A CONSENSYS DILIGENCE AUDIT REPORT

iExec PoCo

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

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 check and effects of the iExec platform are done off-chain and not in the scope of this audit.

The allotted time for 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

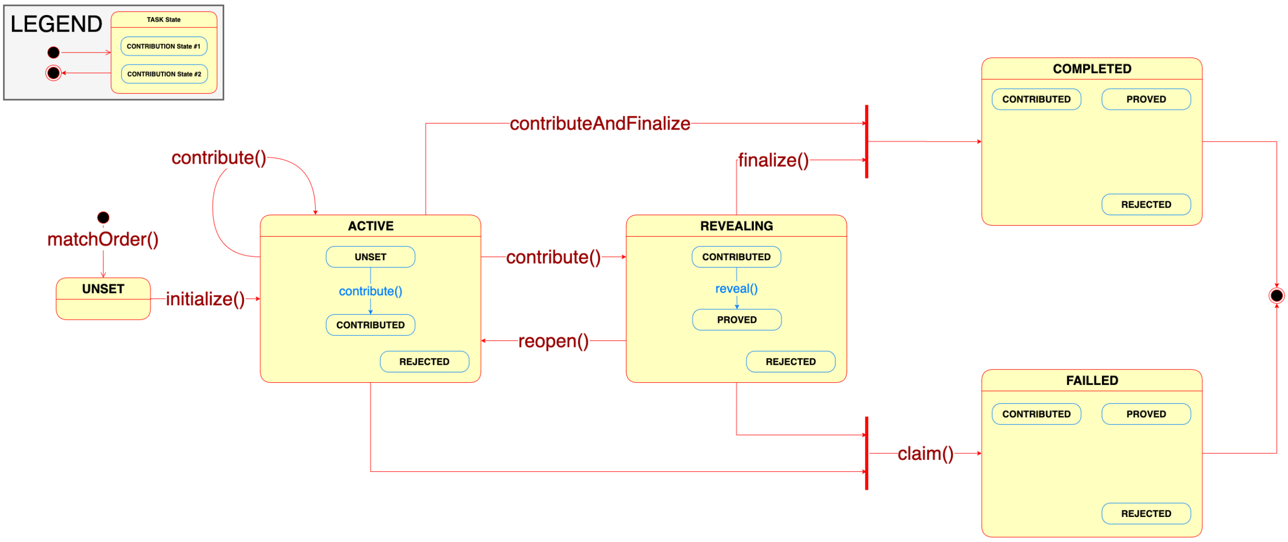
The core part of the PoCo system is the new `PoCoDelegate` smart contract. It replaces what used to be a combination of two smart contracts: the `IexecClerk` and the `IexecHub`.

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 it's 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 Additional Spot Check of Uniswap's Token Swap Delegate

An additional 1-day spot check was performed on the 21st of September of 2020 to validate a small addition to the PoCo codebase encompassed in the following PR: iExecBlockchainComputing/PoCo#45

Aside from helper functions added to existing files (e.g., https://github.com/iExecBlockchainComputing/PoCo/pull/45/files#diff-1e73aff6367b2514e7d2d69b9dc56a91R83-R90), the significant change in the PoCo logic is the addition of the `IexecEscrowTokenSwapDelegate` contract.

The intent of this new delegate contract is to enable atomic Uniswap swaps when depositing ETH to the PoCo system or, more importantly, when matching orders in the PoCo system.

The external functions present in:

https://github.com/iExecBlockchainComputing/PoCo/blob/c9b9bbb39129a0596b3e78b891d7f4be11c892b7/contracts/modules/delegates/IexecEscrowTokenSwapDelegate.sol#L96-L105

Are just wrapper functions over the Uniswap v2 router methods for paths specifically including RLC, iExec's native token, and, therefore, the attack surface they open up is limited.

The most crucial logic addition is in the internal functions handling the token swaps and an extra external function serving as another wrapper to match orders in the PoCo system with ETH while swapping it atomically on Uniswap.

In the internal functions, the Checks-Effects-Interactions pattern is correctly employed. However, given necessity, in the `matchOrdersWithEth` function, the call to the internal `_request` function opens up the possibility of reentrancy by sending back excess ETH to the sender.

The `m_consumed[]` state variable (a mapping) is accessed before the external call inside `_request`, and, therefore, it is not guaranteed that its state can be guaranteed before the call to the `matchOrders` function in `IexecPocoDelegate`.

However, after careful analysis, we can see that `m_consumed[]` is monotonic, which in turn means that the volume of each order will only strictly decrease. Additionally, we can also verify that, in the event the available order volume is not enough, the call will revert.

Tying this together, we conclude that the reliance on the consistent state of `m_consumed[]` before and after the reentrancy is not problematic because it could only result in lost funds for an ill-intended actor and, as a result, there is no incentive to change `m_consumed[]` 's state with the reentrancy.

One small detail that might be worth to mention in user-facing communications from iExec is that the caller of the `matchOrdersWithEth` function in `IexecEscrowTokenSwapDelegate` will always be donating the proceeds of the swap to the order requester and not to himself. However, the audit team is not disagreeing with the way the module is engineered since if the proceeds went to `msg.sender` a class of vulnerabilities would have been surfaced.

5 Recommendations

5.1 Avoid memory manipulation routines in assembly

n though the gas optimizations stemming from direct memory nipulation routines in assembly is commendable (these are mostly present in hashing-related functions in the `IexecLibCore_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/.

5.2 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 a74542102a1c4969eca8fef0f947581f4f834a4c.

5.3 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, uding 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.

5.4 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.

5.5 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 *FAILLED* 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.

5.6 Review the Code Quality recommendations in Appendix 1

Other comments related to readability and best practices are listed in Appendix 1

6 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.

6.1 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()`).

6.2 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.

6.3 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 it’s 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.

7 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.

7.1 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.

7.2 System deployer is fully trusted in this version of the Co 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.

7.3 `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 then 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.
        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.

7.4 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.

7.5 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"`

7.6 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 thee 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 get 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).

7.7 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 3f7f22712821bd5d8cfcf9b279d4af18b0e56bf9. 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-1 Hash
poco-dev/contracts/IexecInterfaceNative.sol	438599f3acea91f811c7f395235c1d8a7deda112
poco-dev/contracts/IexecInterfaceNativeABILegacy.sol	28607ea20a6e91fcc5b925bf12f68ff45b96d999
poco-dev/contracts/IexecInterfaceToken.sol	2ea18304e61a6d88a39823ac7136c72e7e0d6256
poco-dev/contracts/IexecInterfaceTokenABILegacy.sol	e0541ee61d54d9034c53d29c8c93735a7cc4574f
poco-dev/contracts/Store.sol	b5edb04dabdc5983a117d074e7b273e4956fe34f
poco-dev/contracts/libs/IexecLibCore_v5.sol	359c785f15d6ac64197e89a4f8c358c9eba9ff57
poco-dev/contracts/libs/IexecLibOrders_v5.sol	65d30c4d506963649503 4aa62993516ffcd6b006
poco-dev/contracts/modules/DelegateBase.sol	966321486cf7049912cfaf34ea8fcfa36a665b09
poco-dev/contracts/modules/delegates/ENSIntegrationDelegate.sol	509ad5bda5fb7896699fe92fa4f1783f2116453e

File Name	SHA-1 Hash
poco-dev/contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol	257f318160dfd6a848c43bfe2d4db45551398825
poco-dev/contracts/modules/delegates/IexecAccessorsDelegate.sol	8bbc143e3ea0e731c6c5785689d324c3fc7376a8
poco-dev/contracts/modules/delegates/IexecCategoryManagerDelegate.sol	b42cb5c07838d5eb8da1f8088e9a1a6e4dac1fb1
poco-dev/contracts/modules/delegates/IexecERC20Common.sol	54ecb31c576017c96fa7e322102a039453974f73
poco-dev/contracts/modules/delegates/IexecERC20Delegate.sol	6b6e404844c727e57a13991c07d90b1b4ed5d05a
poco-dev/contracts/modules/delegates/IexecEscrowNativeDelegate.sol	d0f96ed32949a8d072695254eb17acdb8a691337
poco-dev/contracts/modules/delegates/IexecEscrowTokenDelegate.sol	1c0177cff23a426fe40c27d65ab2c854e5cf3cfe
poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol	1c1eef2430cc35ce3366a4ac10fcc9139e845e52
poco-dev/contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol	00b3b7ab05f2f79040200a1528a2f1a5249da606
poco-dev/contracts/modules/delegates/IexecOrderManagementDelegate.sol	aa2f3dccf020d9c21f507701279e92e5c4fc6c79

File Name	SHA-1 Hash
poco-dev/contracts/modules/delegates/IexecPocoDelegate.sol	a43fa6b7f4c088adfdfe531aceff8e9c73bcc276
poco-dev/contracts/modules/delegates/IexecRelayDelegate.sol	096d24d4b15593ee1cee7f972bd26cb8deab6179
poco-dev/contracts/modules/delegates/SignatureVerifier.sol	83160d2e5924055aa3206f0578c32fc584131ce4
poco-dev/contracts/modules/interfaces/ENSIntegration.sol	f0ad54cfbc0f3f5dda2048af72f81b3b636eaabb
poco-dev/contracts/modules/interfaces/IOwnable.sol	b33a9ad33d580bb88eed1013e13b69835840ef51
poco-dev/contracts/modules/interfaces/IexecAccessors.sol	c2bff677eb8d606af5698adfd8d247cfb7883565
poco-dev/contracts/modules/interfaces/IexecAccessorsABILegacy.sol	91f97256685b91010441f9bf9e51f0e44585a5d5
poco-dev/contracts/modules/interfaces/IexecCategoryManager.sol	2c0bc1c4f9e3261c4e1cee4b78887b14f65b9e1b
poco-dev/contracts/modules/interfaces/IexecERC20.sol	66841034833adca8c16c3011feaac38cd1c768fc
poco-dev/contracts/modules/interfaces/IexecEscrowNative.sol	d8847e54490a498845664e05b301ee6a59c2e6dd

File Name	SHA-1 Hash
poco-dev/contracts/modules/interfaces/IexecEscrowToken.sol	0ff3340f349dd50126d4a7edeebe3417fe7b033e
poco-dev/contracts/modules/interfaces/IexecMaintenance.sol	1822954ab2aa4f315f00547534657fb5e94e5688
poco-dev/contracts/modules/interfaces/IexecMaintenanceExtra.sol	47bdc786183681f4ba0baf29b3d0fcc009eb30bd
poco-dev/contracts/modules/interfaces/IexecOrderManagement.sol	bdc694d099bc20ca89c1577f7b403ce2b0c06b0d
poco-dev/contracts/modules/interfaces/IexecPoco.sol	f82e8e5e5aa70c35345d7a6a318eaa4c0610c246
poco-dev/contracts/modules/interfaces/IexecRelay.sol	be2ab578ba29627be4643efd27598ebd749e7fae
poco-dev/contracts/modules/interfaces/IexecTokenSpender.sol	202b77df4de1fcdacd1a26d0ec72fd0ad96ae720
poco-dev/contracts/registries/IRegistry.sol	ffe3c15f48605d24c5b1497529e01fffc2066b02
poco-dev/contracts/registries/Registry.sol	a3837bdfa95c5024ad1251e60a27c15d76ddefa1
poco-dev/contracts/registries/RegistryEntry.sol	b6864be405a056d6ef172b4a50b30afc35692622
poco-dev/contracts/registries/apps/App.sol	cac8649f11ce8bc2c93b85e003e429b3bce58c0b

File Name	SHA-1 Hash
poco-dev/contracts/registries/apps/AppRegistry.sol	e1d7c5744cbff24c80dc4b8fd743ed95e1a6e262
poco-dev/contracts/registries/datasets/Dataset.sol	83257f5ac85d8da3460954b2c53fb420b5932390
poco-dev/contracts/registries/datasets/DatasetRegistry.sol	bf147967c07446dde52b7b1c275bafaac0644e37
poco-dev/contracts/registries/workerpools/Workerpool.sol	16be9246eb5652d24a46146b541f063ac90be269
poco-dev/contracts/registries/workerpools/WorkerpoolRegistry.sol	cab0ee262cd9d5b42dce9ee6965e540b6b27d1cf
poco-dev/contracts/tools/Migrations.sol	ab396f2c04aed69f6cdef9a954b8f22da7822d21
poco-dev/contracts/tools/testing/TestClient.sol	0bcf03e777105ce8d52d304a3704064ac5a4d944
poco-dev/contracts/tools/testing/TestReceiver.sol	5404782e56839826c5f9649f42f87be409b082c4

iExecBlockchainComputing/iexec-solidity

File Name	SHA-1 Hash
iexec-solidity/contracts/ENStools/ENSReverseRegistration.sol	20ea50fd7ba8fb5398281b34f3ba2172846e1d49
iexec-solidity/contracts/ERC1154/IERC1154.sol	892b56dee343f68a984bdf29d2b25f9f45953630

