spender is the zero address
 - ✓ reverts (45ms)
- decrease allowance
 - when the spender is not the zero address
 - when the sender has enough balance
 - when there was no approved amount before
 - ✓ reverts (51ms)
 - when the spender had an approved amount
 - ✓ emits an approval event
 - ✓ decreases the spender allowance subtracting the requested amount (64ms)
 - ✓ sets the allowance to zero when all allowance is removed (70ms)
 - ✓ reverts when more than the full allowance is removed (42ms)
 - when the sender does not have enough balance
 - when there was no approved amount before
 - ✓ reverts (45ms)
 - when the spender had an approved amount
 - ✓ emits an approval event (40ms)
 - ✓ decreases the spender allowance subtracting the requested amount (62ms)
 - ✓ sets the allowance to zero when all allowance is removed (60ms)
 - ✓ reverts when more than the full allowance is removed (53ms)
 - when the spender is the zero address
 - ✓ reverts (45ms)
 - increase allowance
 - when the spender is not the zero address
 - when the sender has enough balance
 - ✓ emits an approval event (43ms)
 - when there was no approved amount before
 - ✓ approves the requested amount (63ms)
 - when the spender had an approved amount
 - ✓ increases the spender allowance adding the requested amount (92ms)
 - when the sender does not have enough balance
 - ✓ emits an approval event (61ms)
 - when there was no approved amount before

- ✓ approves the requested amount (63ms)
when the spender had an approved amount
- ✓ increases the spender allowance adding the requested amount (61ms)
when the spender is the zero address
- ✓ reverts (52ms)

approveAndCall

- ✓ accepted by spender (47ms)
- ✓ rejected by spender (55ms)

Contract: EscrowNative

web3 version: 1.2.1
15) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
16) "before all" hook: configure

Contract: OrderManagement

web3 version: 1.2.1
17) "before all" hook: configure

Contract: OrderManagement

web3 version: 1.2.1
18) "before all" hook: configure

Contract: OrderManagement

web3 version: 1.2.1
19) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
20) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
21) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
22) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
23) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
24) "before all" hook: configure

Contract: Poco

web3 version: 1.2.1
25) "before all" hook: configure

```
Contract: Poco
# web3 version: 1.2.1
  26) "before all" hook: configure
```

```
Contract: Poco
# web3 version: 1.2.1
  27) "before all" hook: configure
```

```
Contract: Poco
# web3 version: 1.2.1
  28) "before all" hook: configure
```

```
Contract: Poco
# web3 version: 1.2.1
  29) "before all" hook: configure
```

```
Contract: Poco
# web3 version: 1.2.1
  30) "before all" hook: configure
```

```
Contract: Relay
# web3 version: 1.2.1
  31) "before all" hook: configure
```

```
Contract: Registries
# web3 version: 1.2.1
  32) "before all" hook: configure
```

```
Contract: Ressources
# web3 version: 1.2.1
  33) "before all" hook: configure
```

```
Contract: ERC1154: callback
# web3 version: 1.2.1
  34) "before all" hook: configure
```

```
Contract: ERC1154: resultFor
# web3 version: 1.2.1
  35) "before all" hook: configure
```

```
45 passing (1m)
35 failing
```

```
1) Contract: Fullchain
   "before all" hook: configure:
     TypeError: Cannot read property 'slice' of undefined
       at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
       at Accounts.privateKeyToAccount
```

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
  at Context.before (test/000_fullchain-ABILegacy.js:78:21)
  at <anonymous>
  at process._tickCallback (internal/process/next_tick.js:188:7)
```

2) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
```

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
```

at Context.before (test/000_fullchain.js:78:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

3) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
```

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
```

at Context.before (test/001_fullchain-1workers.js:78:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

4) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
```

```
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
```

at Context.before (test/002_fullchain-2workers.js:78:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

5) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

```
    at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/003_fullchain-3workers.js:78:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)
```

6) Contract: Fullchain

```
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/004_fullchain-4workers.js:78:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)
```

7) Contract: Fullchain

```
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/100_fullchain-5workers-1error.js:78:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)
```

8) Contract: Fullchain

```
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/200_fullchain-bot.js:74:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)
```

9) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/201_fullchain-bot-dualPool.js:74:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

10) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/300_fullchain-reopen.js:73:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

11) Contract: Fullchain

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/400_contributeAndCallback.js:78:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

12) Contract: ENSIntegration

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)


```
at new iExecAgent (utils/odb-tools.js:214:23)
at Context.before (test/byContract/ENSIntegration/ENSIntegration.js:64:21)
at <anonymous>
at process._tickCallback (internal/process/next_tick.js:188:7)
```

13) Contract: Accessors

```
"before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
at new iExecAgent (utils/odb-tools.js:214:23)
at Context.before (test/byContract/IexecAccessors/IexecAccessors.js:61:21)
at <anonymous>
at process._tickCallback (internal/process/next_tick.js:188:7)
```

14) Contract: CategoryManager

```
"before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
at new iExecAgent (utils/odb-tools.js:214:23)
at Context.before
(test/byContract/IexecCategoryManager/IexecCategoryManager.js:63:21)
at <anonymous>
at process._tickCallback (internal/process/next_tick.js:188:7)
```