File Name	SHA-1 Hash
iexec-solidity/contracts/ERC1271/IERC1271.sol	4944fcc92d2ba5abf07a4aa381f1414859b97fd4
iexec-solidity/contracts/ERC1538/ERC1538.sol	c2ff06da81513e4f0a9143ec4dc03fa0e56d402b
iexec-solidity/contracts/ERC1538/ERC1538Proxy.sol	75e468f9819caace38123ab2934cb936774956f3
iexec-solidity/contracts/ERC1538/ERC1538Query.sol	73f28de88815b08cdeeaea3ad874a8bea677d441
iexec-solidity/contracts/ERC1538/ERC1538Store.sol	6f8bbfd330c5cbb78bc0c74694b3db6b5adce274
iexec-solidity/contracts/ERC1538/ERC1538Update.sol	38a9d71ace70289423c577b8ca8931794484a201
iexec-solidity/contracts/ERC1538/IERC1538.sol	2a30f324d44b77a5dda1619c393e1dcc7c45a585
iexec-solidity/contracts/ERC725/IERC725.sol	14e1265d58b916e925300388fff6c4a1b4854c71
iexec-solidity/contracts/ERC734/IERC734.sol	1648464843385275d20db57ba349d78ae95d09af
iexec-solidity/contracts/Factory/CounterfactualFactory.sol	822d7cfba1ca1f2a66304481f59054296e8223f1
iexec-solidity/contracts/Factory/GenericFactory.sol	45888956954bbb2c1a32b60099eeee72a392b135
iexec-solidity/contracts/Libs/SafeMathExtended.sol	988444bcf40be7af53d1485af2f9b8d6d64e27bf

File Name	SHA-1 Hash
iexec-solidity/contracts/Migrations.sol	d6a9049b9ccf34341831c3d34ea0f8d66dcacea0
iexec-solidity/contracts/TestContract.sol	44e98d4544b0e414281a602975e48f7cc931d85d
iexec-solidity/contracts/Upgradeability/BaseUpgradeabilityProxy.sol	1d7fdce8663c7338ff9ca508be7ef95fcc8a49a1
iexec-solidity/contracts/Upgradeability/InitializableUpgradeabilityProxy.sol	fae44f55f71595c17b7fc6a01da5c7a2e757df3c
iexec-solidity/contracts/Upgradeability/Proxy.sol	a6e3c5967eb838e4a79e763f82d12baaf5db7394

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.

```
/iexec-solidity/contracts/upgradeability/baseupgradeabilityproxy.sol
  1:0   warning  A floating pragma is set  SWC-103
  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                                     SW
   1:0   warning  A floating pragma is set                                SW
  15:11  warning  requirement violation                                   SW
  28:3   warning  Potentially unbounded data structure passed to builtin  SW

/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
  12:1507  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                               S
  27:6    warning  Potentially unbounded data structure passed to builtin  S
  28:6    warning  Potentially unbounded data structure passed to builtin  S
  32:4    warning  The caller can jump to any point in the code            S
  32:151  warning  Potentially unbounded data structure passed to builtin  S
  32:161  warning  Potentially unbounded data structure passed to builtin  S

/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.sc
   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)
```

```
/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-
  10:387  warning  requirement violation                                SWC-
  16:35   warning  requirement violation                                SWC-

/poco-dev@iexec/solidity/contracts/upgradeability/initializableupgradeabilit
  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
  10:9428   error    persistent state read after call
  10:11878  error    persistent state write after call
  10:11878  error    persistent state read after call
  10:14333  warning  Potentially unbounded data structure passed to builtin
  10:15790  warning  Unused function parameter "from"
  10:15804  warning  Unused function parameter "to"
  10:15816  warning  Unused function parameter "tokenId"
  72:12641  warning  Unused function parameter "from"
  72:12655  warning  Unused function parameter "to"
  72:12667  warning  Unused function parameter "tokenId"

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

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

/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
  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  S
  141:24  warning  Potentially unbounded data structure passed to builtin  S
  287:29  warning  Potentially unbounded data structure passed to builtin  S
  355:9   warning  The caller can jump to any point in the code            S

/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/iexecescrowtokendelegate.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.

```
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.
  9:1      error      Only use indent of 4 spaces.
  11:1     error      Only use indent of 4 spaces.
  12:1     error      Only use indent of 4 spaces.
  14:1     error      Only use indent of 4 spaces.
  18:0     error      Only use indent of 4 spaces.
  20:1     error      Only use indent of 4 spaces.
  24:27    warning    There should be no whitespace or comments between the
  24:56    warning    There should be no whitespace or comments between the
  25:27    warning    There should be no whitespace or comments between the
  25:56    warning    There should be no whitespace or comments between the
  43:0     error      Only use indent of 4 spaces.

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.                        indenta
  24:0     error    Only use indent of 4 spaces.                        indenta
  26:1     error    Only use indent of 4 spaces.                        indenta
  31:0     error    Only use indent of 4 spaces.                        indenta
  33:1     error    Only use indent of 4 spaces.                        indenta
  37:0     error    Only use indent of 4 spaces.                        indenta
  39:1     error    Only use indent of 4 spaces.                        indenta
  43:0     error    Only use indent of 4 spaces.                        indenta
  45:1     error    Only use indent of 4 spaces.                        indenta
  49:0     error    Only use indent of 4 spaces.                        indenta
  51:1     error    Only use indent of 4 spaces.                        indenta
  75:0     error    Only use indent of 4 spaces.                        indenta
  77:1     error    Only use indent of 4 spaces.                        indenta
  86:4     error    Variable 'funcId' is declared but never used.     no-unus
  110:0    error    Only use indent of 4 spaces.                        indenta
  112:1    error    Only use indent of 4 spaces.                        indenta
  142:1    error    Only use indent of 4 spaces.                        indenta
  143:0    error    Only use indent of 4 spaces.                        indenta

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-assemb
  30:2    error    Avoid using Inline Assembly.    security/no-inline-assemb
  38:3    error    Avoid using Inline Assembly.    security/no-inline-assemb
  42:4    error    Avoid using Inline Assembly.    security/no-inline-assemb
  46:4    error    Avoid using Inline Assembly.    security/no-inline-assemb
  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-assemb
  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-i
  38:3    error      Avoid using Inline Assembly.             security/no-i
  51:2    warning    Provide an error message for require()
  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-i
  38:3    error      Avoid using Inline Assembly.              security/no-i
  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-reasor
  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-reasor
  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-reasor
  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-reasor
  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-reasor
  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-
  135:0    error      Only use indent of 4 spaces.              indentation
```

```
contracts/Libs/SignatureVerifier.sol
  10:1    error      Only use indent of 4 spaces.                 indentatior
  12:1    error      Only use indent of 4 spaces.                 indentatior
  16:2    error      Avoid using Inline Assembly.                 security/nc
  18:0    error      Only use indent of 4 spaces.                 indentatior
  20:1    error      Only use indent of 4 spaces.                 indentatior
  24:0    error      Only use indent of 4 spaces.                 indentatior
  26:1    error      Only use indent of 4 spaces.                 indentatior
  29:2    warning    Line exceeds the limit of 145 characters     max-len
  30:0    error      Only use indent of 4 spaces.                 indentatior
  32:1    error      Only use indent of 4 spaces.                 indentatior
  43:0    error      Only use indent of 4 spaces.                 indentatior

contracts/TestContract.sol
  12:9    error    Syntax error: unexpected token (

contracts/Upgradeability/BaseUpgradeabilityProxy.sol
  3:7     error    "@openzeppelin/contracts/utils/Address.sol": Import state
  4:7     error    "./Proxy.sol": Import statements must use double quotes c
  17:2    error    Only use indent of 4 spaces.
  24:2    error    Only use indent of 4 spaces.
  30:2    error    Only use indent of 4 spaces.
  32:4    error    Avoid using Inline Assembly.
  35:0    error    Only use indent of 4 spaces.
  41:2    error    Only use indent of 4 spaces.
  44:0    error    Only use indent of 4 spaces.
  50:2    error    Only use indent of 4 spaces.
  55:4    error    Avoid using Inline Assembly.
  58:0    error    Only use indent of 4 spaces.

contracts/Upgradeability/InitializableUpgradeabilityProxy.sol
  3:7      error      "./BaseUpgradeabilityProxy.sol": Import statements mus
  19:2     error      Only use indent of 4 spaces.
  20:4     warning    Provide an error message for require()
  24:6     error      Only use indent of 8 spaces.
  24:31    warning    Avoid using low-level function 'delegatecall'.
  25:6     error      Only use indent of 8 spaces.
  25:6     warning    Provide an error message for require()
  27:0     error      Only use indent of 4 spaces.

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

✕ 141 errors, 17 warnings found.
```

```
contracts/IexecInterfaceNative.sol
```

```
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
  7:1      error      Only use indent of 4 spaces.
  8:1      error      Only use indent of 4 spaces.
  8:1      warning    Line exceeds the limit of 145 characters
  9:1      warning    Line exceeds the limit of 145 characters
  9:1      error      Only use indent of 4 spaces.
  10:1     warning    Line exceeds the limit of 145 characters
  10:1     error      Only use indent of 4 spaces.
  11:1     error      Only use indent of 4 spaces.
  11:1     warning    Line exceeds the limit of 145 characters
  12:1     warning    Line exceeds the limit of 145 characters
  12:1     error      Only use indent of 4 spaces.
  13:1     error      Only use indent of 4 spaces.
  13:1     warning    Line exceeds the limit of 145 characters
```

```
    14:1      warning    Line exceeds the limit of 145 characters
    14:1      error      Only use indent of 4 spaces.
    15:1      error      Only use indent of 4 spaces.
    15:1      warning    Line exceeds the limit of 145 characters
    17:1      error      Only use indent of 4 spaces.
    21:0      error      Only use indent of 4 spaces.
    23:1      error      Only use indent of 4 spaces.
    29:0      error      Only use indent of 4 spaces.
    31:1      error      Only use indent of 4 spaces.
    43:0      error      Only use indent of 4 spaces.
    45:1      error      Only use indent of 4 spaces.
    57:0      error      Only use indent of 4 spaces.
    59:1      error      Only use indent of 4 spaces.
    73:0      error      Only use indent of 4 spaces.
    75:1      error      Only use indent of 4 spaces.
    94:0      error      Only use indent of 4 spaces.
    96:1      error      Only use indent of 4 spaces.
    101:0     error      Only use indent of 4 spaces.
    103:1     error      Only use indent of 4 spaces.
    108:0     error      Only use indent of 4 spaces.
    110:1     error      Only use indent of 4 spaces.
    115:0     error      Only use indent of 4 spaces.
    117:1     error      Only use indent of 4 spaces.
    122:0     error      Only use indent of 4 spaces.
    124:1     error      Only use indent of 4 spaces.
    139:2     warning    Assignment operator must have exactly single space on
    140:2     warning    Assignment operator must have exactly single space on
    142:2     error      Avoid using Inline Assembly.
    158:0     error      Only use indent of 4 spaces.
    160:1     error      Only use indent of 4 spaces.
    180:2     error      Avoid using Inline Assembly.
    190:0     error      Only use indent of 4 spaces.
    192:1     error      Only use indent of 4 spaces.
    212:2     error      Avoid using Inline Assembly.
    222:0     error      Only use indent of 4 spaces.
    224:1     error      Only use indent of 4 spaces.
    246:2     error      Avoid using Inline Assembly.
    256:0     error      Only use indent of 4 spaces.
    258:1     error      Only use indent of 4 spaces.
    288:2     error      Avoid using Inline Assembly.
    301:0     error      Only use indent of 4 spaces.
    303:1     error      Only use indent of 4 spaces.
    311:0     error      Only use indent of 4 spaces.
    313:1     error      Only use indent of 4 spaces.
    321:0     error      Only use indent of 4 spaces.
    323:1     error      Only use indent of 4 spaces.
    331:0     error      Only use indent of 4 spaces.
    333:1     error      Only use indent of 4 spaces.
    341:0     error      Only use indent of 4 spaces.
    343:1     error      Only use indent of 4 spaces.
```

```
  347:0    error      Only use indent of 4 spaces.
  349:1    error      Only use indent of 4 spaces.
  353:0    error      Only use indent of 4 spaces.
  355:1    error      Only use indent of 4 spaces.
  364:3    error      Avoid using Inline Assembly.
  373:3    error      Avoid using Inline Assembly.
  388:0    error      Only use indent of 4 spaces.

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

  contracts/modules/delegates/IexecCategoryManagerDelegate.sol
    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.                         ir
    17:0      error    Only use indent of 4 spaces.                         ir
    19:1      error    Only use indent of 4 spaces.                         ir
    24:0      error    Only use indent of 4 spaces.                         ir
    26:1      error    Only use indent of 4 spaces.                         ir
    30:102    error    String literal must be quoted with double quotes.    qu
    32:0      error    Only use indent of 4 spaces.                         ir
    34:1      error    Only use indent of 4 spaces.                         ir
    40:0      error    Only use indent of 4 spaces.                         ir
    42:1      error    Only use indent of 4 spaces.                         ir
    47:0      error    Only use indent of 4 spaces.                         ir
    50:1      error    Only use indent of 4 spaces.                         ir
    55:0      error    Only use indent of 4 spaces.                         ir

  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.
    11:1     error      Only use indent of 4 spaces.
    13:1     error      Only use indent of 4 spaces.
    27:2     warning    Assignment operator must have exactly single space on
    28:2     warning    Assignment operator must have exactly single space on
    29:2     warning    Assignment operator must have exactly single space on
    30:2     warning    Assignment operator must have exactly single space on
    31:2     warning    Assignment operator must have exactly single space on
    32:2     warning    Assignment operator must have exactly single space on
    34:2     warning    Assignment operator must have exactly single space on
    35:2     warning    Assignment operator must have exactly single space on
    36:0     error      Only use indent of 4 spaces.
    38:1     error      Only use indent of 4 spaces.
    38:1     error      Only use indent of 4 spaces.
    42:0     error      Only use indent of 4 spaces.
    44:1     error      Only use indent of 4 spaces.
    49:0     error      Only use indent of 4 spaces.
    51:1     error      Only use indent of 4 spaces.
    57:0     error      Only use indent of 4 spaces.
    59:1     error      Only use indent of 4 spaces.
    63:0     error      Only use indent of 4 spaces.
    65:1     error      Only use indent of 4 spaces.
    69:0     error      Only use indent of 4 spaces.
    71:1     error      Only use indent of 4 spaces.
    74:2     error      Avoid using Inline Assembly.
    75:0     error      Only use indent of 4 spaces.
    77:1     error      Only use indent of 4 spaces.
    81:4     warning    Name 'name': Only "N: V", "N : V" or "N:V" spacing sty
    81:32    warning    ""iExecODB"" should be immediately followed by a comma
    82:5     warning    Name 'version': Only "N: V", "N : V" or "N:V" spacing
    82:34    warning    ""3.0-alpha"" should be immediately followed by a comm
    83:5     warning    Name 'chainId': Only "N: V", "N : V" or "N:V" spacing
    83:33    warning    "_chainId()" should be immediately followed by a comma
    86:0     error      Only use indent of 4 spaces.

  contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol
    10:1    error      Only use indent of 4 spaces.
    16:2    warning    Assignment operator must have exactly single space on b
    17:2    warning    Assignment operator must have exactly single space on b
    19:0    error      Only use indent of 4 spaces.

  contracts/modules/delegates/IexecOrderManagementDelegate.sol
    10:1    error      Only use indent of 4 spaces.                 indentatior
    11:1    error      Only use indent of 4 spaces.                 indentatior
    12:1    error      Only use indent of 4 spaces.                 indentatior
    13:1    error      Only use indent of 4 spaces.                 indentatior
    14:1    error      Only use indent of 4 spaces.                 indentatior
    15:1    error      Only use indent of 4 spaces.                 indentatior
    16:1    error      Only use indent of 4 spaces.                 indentatior
    17:1    error      Only use indent of 4 spaces.                 indentatior
    18:1    error      Only use indent of 4 spaces.                 indentatior
    23:1    error      Only use indent of 4 spaces.                 indentatior
    27:2    warning    Provide an error message for require()       error-reasc
    27:2    warning    Line exceeds the limit of 145 characters     max-len
    40:0    error      Only use indent of 4 spaces.                 indentatior
    42:1    error      Only use indent of 4 spaces.                 indentatior
    46:2    warning    Line exceeds the limit of 145 characters     max-len
    46:2    warning    Provide an error message for require()       error-reasc
    59:0    error      Only use indent of 4 spaces.                 indentatior
    61:1    error      Only use indent of 4 spaces.                 indentatior
    65:2    warning    Provide an error message for require()       error-reasc
    65:2    warning    Line exceeds the limit of 145 characters     max-len
    78:0    error      Only use indent of 4 spaces.                 indentatior
    80:1    error      Only use indent of 4 spaces.                    indentatio
    84:2    warning    Line exceeds the limit of 145 characters        max-len
    84:2    warning    Provide an error message for require()          error-reaso
    97:0    error      Only use indent of 4 spaces.                    indentatio

  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
    10:1      error      Only use indent of 4 spaces.
    10:155    warning    'BroadcastAppOrder': The last argument must not be su
    11:1      warning    Line exceeds the limit of 145 characters
    11:1      error      Only use indent of 4 spaces.
    11:159    warning    'BroadcastDatasetOrder': The last argument must not b
    12:1      error      Only use indent of 4 spaces.
    12:1      warning    Line exceeds the limit of 145 characters
    13:1      warning    Line exceeds the limit of 145 characters
    13:1      error      Only use indent of 4 spaces.
    13:159    warning    'BroadcastRequestOrder': The last argument must not b

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

  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.
  14:1    error      Only use indent of 4 spaces.
  15:1    error      Only use indent of 4 spaces.
  16:1    error      Only use indent of 4 spaces.
  17:1    error      Only use indent of 4 spaces.
  19:1    error      Only use indent of 4 spaces.
  22:2    warning    Assignment operator must have exactly single space on b
  23:2    warning    Assignment operator must have exactly single space on b
  25:0    error      Only use indent of 4 spaces.
  27:1    error      Only use indent of 4 spaces.
  30:2    warning    Provide an error message for require()
  32:2    warning    Assignment operator must have exactly single space on b
  33:0    error      Only use indent of 4 spaces.
  36:1    error      Only use indent of 4 spaces.
  48:0    error      Only use indent of 4 spaces.
  50:1    error      Only use indent of 4 spaces.
  57:0    error      Only use indent of 4 spaces.
  60:1    error      Only use indent of 4 spaces.
  64:0    error      Only use indent of 4 spaces.
  66:1    error      Only use indent of 4 spaces.
  70:0    error      Only use indent of 4 spaces.
  72:1    error      Only use indent of 4 spaces.
  77:0    error      Only use indent of 4 spaces.

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.
  12:1    error      Only use indent of 4 spaces.
  13:1    error      Only use indent of 4 spaces.
  14:1    error      Only use indent of 4 spaces.
  15:1    error      Only use indent of 4 spaces.
  20:1    error      Only use indent of 4 spaces.
  29:2    warning    Assignment operator must have exactly single space on b
  30:2    warning    Assignment operator must have exactly single space on b
  32:2    warning    Assignment operator must have exactly single space on b
  34:0    error      Only use indent of 4 spaces.

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

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

contracts/registries/datasets/DatasetRegistry.sol
  3:7     error    "../Registry.sol": Import statements must use double quot
  4:7     error    "./Dataset.sol": Import statements must use double quotes
  12:1    error    Only use indent of 4 spaces.
  18:0    error    Only use indent of 4 spaces.
  23:1    error    Only use indent of 4 spaces.
  35:0    error    Only use indent of 4 spaces.
  37:1    error    Only use indent of 4 spaces.
  45:0    error    Only use indent of 4 spaces.
  47:1    error    Only use indent of 4 spaces.
  55:0    error    Only use indent of 4 spaces.

contracts/registries/workerpools/Workerpool.sol
  11:1    error      Only use indent of 4 spaces.
  12:1    error      Only use indent of 4 spaces.
  13:1    error      Only use indent of 4 spaces.
  18:1    error      Only use indent of 4 spaces.
  20:0    error      Only use indent of 4 spaces.
  25:1    error      Only use indent of 4 spaces.
  30:2    warning    Assignment operator must have exactly single space on b
  31:2    warning    Assignment operator must have exactly single space on b
  33:0    error      Only use indent of 4 spaces.
  35:1    error      Only use indent of 4 spaces.
  40:2    warning    Provide an error message for require()
  47:2    warning    Assignment operator must have exactly single space on b
  49:0    error      Only use indent of 4 spaces.

contracts/registries/workerpools/WorkerpoolRegistry.sol
  3:7     error    "../Registry.sol": Import statements must use double quot
  4:7     error    "./Workerpool.sol": Import statements must use double quo
  12:1    error    Only use indent of 4 spaces.
  18:0    error    Only use indent of 4 spaces.
  23:1    error    Only use indent of 4 spaces.
  31:0    error    Only use indent of 4 spaces.
  33:1    error    Only use indent of 4 spaces.
  39:0    error    Only use indent of 4 spaces.
  41:1    error    Only use indent of 4 spaces.
  47:0    error    Only use indent of 4 spaces.

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.
  10:1    error      Only use indent of 4 spaces.
  11:1    error      Only use indent of 4 spaces.
  13:1    error      Only use indent of 4 spaces.
  15:1    warning    Code contains empty block
  16:0    error      Only use indent of 4 spaces.
  18:1    error      Only use indent of 4 spaces.
  21:2    warning    Assignment operator must have exactly single space on b
  23:0    error      Only use indent of 4 spaces.

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.

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

File Name	SHA-1 Hash
iexec-solidity/contracts/ENStools/ENSReverseRegistration.sol	20ea50fd7ba8fb5398281b34f3ba2172846e1d49
iexec-solidity/contracts/ERC1154/IERC1154.sol	892b56dee343f68a984bdf29d2b25f9f45953630
iexec-solidity/contracts/ERC1271/IERC1271.sol	4944fcc92d2ba5abf07a4aa381f1414859b97fd4
iexec-solidity/contracts/ERC1538/ERC1538.sol	c2ff06da81513e4f0a9143ec4dc03fa0e56d402b
iexec-solidity/contracts/ERC1538/ERC1538Proxy.sol	75e468f9819caace38123ab2934cb936774956f3
iexec-solidity/contracts/ERC1538/ERC1538ProxyV2.sol	05a295a9c62eda7d6c106174a36cfc87dc446107
iexec-solidity/contracts/ERC1538/ERC1538Query.sol	73f28de88815b08cdeeaea3ad874a8bea677d441
iexec-solidity/contracts/ERC1538/ERC1538Store.sol	6f8bbfd330c5cbb78bc0c74694b3db6b5adce274
iexec-solidity/contracts/ERC1538/ERC1538Update.sol	38a9d71ace70289423c577b8ca8931794484a201
iexec-solidity/contracts/ERC1538/ERC1538UpdateV2.sol	6830163504f53c40271a7a51e515421d62d2137b
iexec-solidity/contracts/ERC1538/IERC1538.sol	2a30f324d44b77a5dda1619c393e1dcc7c45a585
iexec-solidity/contracts/ERC725/IERC725.sol	14e1265d58b916e925300388fff6c4a1b4854c71

File Name	SHA-1 Hash
iexec-solidity/contracts/ERC734/IERC734.sol	1648464843385275d20db57ba349d78ae95d09af
iexec-solidity/contracts/Factory/CounterfactualFactory.sol	822d7cfba1ca1f2a66304481f59054296e8223f1
iexec-solidity/contracts/Factory/GenericFactory.sol	45888956954bbb2c1a32b60099eeee72a392b135
iexec-solidity/contracts/Libs/ECDSA.sol	3fa8517670e83c2219c5c0ead6416233e6c03c20
iexec-solidity/contracts/Libs/ECDSALib.sol	ea8e62fa6f1f489ecc26f156f603dfb1ffe6ba9d
iexec-solidity/contracts/Libs/SafeMathExtended.sol	988444bcf40be7af53d1485af2f9b8d6d64e27bf
iexec-solidity/contracts/Libs/SignatureVerifier.sol	54f3d4406e3998d6effe31b9366d71460229cdda
iexec-solidity/contracts/Migrations.sol	d6a9049b9ccf34341831c3d34ea0f8d66dcacea0
iexec-solidity/contracts/TestContract.sol	44e98d4544b0e414281a602975e48f7cc931d85d
iexec-solidity/contracts/Upgradeability/BaseUpgradeabilityProxy.sol	1d7fdce8663c7338ff9ca508be7ef95fcc8a49a1
iexec-solidity/contracts/Upgradeability/InitializableUpgradeabilityProxy.sol	fae44f55f71595c17b7fc6a01da5c7a2e757df3c
iexec-solidity/contracts/Upgradeability/Proxy.sol	a6e3c5967eb838e4a79e763f82d12baaf5db7394

Contract	Type	Bases		
└	Function Name	Visibility	Mutability	Modifiers
IReverseRegistrar	Interface			
└	claim	External ❗	🛑	NO❗
└	claimWithResolver	External ❗	🛑	NO❗
└	setName	External ❗	🛑	NO❗
└	node	External ❗		NO❗
ENSReverseRegistration	Implementation			
└	_setName	Internal 🔒	🛑	
IOracleConsumer	Interface			
└	receiveResult	External ❗	🛑	NO❗
IOracle	Interface			
└	resultFor	External ❗		NO❗
IERC1271	Implementation			
└	isValidSignature	Public ❗		NO❗
ERC1538	Implementation	IERC1538, ERC1538Store		
└		Public ❗	🛑	NO❗