15) Contract: EscrowNative

```
"before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
at Object.fromPrivate
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
at Accounts.privateKeyToAccount
(/Users/gnsps/.npm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
at new iExecAgent (utils/odb-tools.js:214:23)
at Context.before (test/byContract/IexecEscrow/IexecEscrowNative.js:62:21)
at <anonymous>
at process._tickCallback (internal/process/next_tick.js:188:7)
```

16) Contract: POCO

```
"before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
at Object.fromPrivate
```

```
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
  at Context.before (test/byContract/IexecMaintenance/configure.js:59:21)
  at <anonymous>
  at process._tickCallback (internal/process/next_tick.js:188:7)

17) Contract: OrderManagement
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
  at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
  at Context.before (test/byContract/IexecOrderManagement/close.js:59:21)
  at <anonymous>
  at process._tickCallback (internal/process/next_tick.js:188:7)

18) Contract: OrderManagement
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
  at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
  at Context.before (test/byContract/IexecOrderManagement/invalid.js:59:21)
  at <anonymous>
  at process._tickCallback (internal/process/next_tick.js:188:7)

19) Contract: OrderManagement
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
  at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
  at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
  at new iExecAgent (utils/odb-tools.js:214:23)
  at Context.before (test/byContract/IexecOrderManagement/sign.js:59:21)
  at <anonymous>
  at process._tickCallback (internal/process/next_tick.js:188:7)
```

20) Contract: Poco

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/byContract/IexecPoco/00_matchorders.js:63:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

21) Contract: Poco

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/byContract/IexecPoco/01_initialize.js:72:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

22) Contract: Poco

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

at Context.before (test/byContract/IexecPoco/02_contribute-tag.js:72:21)

at <anonymous>

at process._tickCallback (internal/process/next_tick.js:188:7)

23) Contract: Poco

"before all" hook: configure:

TypeError: Cannot read property 'slice' of undefined

at Object.fromPrivate

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)

at Accounts.privateKeyToAccount

(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)

at new iExecAgent (utils/odb-tools.js:214:23)

```
at Context.before (test/byContract/IexecPoco/02_contribute.js:72:21)
at <anonymous>
at process._tickCallback (internal/process/next_tick.js:188:7)

24) Contract: Poco
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/03_reveal.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

25) Contract: Poco
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/04_finalize.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

26) Contract: Poco
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/05_reopen.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

27) Contract: Poco
  "before all" hook: configure:
  TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
```

```
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/06_claim.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

28) Contract: Poco
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/07_array.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

29) Contract: Poco
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/08_kitty.js:72:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

30) Contract: Poco
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecPoco/verify.js:59:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

31) Contract: Relay
    "before all" hook: configure:
```

```
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/IexecRelay/IexecRelay.js:68:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

32) Contract: Registries
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/registries/registries.js:63:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

33) Contract: Ressources
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/byContract/registries/resources.js:66:21)
    at <anonymous>
    at process._tickCallback (internal/process/next_tick.js:188:7)

34) Contract: ERC1154: callback
    "before all" hook: configure:
TypeError: Cannot read property 'slice' of undefined
    at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
    at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
    at new iExecAgent (utils/odb-tools.js:214:23)
    at Context.before (test/ERC1154/callback.js:77:21)
    at <anonymous>
```

```
at process._tickCallback (internal/process/next_tick.js:188:7)

35) Contract: ERC1154: resultFor
  "before all" hook: configure:
    TypeError: Cannot read property 'slice' of undefined
      at Object.fromPrivate
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/lib/lib/account.js:29:1)
      at Accounts.privateKeyToAccount
(/Users/gnsps/.nvm/versions/node/v8.10.0/lib/node_modules/truffle/build/webpack:/node_modules/eth-accounts/src/index.js:129:1)
      at new iExecAgent (utils/odb-tools.js:214:23)
      at Context.before (test/ERC1154/resultFor.js:71:21)
      at <anonymous>
      at process._tickCallback (internal/process/next_tick.js:188:7)
```


Appendix 4 - Disclosure

ConsenSys Diligence (“CD”) typically receives compensation from one or more clients (the “Clients”) for performing the analysis contained in these reports (the “Reports”). The Reports may be distributed through other means, including via ConsenSys publications and other distributions.

The Reports are not an endorsement or indictment of any particular project or team, and the Reports do not guarantee the security of any particular project. This Report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. No Report provides any warranty or representation to any Third-Party in any respect, including regarding the bugfree nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the Reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this Report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project. CD owes no duty to any Third-Party by virtue of publishing these Reports.

PURPOSE OF REPORTS The Reports and the analysis described therein are created solely for Clients and published with their consent. The scope of our review is limited to a review of Solidity code and only the Solidity code we note as being within the scope of our review within this report. The Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond Solidity that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty.

CD makes the Reports available to parties other than the Clients (i.e., “third parties”) – on its website. CD hopes that by making these analyses publicly available, it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.

LINKS TO OTHER WEB SITES FROM THIS WEB SITE You may, through hypertext or other computer links, gain access to web sites operated by persons other than ConsenSys and CD. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites’ owners. You agree that ConsenSys and CD are not responsible for the content or operation of such Web sites, and that ConsenSys and CD 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 ConsenSys and CD 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 Reports. ConsenSys and CD assumes no responsibility for the use of third party software on the Web Site and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

TIMELINESS OF CONTENT The content contained in the Reports is current as of the date appearing on the Report and is subject to change without notice. Unless indicated otherwise, by ConsenSys and CD.