Contract	Type	Bases		
└	_setFunc	Internal 🔒	🛑	
ERC1538Proxy	Implementation	ERC1538, Proxy		
└		Public ❗️	🛑	NO❗️
└	_implementation	Internal 🔒		
ERC1538ProxyV2	Implementation	ERC1538, Proxy		
└		Public ❗️	🛑	NO❗️
└	_implementation	Internal 🔒		
ERC1538Query	Interface			
└	totalFunctions	External ❗️		NO❗️
└	functionByIndex	External ❗️		NO❗️
└	functionById	External ❗️		NO❗️
└	functionExists	External ❗️		NO❗️
└	functionSignatures	External ❗️		NO❗️
└	delegateFunctionSignatures	External ❗️		NO❗️
└	delegateAddress	External ❗️		NO❗️

Contract	Type	Bases		
L	delegateAddresses	External ❗		NO❗
ERC1538QueryDelegate	Implementation	ERC1538Query, ERC1538		
L	totalFunctions	External ❗		NO❗
L	functionByIndex	External ❗		NO❗
L	functionById	External ❗		NO❗
L	functionExists	External ❗		NO❗
L	delegateAddress	External ❗		NO❗
L	functionSignatures	External ❗		NO❗
L	delegateFunctionSignatures	External ❗		NO❗
L	delegateAddresses	External ❗		NO❗
ERC1538Store	Implementation	Ownable		
ERC1538Update	Interface			
L	updateContract	External ❗	🛑	NO❗

Contract	Type	Bases		
ERC1538UpdateDelegate	Implementation	ERC1538Update, ERC1538		
└	updateContract	External ❗	🛑	onlyOwner
ERC1538UpdateV2	Interface			
└	updateContract	External ❗	🛑	NO❗
ERC1538UpdateV2Delegate	Implementation	ERC1538UpdateV2, ERC1538		
└	updateContract	External ❗	🛑	onlyOwner
IERC1538	Interface			
IERC725	Interface			
└	getData	External ❗		NO❗
└	setData	External ❗	🛑	NO❗
└	execute	External ❗	🛑	NO❗
IERC734	Implementation			
└	getKey	External ❗		NO❗
└	keyHasPurpose	External ❗		NO❗
└	getKeysByPurpose	External ❗		NO❗
└	addKey	External ❗	🛑	NO❗

Contract	Type	Bases		
└	removeKey	External ❗	🛑	NO❗
└	execute	External ❗	🛑	NO❗
└	approve	External ❗	🛑	NO❗
CounterfactualFactory	Implementation			
└	_create2	Internal 🔒	🛑	
└	_predictAddress	Internal 🔒		
GenericFactory	Implementation	CounterfactualFactory		
└	predictAddress	Public ❗		NO❗
└	createContract	Public ❗	🛑	NO❗
└	predictAddressWithCall	Public ❗		NO❗
└	createContractAndCall	Public ❗	🛑	NO❗
ECDSA	Implementation			
└	recover	Internal 🔒		
└	recover	Internal 🔒		
└	toEthSignedMessageHash	Internal 🔒		
└	toEthTypedStructHash	Internal 🔒		

Contract	Type	Bases		
ECDSALib	Library			
└	recover	Public ❗		NO❗
└	recover	Public ❗		NO❗
└	toEthSignedMessageHash	Public ❗		NO❗
└	toEthTypedStructHash	Public ❗		NO❗
SafeMathExtended	Library			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	max	Internal 🔒		
└	min	Internal 🔒		
└	mulByFraction	Internal 🔒		
└	percentage	Internal 🔒		
└	log	Internal 🔒		
SignatureVerifier	Implementation	ECDSA		
└	_isContract	Internal 🔒		
└	_addrToKey	Internal 🔒		

Contract	Type	Bases		
└	_checkIdentity	Internal 🔒		
└	_checkSignature	Internal 🔒		
Migrations	Implementation			
└		Public ❗	🛑	NO❗
└	setCompleted	Public ❗	🛑	restricted
└	upgrade	Public ❗	🛑	restricted
TestContract	Implementation			
└		External ❗	💵	NO❗
└		External ❗	💵	NO❗
└	set	External ❗	🛑	NO❗
BaseUpgradeabilityProxy	Implementation	Proxy		
└	_implementation	Internal 🔒		
└	_upgradeTo	Internal 🔒	🛑	
└	_setImplementation	Internal 🔒	🛑	
InitializableUpgradeabilityProxy	Implementation	BaseUpgradeabilityProxy		
└	initialize	Public ❗	💵	NO❗

Contract	Type	Bases		
Proxy	Implementation			
└		External ❗	💵	NO❗
└		External ❗	💵	NO❗
└	_implementation	Internal 🔒		
└	_delegate	Internal 🔒	🛑	
└	_willFallback	Internal 🔒	🛑	
└	_fallback	Internal 🔒	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

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

File Name	SHA-1 Hash
poco-dev/contracts/IexecInterfaceNative.sol	438599f3acea91f811c7f395235c1d8a7deda112
poco-dev/contracts/IexecInterfaceNativeABILegacy.sol	28607ea20a6e91fcc5b925bf12f68ff45b96d999
poco-dev/contracts/IexecInterfaceToken.sol	2ea18304e61a6d88a39823ac7136c72e7e0d6256
poco-dev/contracts/IexecInterfaceTokenABILegacy.sol	e0541ee61d54d9034c53d29c8c93735a7cc4574f

File Name	SHA-1 Hash
poco-dev/contracts/Store.sol	b5edb04dabdc5983a117d074e7b273e4956fe34f
poco-dev/contracts/libs/IexecLibCore_v5.sol	359c785f15d6ac64197e89a4f8c358c9eba9ff57
poco-dev/contracts/libs/IexecLibOrders_v5.sol	65d30c4d5069636495034aa62993516ffcd6b006
poco-dev/contracts/modules/DelegateBase.sol	966321486cf7049912cfaf34ea8fcfa36a665b09
poco-dev/contracts/modules/delegates/ENSIntegrationDelegate.sol	509ad5bda5fb7896699fe92fa4f1783f2116453e
poco-dev/contracts/modules/delegates/IexecAccessorsABILegacyDelegate.sol	257f318160dfd6a848c43bfe2d4db45551398825
poco-dev/contracts/modules/delegates/IexecAccessorsDelegate.sol	8bbc143e3ea0e731c6c5785689d324c3fc7376a8
poco-dev/contracts/modules/delegates/IexecCategoryManagerDelegate.sol	b42cb5c07838d5eb8da1f8088e9a1a6e4dac1fb1
poco-dev/contracts/modules/delegates/IexecERC20Common.sol	54ecb31c576017c96fa7e322102a039453974f73
poco-dev/contracts/modules/delegates/IexecERC20Delegate.sol	6b6e404844c727e57a13991c07d90b1b4ed5d05a
poco-dev/contracts/modules/delegates/IexecEscrowNativeDelegate.sol	d0f96ed32949a8d072695254eb17acdb8a691337

File Name	SHA-1 Hash
poco-dev/contracts/modules/delegates/IexecEscrowTokenDelegate.sol	1c0177cff23a426fe40c27d65ab2c854e5cf3cfe
poco-dev/contracts/modules/delegates/IexecMaintenanceDelegate.sol	1c1eef2430cc35ce3366a4ac10fcc9139e845e52
poco-dev/contracts/modules/delegates/IexecMaintenanceExtraDelegate.sol	00b3b7ab05f2f79040200a1528a2f1a5249da606
poco-dev/contracts/modules/delegates/IexecOrderManagementDelegate.sol	aa2f3dccf020d9c21f507701279e92e5c4fc6c79
poco-dev/contracts/modules/delegates/IexecPocoDelegate.sol	a43fa6b7f4c088adfdfe531aceff8e9c73bcc276
poco-dev/contracts/modules/delegates/IexecRelayDelegate.sol	096d24d4b15593ee1cee7f972bd26cb8deab6179
poco-dev/contracts/modules/delegates/SignatureVerifier.sol	83160d2e5924055aa3206f0578c32fc584131ce4
poco-dev/contracts/modules/interfaces/ENSIntegration.sol	f0ad54cfbc0f3f5dda2048af72f81b3b636eaabb
poco-dev/contracts/modules/interfaces/IOwnable.sol	b33a9ad33d580bb88eed1013e13b69835840ef51
poco-dev/contracts/modules/interfaces/IexecAccessors.sol	c2bff677eb8d606af5698adfd8d247cfb7883565

File Name	SHA-1 Hash
poco-dev/contracts/modules/interfaces/IexecAccessorsABILegacy.sol	91f97256685b91010441f9bf9e51f0e44585a5d5
poco-dev/contracts/modules/interfaces/IexecCategoryManager.sol	2c0bc1c4f9e3261c4e1cee4b78887b14f65b9e1b
poco-dev/contracts/modules/interfaces/IexecERC20.sol	66841034833adca8c16c3011feaac38cd1c768fc
poco-dev/contracts/modules/interfaces/IexecEscrowNative.sol	d8847e54490a498845664e05b301ee6a59c2e6dd
poco-dev/contracts/modules/interfaces/IexecEscrowToken.sol	0ff3340f349dd50126d4a7edeebe3417fe7b033e
poco-dev/contracts/modules/interfaces/IexecMaintenance.sol	1822954ab2aa4f315f00547534657fb5e94e5688
poco-dev/contracts/modules/interfaces/IexecMaintenanceExtra.sol	47bdc786183681f4ba0baf29b3d0fcc009eb30bd
poco-dev/contracts/modules/interfaces/IexecOrderManagement.sol	bdc694d099bc20ca89c1577f7b403ce2b0c06b0d
poco-dev/contracts/modules/interfaces/IexecPoco.sol	f82e8e5e5aa70c35345d7a6a318eaa4c0610c246
poco-dev/contracts/modules/interfaces/IexecRelay.sol	be2ab578ba29627be4643efd27598ebd749e7fae

File Name	SHA-1 Hash
poco-dev/contracts/modules/interfaces/IexecTokenSpender.sol	202b77df4de1fcdacd1a26d0ec72fd0ad96ae720
poco-dev/contracts/registries/IRegistry.sol	ffe3c15f48605d24c5b1497529e01fffc2066b02
poco-dev/contracts/registries/Registry.sol	a3837bdfa95c5024ad1251e60a27c15d76ddefa1
poco-dev/contracts/registries/RegistryEntry.sol	b6864be405a056d6ef172b4a50b30afc35692622
poco-dev/contracts/registries/apps/App.sol	cac8649f11ce8bc2c93b85e003e429b3bce58c0b
poco-dev/contracts/registries/apps/AppRegistry.sol	e1d7c5744cbff24c80dc4b8fd743ed95e1a6e262
poco-dev/contracts/registries/datasets/Dataset.sol	83257f5ac85d8da3460954b2c53fb420b5932390
poco-dev/contracts/registries/datasets/DatasetRegistry.sol	bf147967c07446dde52b7b1c275bafaac0644e37
poco-dev/contracts/registries/workerpools/Workerpool.sol	16be9246eb5652d24a46146b541f063ac90be269
poco-dev/contracts/registries/workerpools/WorkerpoolRegistry.sol	cab0ee262cd9d5b42dce9ee6965e540b6b27d1cf
poco-dev/contracts/tools/Migrations.sol	ab396f2c04aed69f6cdef9a954b8f22da7822d21
poco-dev/contracts/tools/testing/TestClient.sol	0bcf03e777105ce8d52d304a3704064ac5a4d944

File Name	SHA-1 Hash
poco-dev/contracts/tools/testing/TestReceiver.sol	5404782e56839826c5f9649f42f87be409b082c4

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
IexecInterfaceNative	Interface	IOwnable, IexecAccessors, IexecCategoryManager, IexecERC20, IexecEscrowNative, IexecMaintenance, IexecOrderManagement, IexecPoco, IexecRelay, IexecTokenSpender, ENSIntegration		

Contract	Type	Bases		
IexecInterfaceNativeABILegacy	Interface	IOwnable, IexecAccessors, IexecAccessorsABILegacy, IexecCategoryManager, IexecERC20, IexecEscrowNative, IexecMaintenance, IexecOrderManagement, IexecPoco, IexecRelay, IexecTokenSpender, ENSIntegration		
IexecInterfaceToken	Interface	IOwnable, IexecAccessors, IexecCategoryManager, IexecERC20, IexecEscrowToken, IexecMaintenance, IexecOrderManagement, IexecPoco, IexecRelay, IexecTokenSpender, ENSIntegration		

Contract	Type	Bases		
IexecInterfaceTokenABILegacy	Interface	IOwnable, IexecAccessors, IexecAccessorsABILegacy, IexecCategoryManager, IexecERC20, IexecEscrowToken, IexecMaintenance, IexecOrderManagement, IexecPoco, IexecRelay, IexecTokenSpender, ENSIntegration		
Store	Implementation	ERC1538Store		
IexecLibCore_v5	Library			
IexecLibOrders_v5	Library			
L	hash	Public ❗		NO❗
L	hash	Public ❗		NO❗
L	hash	Public ❗		NO❗
L	hash	Public ❗		NO❗
L	hash	Public ❗		NO❗
L	hash	Public ❗		NO❗

Contract	Type	Bases		
└	hash	Public ❗		NO❗
└	hash	Public ❗		NO❗
└	hash	Public ❗		NO❗
└	toEthSignedMessageHash	Public ❗		NO❗
└	toEthTypedStructHash	Public ❗		NO❗
└	recover	Public ❗		NO❗
DelegateBase	Implementation	Store		
└		Internal 🔒	🛑	
ENSIntegrationDelegate	Implementation	ENSIntegration, ENSReverseRegistration, DelegateBase		
└	setName	External ❗	🛑	onlyOwner
IexecAccessorsABILegacyDelegate	Implementation	IexecAccessorsABILegacy, DelegateBase		
└	viewDealABILegacy_pt1	External ❗		NO❗
└	viewDealABILegacy_pt2	External ❗		NO❗

Contract	Type	Bases		
└	viewConfigABILegacy	External ❗		NO❗
└	viewAccountABILegacy	External ❗		NO❗
└	viewTaskABILegacy	External ❗		NO❗
└	viewContributionABILegacy	External ❗		NO❗
└	viewCategoryABILegacy	External ❗		NO❗
IexecAccessorsDelegate	Implementation	IexecAccessors, DelegateBase		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	frozenOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	viewAccount	External ❗		NO❗
└	token	External ❗		NO❗
└	viewDeal	External ❗		NO❗

Contract	Type	Bases		
L	viewConsumed	External ❗		NO❗
L	viewPresigned	External ❗		NO❗
L	viewTask	External ❗		NO❗
L	viewContribution	External ❗		NO❗
L	viewScore	External ❗		NO❗
L	resultFor	External ❗		NO❗
L	viewCategory	External ❗		NO❗
L	countCategory	External ❗		NO❗
L	appregistry	External ❗		NO❗
L	datasetregistry	External ❗		NO❗
L	workerpoolregistry	External ❗		NO❗
L	teebroker	External ❗		NO❗
L	callbackgas	External ❗		NO❗
L	contribution_deadline_ratio	External ❗		NO❗
L	reveal_deadline_ratio	External ❗		NO❗
L	final_deadline_ratio	External ❗		NO❗

Contract	Type	Bases		
L	workerpool_stake_ratio	External ❗		NO❗
L	kitty_ratio	External ❗		NO❗
L	kitty_min	External ❗		NO❗
L	kitty_address	External ❗		NO❗
L	groupmember_purpose	External ❗		NO❗
L	eip712domain_separator	External ❗		NO❗
IexecCategoryManagerDelegate	Implementation	IexecCategoryManager, DelegateBase		
L	createCategory	External ❗	🛑	onlyOwner
IexecERC20Common	Implementation	DelegateBase		
L	_transfer	Internal 🔒	🛑	
L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
L	_approve	Internal 🔒	🛑	

Contract	Type	Bases		
IexecERC20Delegate	Implementation	IexecERC20, DelegateBase, IexecERC20Common		
L	transfer	External ❗	🛑	NO❗
L	approve	External ❗	🛑	NO❗
L	approveAndCall	External ❗	🛑	NO❗
L	transferFrom	External ❗	🛑	NO❗
L	increaseAllowance	External ❗	🛑	NO❗
L	decreaseAllowance	External ❗	🛑	NO❗
IexecEscrowNativeDelegate	Implementation	IexecEscrowNative, DelegateBase, IexecERC20Common		
L		External ❗	💵	NO❗
L	deposit	External ❗	💵	NO❗
L	depositFor	External ❗	💵	NO❗
L	depositForArray	External ❗	💵	NO❗
L	withdraw	External ❗	🛑	NO❗
L	recover	External ❗	🛑	onlyOwner
L	_deposit	Internal 🔒	🛑	
L	_withdraw	Internal 🔒	🛑	

Contract	Type	Bases		
IexecEscrowTokenDelegate	Implementation	IexecEscrowToken, IexecTokenSpender, DelegateBase, IexecERC20Common		
L		External ❗	💵	NO❗
L	deposit	External ❗	🛑	NO❗
L	depositFor	External ❗	🛑	NO❗
L	depositForArray	External ❗	🛑	NO❗
L	withdraw	External ❗	🛑	NO❗
L	recover	External ❗	🛑	onlyOwner
L	receiveApproval	External ❗	🛑	NO❗
L	_deposit	Internal 🔒	🛑	
L	_withdraw	Internal 🔒	🛑	
IexecMaintenanceDelegate	Implementation	IexecMaintenance, DelegateBase		
L	configure	External ❗	🛑	onlyOwner
L	domain	External ❗		NO❗
L	updateDomainSeparator	External ❗	🛑	NO❗
L	importScore	External ❗	🛑	NO❗

Contract	Type	Bases		
L	setTeeBroker	External ❗	🛑	onlyOwner
L	setCallbackGas	External ❗	🛑	onlyOwner
L	_chainId	Internal 🔒		
L	_domain	Internal 🔒		
IexecMaintenanceExtraDelegate	Implementation	IexecMaintenanceExtra, DelegateBase		
L	changeRegistries	External ❗	🛑	onlyOwner
IexecOrderManagementDelegate	Implementation	IexecOrderManagement, DelegateBase		
L	manageAppOrder	Public ❗	🛑	NO❗
L	manageDatasetOrder	Public ❗	🛑	NO❗
L	manageWorkerpoolOrder	Public ❗	🛑	NO❗
L	manageRequestOrder	Public ❗	🛑	NO❗

Contract	Type	Bases		
IexecPocoDelegate	Implementation	IexecPoco, DelegateBase, IexecERC20Common, SignatureVerifier		
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 ❗		NO❗
L	verifyPresignature	External ❗		NO❗

Contract	Type	Bases		
L	verifyPresignatureOrSignature	External ❗		NO❗
L	matchOrders	Public ❗	🛑	NO❗
L	initialize	Public ❗	🛑	NO❗
L	contribute	Public ❗	🛑	NO❗
L	reveal	External ❗	🛑	NO❗
L	reopen	External ❗	🛑	onlyScheduler
L	finalize	External ❗	🛑	onlyScheduler
L	claim	Public ❗	🛑	NO❗
L	contributeAndFinalize	Public ❗	🛑	NO❗
L	checkConsensus	Internal 🔒	🛑	
L	distributeRewards	Internal 🔒	🛑	
L	executeCallback	Internal 🔒	🛑	
L	initializeArray	External ❗	🛑	NO❗
L	claimArray	External ❗	🛑	NO❗
L	initializeAndClaimArray	External ❗	🛑	NO❗

Contract	Type	Bases		
IexecRelayDelegate	Implementation	IexecRelay, DelegateBase		
L	broadcastAppOrder	External ❗	🛑	NO❗
L	broadcastDatasetOrder	External ❗	🛑	NO❗
L	broadcastWorkerpoolOrder	External ❗	🛑	NO❗
L	broadcastRequestOrder	External ❗	🛑	NO❗
SignatureVerifier	Implementation	DelegateBase		
L	_isContract	Internal 🔒		
L	_addrToKey	Internal 🔒		
L	_checkIdentity	Internal 🔒		
L	_checkSignature	Internal 🔒		
L	_checkPresignature	Internal 🔒		
L	_checkPresignatureOrSignature	Internal 🔒		

Contract	Type	Bases		
ENSIntegration	Interface			
L	setName	External ❗	🛑	NO❗
IOwnable	Interface			
L	owner	External ❗		NO❗
L	renounceOwnership	External ❗	🛑	NO❗
L	transferOwnership	External ❗	🛑	NO❗
IexecAccessors	Interface	IOracle		
L	name	External ❗		NO❗
L	symbol	External ❗		NO❗
L	decimals	External ❗		NO❗
L	totalSupply	External ❗		NO❗
L	balanceOf	External ❗		NO❗
L	frozenOf	External ❗		NO❗
L	allowance	External ❗		NO❗
L	viewAccount	External ❗		NO❗
L	token	External ❗		NO❗
L	viewDeal	External ❗		NO❗
L	viewConsumed	External ❗		NO❗
L	viewPresigned	External ❗		NO❗

Contract	Type	Bases		
L	viewTask	External ❗		NO❗
L	viewContribution	External ❗		NO❗
L	viewScore	External ❗		NO❗
L	viewCategory	External ❗		NO❗
L	countCategory	External ❗		NO❗
L	appregistry	External ❗		NO❗
L	datasetregistry	External ❗		NO❗
L	workerpoolregistry	External ❗		NO❗
L	teebroker	External ❗		NO❗
L	callbackgas	External ❗		NO❗
L	contribution_deadline_ratio	External ❗		NO❗
L	reveal_deadline_ratio	External ❗		NO❗
L	final_deadline_ratio	External ❗		NO❗
L	workerpool_stake_ratio	External ❗		NO❗
L	kitty_ratio	External ❗		NO❗
L	kitty_min	External ❗		NO❗

Contract	Type	Bases		
L	kitty_address	External ❗		NO❗
L	groupmember_purpose	External ❗		NO❗
L	eip712domain_separator	External ❗		NO❗
IexecAccessorsABILegacy	Interface			
L	viewAccountABILegacy	External ❗		NO❗
L	viewDealABILegacy_pt1	External ❗		NO❗
L	viewDealABILegacy_pt2	External ❗		NO❗
L	viewTaskABILegacy	External ❗		NO❗
L	viewContributionABILegacy	External ❗		NO❗
L	viewCategoryABILegacy	External ❗		NO❗
L	viewConfigABILegacy	External ❗		NO❗

Contract	Type	Bases		
IexecCategoryManager	Interface			
L	createCategory	External ❗	🛑	NO❗
IexecERC20	Interface			
L	transfer	External ❗	🛑	NO❗
L	approve	External ❗	🛑	NO❗
L	transferFrom	External ❗	🛑	NO❗
L	increaseAllowance	External ❗	🛑	NO❗
L	decreaseAllowance	External ❗	🛑	NO❗
L	approveAndCall	External ❗	🛑	NO❗
IexecEscrowNative	Interface			
L		External ❗	💵	NO❗
L	deposit	External ❗	💵	NO❗
L	depositFor	External ❗	💵	NO❗
L	depositForArray	External ❗	💵	NO❗
L	withdraw	External ❗	🛑	NO❗
L	recover	External ❗	🛑	NO❗

Contract	Type	Bases		
IexecEscrowToken	Interface			
L		External ❗	💵	NO❗
L	deposit	External ❗	🛑	NO❗
L	depositFor	External ❗	🛑	NO❗
L	depositForArray	External ❗	🛑	NO❗
L	withdraw	External ❗	🛑	NO❗
L	recover	External ❗	🛑	NO❗
IexecMaintenance	Interface			
L	configure	External ❗	🛑	NO❗
L	domain	External ❗		NO❗
L	updateDomainSeparator	External ❗	🛑	NO❗
L	importScore	External ❗	🛑	NO❗
L	setTeeBroker	External ❗	🛑	NO❗
L	setCallbackGas	External ❗	🛑	NO❗
IexecMaintenanceExtra	Interface			
L	changeRegistries	External ❗	🛑	NO❗

Contract	Type	Bases		
IexecOrderManagement	Interface			
L	manageAppOrder	External ❗	🛑	NO❗
L	manageDatasetOrder	External ❗	🛑	NO❗
L	manageWorkerpoolOrder	External ❗	🛑	NO❗
L	manageRequestOrder	External ❗	🛑	NO❗
IexecPoco	Interface			
L	verifySignature	External ❗		NO❗
L	verifyPresignature	External ❗		NO❗
L	verifyPresignatureOrSignature	External ❗		NO❗
L	matchOrders	External ❗	🛑	NO❗
L	initialize	External ❗	🛑	NO❗
L	contribute	External ❗	🛑	NO❗
L	reveal	External ❗	🛑	NO❗
L	reopen	External ❗	🛑	NO❗
L	finalize	External ❗	🛑	NO❗
L	claim	External ❗	🛑	NO❗

Contract	Type	Bases		
L	contributeAndFinalize	External ❗	🛑	NO❗
L	initializeArray	External ❗	🛑	NO❗
L	claimArray	External ❗	🛑	NO❗
L	initializeAndClaimArray	External ❗	🛑	NO❗
IexecRelay	Interface			
L	broadcastAppOrder	External ❗	🛑	NO❗
L	broadcastDatasetOrder	External ❗	🛑	NO❗
L	broadcastWorkerpoolOrder	External ❗	🛑	NO❗
L	broadcastRequestOrder	External ❗	🛑	NO❗
IexecTokenSpender	Interface			
L	receiveApproval	External ❗	🛑	NO❗
IRegistry	Implementation	IERC721Enumerable		

Contract	Type	Bases		
L	isRegistered	External ❗		NO❗
Registry	Implementation	IRegistry, ERC721Full, ENSReverseRegistration, Ownable		
L		Public ❗	🛑	ERC721Full
L	initialize	External ❗	🛑	onlyOwner
L	_mintCreate	Internal 🔒	🛑	
L	_mintPredict	Internal 🔒		
L	isRegistered	External ❗		NO❗
L	setName	External ❗	🛑	onlyOwner
L	setTokenURI	External ❗	🛑	NO❗
RegistryEntry	Implementation	ENSReverseRegistration		
L	_initialize	Internal 🔒	🛑	
L	owner	Public ❗		NO❗
L	setName	External ❗	🛑	onlyOwner
App	Implementation	RegistryEntry		
L	initialize	Public ❗	🛑	NO❗

Contract	Type	Bases		
AppRegistry	Implementation	Registry		
└		Public ❗	🛑	Registry
└	encodeInitializer	Internal 🔒		
└	createApp	External ❗	🛑	NO❗
└	predictApp	External ❗		NO❗
Dataset	Implementation	RegistryEntry		
└	initialize	Public ❗	🛑	NO❗
DatasetRegistry	Implementation	Registry		
└		Public ❗	🛑	Registry
└	encodeInitializer	Internal 🔒		
└	createDataset	External ❗	🛑	NO❗
└	predictDataset	External ❗		NO❗
Workerpool	Implementation	RegistryEntry		
└	initialize	Public ❗	🛑	NO❗
└	changePolicy	External ❗	🛑	onlyOwner
WorkerpoolRegistry	Implementation	Registry		

Contract	Type	Bases		
L		Public ❗	🛑	Registry
L	encodeInitializer	Internal 🔒		
L	createWorkerpool	External ❗	🛑	NO❗
L	predictWorkerpool	External ❗		NO❗
Migrations	Implementation	Ownable		
L		Public ❗	🛑	NO❗
L	setCompleted	Public ❗	🛑	onlyOwner
L	upgrade	Public ❗	🛑	onlyOwner
TestClient	Implementation	IOracleConsumer		
L		Public ❗	🛑	NO❗
L	receiveResult	External ❗	🛑	NO❗
TestReceiver	Implementation	IexecTokenSpender		
L		Public ❗	🛑	NO❗
L	receiveApproval	External ❗	🛑	NO❗

Legend

Symbol	Meaning
🛑	Function can modify state

Symbol	Meaning
💵	Function is payable

A.3.4 Tests Suite

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

```
Started ganache daemon (pid=33197)
Compiling ... success
Migrating ... success
Running tests ... Using network 'development'.


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

# web3 version: 1.2.1
Chainid is: 1589476946750
Chaintype is: private


  Contract: ERC1538
    ✓ Ownership (100ms)
    ✓ ERC1538Query - totalFunctions
    ✓ ERC1538Query - functionByIndex (324ms)
    ✓ ERC1538Query - functionById (300ms)
    ✓ ERC1538Query - functionExists (262ms)
    ✓ ERC1538Query - functionSignatures (161ms)
    ✓ ERC1538Query - delegateFunctionSignatures (200ms)
    ✓ ERC1538Query - delegateAddress (226ms)
    ✓ ERC1538Query - delegateAddresses (42ms)
    ✓ ERC1538 - receive (81ms)
    ✓ ERC1538 - fallback (75ms)
    ✓ ERC1538 - no update
    ✓ ERC1538 - remove fallback (48ms)

  Contract: ERC1538
    ✓ Ownership (81ms)
    ✓ ERC1538Query - totalFunctions
    ✓ ERC1538Query - functionByIndex (258ms)
    ✓ ERC1538Query - functionById (242ms)
    ✓ ERC1538Query - functionExists (224ms)
    ✓ ERC1538Query - functionSignatures (125ms)
    ✓ ERC1538Query - delegateFunctionSignatures (185ms)
    ✓ ERC1538Query - delegateAddress (227ms)
    ✓ ERC1538Query - delegateAddresses (38ms)
    ✓ ERC1538 - receive (78ms)
    ✓ ERC1538 - fallback (87ms)
    ✓ ERC1538 - no update (46ms)
    ✓ ERC1538 - remove fallback (59ms)

  Contract: GenericFactory
    createContract
      ✓ select random salt
      ✓ predict address
      ✓ success (first) (41ms)
      ✓ failure (duplicate) (42ms)
      ✓ post check (63ms)
    createContractAndCall
      ✓ select random salt and value
      ✓ predict address
      ✓ success (first) (48ms)
      ✓ failure (duplicate) (46ms)
      ✓ post check (63ms)


  36 passing (5s)

success
```

```
Started ganache daemon (pid=41839)
Compiling ... success
Migrating ... success
Running tests ... Using network 'development'.


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

# web3 version: 1.2.1
Chainid is: 1589478046040
Chaintype is: private
Checking factory availability
→ Factory is available on this network
# web3 version: 1.2.1
Chainid is: 1589478046040
Chaintype is: private
Deployer is: 0x5132931eec048e21237A61611E9B0E3f45740A81
[factoryDeployer] IexecLibOrders_v5
[factory] Preparing to deploy IexecLibOrders_v5 ...
[factory] IexecLibOrders_v5 successfully deployed at 0xEb13F139AAc341c7Af13
```

```
[factoryDeployer] ERC1538UpdateDelegate
[factoryDeployer] ERC1538QueryDelegate
[factoryDeployer] IexecAccessorsDelegate
[factoryDeployer] IexecAccessorsABILegacyDelegate
[factoryDeployer] IexecCategoryManagerDelegate
[factoryDeployer] IexecERC20Delegate
[factoryDeployer] IexecEscrowTokenDelegate
[factoryDeployer] IexecMaintenanceDelegate
[factoryDeployer] IexecOrderManagementDelegate
[factoryDeployer] IexecPocoDelegate
[factoryDeployer] IexecRelayDelegate
[factoryDeployer] ENSIntegrationDelegate
[factoryDeployer] IexecMaintenanceExtraDelegate
[factory] Preparing to deploy ERC1538UpdateDelegate ...
[factory] Preparing to deploy ERC1538QueryDelegate ...
[factory] Preparing to deploy IexecAccessorsDelegate ...
[factory] Preparing to deploy IexecAccessorsABILegacyDelegate ...
[factory] Preparing to deploy IexecCategoryManagerDelegate ...
[factory] Preparing to deploy IexecERC20Delegate ...
[factory] Preparing to deploy IexecEscrowTokenDelegate ...
[factory] Preparing to deploy IexecRelayDelegate ...
[factory] Preparing to deploy ENSIntegrationDelegate ...
[factory] Preparing to deploy IexecMaintenanceExtraDelegate ...
[factory] Preparing to deploy IexecMaintenanceDelegate ...
[factory] Preparing to deploy IexecOrderManagementDelegate ...
[factory] Preparing to deploy IexecPocoDelegate ...
[factory] ERC1538UpdateDelegate successfully deployed at 0x910E52F82235A04dA
[factory] ERC1538QueryDelegate successfully deployed at 0xF340a314A5C1124c19
[factory] IexecAccessorsDelegate successfully deployed at 0xBa04C795A66C5A92
[factory] IexecAccessorsABILegacyDelegate successfully deployed at 0x7518B56
[factory] IexecCategoryManagerDelegate successfully deployed at 0xEe13BF38ef
[factory] IexecERC20Delegate successfully deployed at 0x6075792A9Fd3E7866329
[factory] IexecEscrowTokenDelegate successfully deployed at 0x50CC88A50687b8
[factory] IexecRelayDelegate successfully deployed at 0x6eaF90784D9D4e488782
[factory] ENSIntegrationDelegate successfully deployed at 0x8c5A8ed5e894083a
[factory] IexecMaintenanceExtraDelegate successfully deployed at 0x63C79fd11
[factory] IexecMaintenanceDelegate successfully deployed at 0x857e990ea784Df
[factory] IexecOrderManagementDelegate successfully deployed at 0xf31B0ecD9c
[factory] IexecPocoDelegate successfully deployed at 0x0C58DAe9F07e3568648C0
[factoryDeployer] ERC1538Proxy
[factory] Preparing to deploy ERC1538Proxy ...
[factory] ERC1538Proxy successfully deployed at 0x01B82aa475cA4767bF9142D25A
IexecInstance deployed at address: 0x01B82aa475cA4767bF9142D25AfF95C002b644a
ERC1538 link: ERC1538QueryDelegate
ERC1538 link: IexecAccessorsDelegate
ERC1538 link: IexecAccessorsABILegacyDelegate
ERC1538 link: IexecCategoryManagerDelegate
 C1538 link: IexecERC20Delegate
 RC1538 link: IexecEscrowTokenDelegate
ERC1538 link: IexecMaintenanceDelegate
```

```
ERC1538 link: IexecOrderManagementDelegate
ERC1538 link: IexecPocoDelegate
ERC1538 link: IexecRelayDelegate
ERC1538 link: ENSIntegrationDelegate
ERC1538 link: IexecMaintenanceExtraDelegate
[factoryDeployer] AppRegistry
[factoryDeployer] DatasetRegistry
[factoryDeployer] WorkerpoolRegistry
[factory] Preparing to deploy AppRegistry ...
[factory] Preparing to deploy DatasetRegistry ...
[factory] Preparing to deploy WorkerpoolRegistry ...
[factory] AppRegistry successfully deployed at 0x535912F1a9fADA4bc7140d7835b
[factory] DatasetRegistry successfully deployed at 0x77b837dCfC9Ee3332B45cBb
[factory] WorkerpoolRegistry successfully deployed at 0x8A5BE516b28Bdf6E1641
AppRegistry        deployed at address: 0x535912F1a9fADA4bc7140d7835beED72af
DatasetRegistry    deployed at address: 0x77b837dCfC9Ee3332B45cBb003d0A6d842
WorkerpoolRegistry deployed at address: 0x8A5BE516b28Bdf6E1641Ea46e4a5cBe4Bb
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
# web3 version: 1.2.1
Chainid is: 1589478046040
Chaintype is: private
Deployer is: 0x5132931eec048e21237A61611E9B0E3f45740A81
ENSRegistry deployed at address: 0x7c4b77ea0B14e8921504F3BFd29Af8c4b7149697
PublicResolver deployed at address: 0xc458F93f859cE58C48632e28ef8eECd99A9074
# web3 version: 1.2.1
Chainid is: 1589478046040
Chaintype is: private
Deployer is: 0x5132931eec048e21237A61611E9B0E3f45740A81
0xabcd1339Ec7e762e639f4887E2bFe5EE8023E23E received 10000000
0x000a9c787a972F70F0903890E266F41c795C4DcA received 10000000
0x1a69b2EB604dB8eBa185dF03ea4F5288dcbbD248 received 1000
0x2Ab2674aA374Fe6415d11f0a8FcbD8027fc1e6A9 received 1000
0x3A3406E69ADf886c442Ff1791cbf67CEA679275D received 1000
0x4AEF50214110FdaD4e8B9128347F2Ba1eC72F614 received 1000
0x5AF4eef749db212C594EFAc14C056a05261deDA9 received 1000
0x6A5A96F946b6d5054B3eAf032D30744A3818f81F received 1000
0x7A9519E67F552f154657D65C2efe88D52bFeb025 received 1000
x8a5fDA948126db50687Ba100F7D6555ea92Ec841 received 1000
x9A2Df059ddFC9937d6673a7C6786E71F98b7f1cf received 1000
0x10aa7Fc6B27aEfF79Ff52924AfC23Da40A8261ca received 1000
```

```
0x11aCBF759A658c229F4bE1Adb9aAB1CF660FF192 received 1000
0x12aa1fec8Ad2FD03157A11A6825DD9feB24D0b34 received 1000
0x13aE3ce3DC8b9D8401894Bc178a1E48a7dce2218 received 1000
0x14a60197Ed9cd183e4275c207CA8B1c594016392 received 1000
0x15a7853A3E9EA1bBae16935f5f32207030cCFbAc received 1000
0x16a1E3872210A20F99307E6b716f87F247dB11C8 received 1000
0x17A7212Bea68Ac0588bEA6e575a9f320C3640EA5 received 1000
0x18a9b259Bb67Fe5d19281c341f868dEb2bD86343 received 1000
0x19A1fAad2a0E0e3201fd0c8ea0EE465735225853 received 1000
0x20ae0f1D4659AD306b6960237FFc90Ef0c2f280f received 1000
0x21A4d0C871fA050Fb1452BD19293A25bFC4D5702 received 1000
0x22A0689175038c13523c646924f86e1857284619 received 1000
0x23aeD71591b1b3a67CBEd6C6262137Be7cBd59e3 received 1000
0x24A854e8701b9Bf212F87EA11713c41d3f05966c received 1000
0x25A643502C3EbcF3d2754423d5330213024A0cBA received 1000
0x26aCa9d1b57f35FF51BB7C485e78B4E44E962357 received 1000
0x27ABdc52E2A4Fd3eE7D925BF1df3cf53572bC477 received 1000
0x28aDC8519C97f1BC958202aEAC903F1d0ab47F8C received 1000
0x29A338B1b1c236CCb1cF3cB1E0651B450E430317 received 1000
0x30A5EE7052E49788188e61169B5D6B005a8b5d2F received 1000
0x31A4d10b5E3a9e31F63e5999607894F48eD882eA received 1000
0x32A41A8ddE2380cEF575395B5791324c577d71a6 received 1000
0x33A52EF23051e987f3E09DE1cF1a67162F70482d received 1000
0x34a12776b37209328a8e5163C1702863d418e955 received 1000
0x35AE22B5E0a41C7A9d85D4Fa6a837090Ca79e993 received 1000
0x36A1b8383fed641503e98b179494Bbf5F27AaF8c received 1000
0x37aDF6AE77f17A4Cc0C8389d8c3D230c11Ac5bF8 received 1000
0x38a0C2964A4cd8512174A0Cd0e803BBa4e267076 received 1000
0x39Af7D9b9cC9a68674E243Cf0CcDBd6ea8a2357f received 1000
0x40a7c92Bf935A4818Effc7817EC00C4C240632D6 received 1000
0x41A5dE13C0A709776619c5A1a882d716199bC6ad received 1000
0x42a6957A345bd26218FdAA3Fb2fcD30cEDFF7FAc received 1000
0x43A21F43B8425299B8604954A847a392DA294ab4 received 1000
0x44a95B35B96f707119f6c339417E17B7B12E621b received 1000
0x45a5C24eFf3F2BeB48d98ED528c6A1c0670aD068 received 1000
0x46a63E885A308A1815A3b6a6A57563999123d7Eb received 1000
0x47A226F54A079263b29A9a230CF46f7bd844D576 received 1000
0x48A8C9183A7Af6e7C9A4fAbd7aD620e81d00A33f received 1000
0x49a215ac86A096219188427De3FD6690072cB855 received 1000
0x50ad6FeE6402bf20D6302cA5C7E00a9b8639Fdc3 received 1000
0x51AfC7821A57fBc594E1a34650fbB1766D776182 received 1000
0x52A6E86048296FC020CBA86BcBd33D532E551db8 received 1000
0x53a3A945aB61e629dbE3F74aee63c5947A98f67B received 1000
0x54a96145bDAc3e25b84C1aD24679b3823e90312b received 1000
0x55a77232ef101de4D346a16b2b9A07E9a566ac9C received 1000
0x56a65029221167a44d341359944Bfb775A4DB68f received 1000
0x57Aa7b7621a36FE71FfED623C7E611F75C9802cE received 1000
0x58a02eDFa30C9F56EBe0D4d58164dA4e35c7aABd received 1000
0x59A71610cCfa580d6aFe9bF2CC4D5f8Ab48c71b1 received 1000
0x60A6E7dC4B69d815D40f18feddc149Df456D2118 received 1000
```

```
0x61A10043CEaB4FbA94FeEfF78888484DD7575a9A received 1000
0x62aE40A538345BcEC2b2A73f441B0AD7C4e1D667 received 1000
0x63Abae0eEbCD23Bb84FB88Be6Fe6fbfBf0c16EF7 received 1000
0x64a230bca31dCe0Ce78F46C55f338564881A6B7e received 1000
0x65a6802FC9Cc481762A691B01fccf8DB2aA36e60 received 1000
0x66A5165E97869b09e4a55b25d5E0c6c3daAa85E9 received 1000
0x67aaba1Efa65c308dE1Df6b952271Fc2b0742c3a received 1000
0x68A19Af4fcA17311b4be6AF8AE2309E3055cfABd received 1000
0x69A8093b4f44fE25274a26330be0fB2D4B5857BB received 1000
0x70a0B33623839c1a0f952c51Ae13Efd745e6d2c7 received 1000
0x71ac40D0eb099182868d3D947Bdf92804A478C4f received 1000
0x72ac54F114EE0dfB4EC56B183a0c7Bb85f779168 received 1000
0x73A834A6c616899A7484E1f6eA36BA737Fb948e1 received 1000
0x74a100c60966b833b63FFa9F32f54D2ab5AFfD49 received 1000
0x75aa687E0E68f57587F8de8aF873d1d2DE5c397b received 1000
0x76a6C64a9a26246571C8769bc3258F1F3fFdDE8B received 1000
0x77a220e10dD3698d86A46E0781EA787024278DC7 received 1000
0x78A974a701275Ee61714842B9cFA04731C55A8Ca received 1000
0x79AFF737E77Da55ABA900177A06936CAa1048D31 received 1000
0x80aFf346ECf0D1499A9C1A3A0c9EBb70318769D3 received 1000
0x81A3cae5ACCa20B1f9Bfb07fcDD1D329621E895B received 1000
0x82A5157d6A66c28d7C2bEE46b7eBAEB77052ba75 received 1000
0x83a0D67107a4D65C0f47AaF1A804450BaFf71b20 received 1000
0x84A69E2BE32d26ea10CFFE138E50797412A7B44F received 1000
0x85a724eC22872A20d7B038e8A8216582Da0C64eF received 1000
0x86a0AB0Df4EbC6E5307E689f9360F59FF965d4b2 received 1000
0x87aa664CACf8e28B951186329420D96bDC8F70F5 received 1000
0x88AFd7E3d6eF74Dd8d56F6FD4181733127807A6d received 1000
0x89A7cf637A5f6caAC2FC3F47Cdaac9Fcc3574e10 received 1000
0x90AcB3C757F6F3060043Bd533548D9c0aF13dC8E received 1000
0x91aEE896557143b7FCda0372ec6673aB213B1469 received 1000
0x92a909d30C710fA4DB53b863Fe07e065E4C7f17A received 1000
0x93aA915f4D9265be9a9d3bc4D6C131c79BDDfE7b received 1000
0x94a5a325c5953240F33fb44d325f64374687f449 received 1000
0x95ADFFb8CF8754d6Cb67c71A46F07aA667D6fFE1 received 1000
0x96aEa88341402f4ab071eb15b76061E5CEBA0eBE received 1000
0x97a7EC10d982e97E514cB96E65a796b437157e3c received 1000
0x98Ad26771c4a990e0e166925Cc8aD0BC5Ce5848F received 1000
0x99afcbb25Ccb26d09982342b1a14c306Bf38bb0f received 1000
0x100Ad00aF2144cD3D65A3789a09C05684463a4c5 received 1000
0x101AF8cD450eAa0b596585aF7078b08Ea46eC55f received 1000
0x102aD376f258b4e0CcC25069B8d78E828F96DF16 received 1000
0x103af1BdF6C91f8d99D2287C3e3d7df6CCF25C37 received 1000
0x104A77819dE2FEE866fc7003897F808ACc5BD225 received 1000
0x105A03787f89DCBF418d79965490815F609a636a received 1000
0x106ae86bE3D46Ac4211f4950318A728C2aeD5048 received 1000
0x107AD4F890b9B8842BB3ee587dD547bffB4A42b9 received 1000
0x108A359CBDBFD92527B6d098e8456cC3121ECdF5 received 1000
0x109aa7B2e94dEAf1FF3002FAB13278EF354e8e1d received 1000
```

```
0x110a268dEb44734E9884c9f6e7241dEB3e757aFc received 1000
0x111A35B42Bb128A0b7d4272dE8AB5e4D71224540 received 1000
0x112A60b70F2835B053b62f17DFCf651BBA8143E8 received 1000
0x113adECfad0B63f1bd0c4D5D03B00A1b12263339 received 1000
0x114a72518770E64c2063c5A87F3F00Cf9dF78C2b received 1000
0x115A664e8c254a6042d48cdBfB9249fC55baF2B5 received 1000
0x116a0A6815076224Bb1C8570Da56288a4C2617b3 received 1000
0x117a0eE6a85c40F0570E285D7E022226ABe160a5 received 1000
0x118A935490A6C110E0bA6654d8aF992647796f77 received 1000
0x119aE6a195b3048e05206B9EAF3012723b52aD38 received 1000
0x120Ae1332E852118074632F1188ce8B5548A9cE8 received 1000
0x122aF4bb0c562029eA5333D2B6364dfb558Ab88A received 1000
0x121a9CBa5f33Ea435153a62FADA442a263290bD5 received 1000
0x123a783F50437633D120088C45706D99D9C8c163 received 1000
0x124A7a834D29f7D979AD125FA41c5be121493124 received 1000
0x125ad0ca6EE6eAd3328da248eB1640604b6Aeecb received 1000
0x126a3f609bf8EDcfD3a336c4E833Bae2952408db received 1000
0x127a064b169d38C0B322D722dA84cDa991Bd315e received 1000
0x128a75434761b0CD9840132958A9cacEFC4bf072 received 1000
0x129Af5D4C362F0522875938ACfaefcD459Bb6253 received 1000
0x130Acec95F4C11C317Ef7F00Be692686d5ae5A44 received 1000
0x131A707664eeE61139118945DB112D85302f78A9 received 1000
0x132a0bB6E3A40cb412E4ad125ED0954C01b91b67 received 1000
0x133AA93376306658C09e2f187BF934E3C134c239 received 1000
0x134A365E26b5dbd1BaCA93AB46c0d35a992D095a received 1000
0x135AD7C99a99405C5D8783D78614FEAE8c0961E7 received 1000
0x136aB508Bf8A3dBCe300F0e4991876202FC80CB9 received 1000
0x137A88fB258F66D2817E33366b065C723a7F0704 received 1000
0x138a285dE4EC9437CC5aE6072c3B17D6BF03eDfc received 1000
0x139ADD64267eE1e217B2183D874a6E87f2273c49 received 1000
0x140a3Db8f02E3de807908A1C269508B7dBCDefeC received 1000
0x141Aa5767D71c5e08bcC52B63aD4a51a82910cee received 1000
0x142ab121D4d641e2Ab82aC7A45d13FDAb9d432ee received 1000
0x143a2313b3e966DBA3854A02d6aeFd0c23489B82 received 1000
0x144af280E84341cCeaDFb7B317c18B880A228b6f received 1000
0x145abBf00384cAf891aF1623B7B240ef5f0E36D4 received 1000
0x146aeFb264ca2b94cA807186c16EE2B687ec039C received 1000
0x147AdCA34520bd99E1f1C03A71831cCEf2CA5f4c received 1000
0x148abcD2674Ed44893dcFeAA509cA87FD46f16f5 received 1000
0x149aAECDaD6cfeb5bB105b80d5c3539E948644fc received 1000
0x150a93c20AE038ea7453856b907321908C48f72e received 1000
0x151A4D3c898bA7639EdE5083448b904C713A92F5 received 1000
0x152A3ce83261FDfa77c2930770C5d23342bbf088 received 1000
0x153AC70724B2033a7Fcbe969193786BA33fb4d8C received 1000
0x154A03b6C9352dd18C7343096FA372f1030D6D48 received 1000
0x155A99EC6c6f91D531EfEEA2bEd728232859B198 received 1000
0x156AbA3eFF44957e8D746754C72F67a455a07508 received 1000
 x157a5135F0eEf861972fBc24A9BF381918eA2FdF received 1000
  158ADd5AEc7dC30aA90589B99e09065eCFF8BDAd received 1000
0x159AB5f6b9cB33ab5B83144bFC636069d5670A01 received 1000
```

```
0x160adEA2A9399AeB5758B622B84335DA13047A0E received 1000
0x161AA2012F3825c28cAa62A52E13aAF8F1140E4c received 1000
0x162AbD33846ca2fD2195A3e47A241693625c14f1 received 1000
0x163aF6A07C41a9DEC559EB7F95eeeb54439A986d received 1000
0x164Aec18D489Ac1833092517fA9AC1729D43CFCe received 1000
0x165aD5fA053cbea3af07E07165B641B6858AD97d received 1000
0x166A3B3A5efDb986c4014E375506ca944Fc169b1 received 1000
0x167a69Dbc31B55CD8973538692d9678263DE0f92 received 1000
0x168aE3966e0dab4C71AA5fC49D6BB162Adb6ea1E received 1000
0x169A022f508d0733F2F05F9A6828372829A14D3C received 1000
0x170a1E89e460F145fA602B28c82f39A63147dff5 received 1000
0x171ACC73D210772D9d83B71a435e163FB62F805F received 1000
0x172af2f797afb825e17988DFD595Fe2edF5b078F received 1000
0x173A8e207FF51e5ac17Da7E7B0020e5a595f216C received 1000
0x174A04c0e4f46f750b8F3Bcee2654EAF1cD3A3C0 received 1000
0x175A3765Af6B1658828A42dF38D760Ef038Bd6c6 received 1000
0x176A3d1a06E30846d6Cc5a698a04E0a036ce8822 received 1000
0x177A4d59Ce426745F4a84b6e54c0Cf89de40627C received 1000
0x178a81324F7d58E955eA0A310cadD86AFcd25F37 received 1000
0x179Ac618B76EA27be5e7d5Ec5C8761B72d61C01d received 1000
0x180A829B7F62Ef0516B826fab14847b9EAa04552 received 1000
0x181a030FDa05E906833aD2A1DB4A9bD8Bde23FF4 received 1000
0x182a4696A1ce62FBd44702E8085DB15d31C00bd2 received 1000
0x183AD0FE4abfd421F2974C8E69aE544FE70d6642 received 1000
0x184aC75B5d0124BA0411972Ac28819deC2f71F9e received 1000
0x185a5d55e9B0FfFEF4934c8e8c8bb46D8e1Cc319 received 1000
0x186A4287430A7F279A75d78b3Df5F80602F045C6 received 1000
0x187A9A44f2a536ad170f65139f80D3Da421401d2 received 1000
0x188a9b9Ca5C589299Ee4C853B800dF6E3208C47f received 1000
0x189A02cbA4a1a842EB307886D9C233Bf8eB342eb received 1000
0x190aa36be17a7067C46cb241916554F3b8F5f8fC received 1000
0x191Ae12537940d8a68007772DcA660cAD28E24CE received 1000
0x192a5313a6997B4E9993aAD011c9E3015Ff15fFe received 1000
0x193A1621298978848381Ca6FDe161B648a071387 received 1000
0x194A92602C770eCe78eF575A3C31A2A8ad34284d received 1000
0x195A18fB280ED190f30Be8CD80C3eE851d414d5e received 1000
0x196A7cA3529049B48C9372c0c039F2741F817090 received 1000
0x197A37eD6552f3Dbd5B4C37865379Bc711cfE523 received 1000
0x198a3588f389F32f18C8B6832cC1C38BC2b468F5 received 1000
0x199a3aE634249Aa216FAFD76fff9be7721b64E50 received 1000
0x200Ac17Cae67a7A10372d7262D31972fD2b59809 received 1000
0x201a31d8db88ddA273E1f84cCd63A81743Ad57b8 received 1000
0x202A44a04A03cBC6BbbAd505BCc31EAd6c48F31C received 1000
0x203aD2082639D49594a733e4b6ECb5a2029226a1 received 1000
0x204Af0eEE643Dc3fbE59fe6802E0a6756c43BCEc received 1000
0x205A96e5B1E4dd880FFB163A9909E4dE2C4663d5 received 1000
0x206aDB086bD6D07663623d9097CC87Db2ACfC0eE received 1000
x207aD2d733f74C1f81Ab9Bf88fFa8cE6B24107C7 received 1000
x208a2864F33022A1520915671557dC660aD10eEA received 1000
0x209Adc0230b4d47388CF15a778106F0289584eDc received 1000
```

```
0x210AF403293e0f4bc55f04cebBb5a957ae57fF6d received 1000
0x211ACC33CaD39F8f5A58e9Bc1E6BAA9e87692574 received 1000
0x212ad4Ba61aF5C5963F6234B7B5c7b745EC2a0D5 received 1000
0x213A008eAdC9e886De32b3BEe6d9b0b762FA6107 received 1000
0x214aA361cAeD44920b7673E25f2a20AB807B2d8E received 1000
0x215Ac7e465e109A8e678534623700d89cDdB7B47 received 1000
0x216aA1642df616ACeC88A9E0ccAB40BfeE5E4670 received 1000
0x217a025c0ddf3832c0B32A36C597665cB25769Fb received 1000
0x218AA95a897F2289708910803ACa10570E1eB951 received 1000
0x219a156696E6F12C07EE7F2348660C995D3fca3F received 1000
0x220aaE72C25f536aE648206DE1aDA44c98f9EB2f received 1000
0x221a4A36271EC5811cA22A330EDe98914d1dE1Bc received 1000
0x222A0Aa930caB0e4023778A3d9eB1625D963c300 received 1000
0x223a8a303Ca0f37E668ea7A54A0dC67579Ee1d28 received 1000
0x224a6142263d4107a2709A01Bc66BDc2b55Cd376 received 1000
0x225a7A70E4afaE96d3Dd137dE102F8b6043DeAc1 received 1000
0x226A8b66628ca81e3Bf35D0CEe77781e6291646D received 1000
0x227AD65232ad8804f19Dee818109eAB63AdeBFfb received 1000
0x228A19dDF28B6766b91EABeb2e31862f643f473B received 1000
0x229A7A304474016C8A2fEe2FA7668f0c021f2092 received 1000
0x230AdD06091495cC05053Cf3fe01961C7f0d3F71 received 1000
0x231Ad4FF515e7c713a6123d413e167E22dF6a6B1 received 1000
0x232A24fE2768C4F55009434B5d70Fc4Fe9e6Ec6b received 1000
0x233aF87AE95093B7893D4366218e72253dd6bF6B received 1000
0x234Acfafb44241Dfb3885D2575e4271B024EEe92 received 1000
0x235aBDAa4A17cCBE7Ae45FAcD5421b6941349a03 received 1000
0x236aA1eF8661ab1f62d00ed5c2ed54018C9617d8 received 1000
0x237a8f766ee194b8f89E907d1653442B004dd5cA received 1000
0x238ae320D6A38bFA9BD51D2347c2B6C6a3cc64e9 received 1000
0x239Ab6Ed796C8Dc882Cbf699498aD786Cf4DD0A9 received 1000
0x240a500c9b3D45678D5F7e14401F138b9296A213 received 1000
0x241AF60fc6A83274698b04e139dc8D6144A0B8e4 received 1000
0x242a4299EE6b1E467a7b3d4Bf9DC7F5Bf694AC98 received 1000
0x243a1360Eb0bdB806DFE3a7b9A1EbB5Ef05BdD0F received 1000
0x244a4644EE0B41E5Bb8061A9C6dD7b97EAaF7137 received 1000
0x245aA01A0Fe737cDe0ca670b354ab5842696FAE3 received 1000
0x246A5c3bd98A3c83A107134Eb3a297d2fAa811Fa received 1000
0x247AA64022f7E59B9476341B05c1A1184e5FF54B received 1000
0x248A3E336c7B37319C40c7aEe4F09E86125699B1 received 1000
0x249AaB1b71Dc59c682e7Ad24089372BE22591A7a received 1000
0x250a3919982ca7CEF58960fF716122dbb4514036 received 1000
The deployed ERC1538Proxy supports 95 functions:
[0] 0x910E52F82235A04dA139C19E28924edFFa68FF39 updateContract(address,string
[1] 0x63C79fd1121FAC33f619c2322c54ab37Da8EE143 owner()
[2] 0x63C79fd1121FAC33f619c2322c54ab37Da8EE143 renounceOwnership()
[3] 0x63C79fd1121FAC33f619c2322c54ab37Da8EE143 transferOwnership(address)
[4] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 totalFunctions()
[5] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 functionByIndex(uint256)
[6] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 functionById(bytes4)
[7] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 functionExists(string)
```

```
[8] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 delegateAddress(string)
[9] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 functionSignatures()
[10] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 delegateFunctionSignatures(a
[11] 0xF340a314A5C1124c19DBc7dC30Ca954f432CAEf8 delegateAddresses()
[12] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd name()
[13] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd symbol()
[14] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd decimals()
[15] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd totalSupply()
[16] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd balanceOf(address)
[17] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd frozenOf(address)
[18] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd allowance(address,address)
[19] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewAccount(address)
[20] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd token()
[21] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewDeal(bytes32)
[22] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewConsumed(bytes32)
[23] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewPresigned(bytes32)
[24] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewTask(bytes32)
[25] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewContribution(bytes32,add
[26] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewScore(address)
[27] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd resultFor(bytes32)
[28] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd viewCategory(uint256)
[29] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd countCategory()
[30] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd appregistry()
[31] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd datasetregistry()
[32] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd workerpoolregistry()
[33] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd teebroker()
[34] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd callbackgas()
[35] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd contribution_deadline_ratio(
[36] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd reveal_deadline_ratio()
[37] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd final_deadline_ratio()
[38] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd workerpool_stake_ratio()
[39] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd kitty_ratio()
[40] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd kitty_min()
[41] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd kitty_address()
[42] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd groupmember_purpose()
[43] 0xBa04C795A66C5A9224D88505B892095c4aCa54fd eip712domain_separator()
[44] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewDealABILegacy_pt1(bytes3
[45] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewDealABILegacy_pt2(bytes3
[46] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewConfigABILegacy(bytes32)
[47] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewAccountABILegacy(address
[48] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewTaskABILegacy(bytes32)
[49] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewContributionABILegacy(by
[50] 0x7518B5618571919Dc888F0AcA9fe9243BCdD4892 viewCategoryABILegacy(uint25
[51] 0xEe13BF38ef953Cf37F931E895E282b86aC7E37Df createCategory(string,string
[52] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef transfer(address,uint256)
[53] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef approve(address,uint256)
[54] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef approveAndCall(address,uint2
[55] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef transferFrom(address,address
[56] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef increaseAllowance(address,ui
[57] 0x6075792A9Fd3E78663291A10295b2E468432c0Ef decreaseAllowance(address,ui
[57] [illegible] decreaseAllowance(address,ui
[58] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f receive
[59] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f deposit(uint256)
[60] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f depositFor(uint256,address)
[61] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f depositForArray(uint256[],ac
[62] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f withdraw(uint256)
[63] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f recover()
[64] 0x50CC88A50687b8Ed0fc7C5AA985Fa17e5D67440f receiveApproval(address,uint
[65] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 configure(address,string,str
[66] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 domain()
[67] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 updateDomainSeparator()
[68] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 importScore(address)
[69] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 setTeeBroker(address)
[70] 0x857e990ea784Df1304F15AFDe4739422F0bf4572 setCallbackGas(uint256)
[71] 0xf31B0ecD9dB3c4e204896730d7131BD0A625b6B8 manageAppOrder(((address,uir
[72] 0xf31B0ecD9dB3c4e204896730d7131BD0A625b6B8 manageDatasetOrder(((address
[73] 0xf31B0ecD9dB3c4e204896730d7131BD0A625b6B8 manageWorkerpoolOrder(((addr
[74] 0xf31B0ecD9dB3c4e204896730d7131BD0A625b6B8 manageRequestOrder(((address
[75] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 verifySignature(address,byte
[76] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 verifyPresignature(address,b
[77] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 verifyPresignatureOrSignatur
[78] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 matchOrders((address,uint256
[79] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 initialize(bytes32,uint256)
[80] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 contribute(bytes32,bytes32,b
[81] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 reveal(bytes32,bytes32)
[82] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 reopen(bytes32)
[83] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 finalize(bytes32,bytes)
[84] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 claim(bytes32)
[85] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 contributeAndFinalize(bytes3
[86] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 initializeArray(bytes32[],ui
[87] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 claimArray(bytes32[])
[88] 0x0C58DAe9F07e3568648C05aE9561Fc618Db95843 initializeAndClaimArray(byte
[89] 0x6eaF90784D9D4e48878236B4A9cb07Cd2f374b47 broadcastAppOrder((address,u
[90] 0x6eaF90784D9D4e48878236B4A9cb07Cd2f374b47 broadcastDatasetOrder((addre
[91] 0x6eaF90784D9D4e48878236B4A9cb07Cd2f374b47 broadcastWorkerpoolOrder((ac
[92] 0x6eaF90784D9D4e48878236B4A9cb07Cd2f374b47 broadcastRequestOrder((addre
[93] 0x8c5A8ed5e894083a233Ee00617AbD1Cc4347F3fD setName(address,string)
[94] 0x63C79fd1121FAC33f619c2322c54ab37Da8EE143 changeRegistries(address,adc


  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (135ms)
      assets
        app
          ✓ create (125ms)
        dataset
          ✓ create (150ms)
        workerpool
          ✓ create (191ms)
          ✓ create (101ms)
          ✓ change policy (44ms)
      tokens
        ✓ balances before (199ms)
        ✓ deposit (323ms)
        ✓ balances after (198ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify (42ms)
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (213ms)
        checks
          ✓ deal (61ms)
          ✓ config
          ✓ balances (189ms)
      [2] initialization
        ✓ [TX] initialize (63ms)
        checks
          ✓ task (53ms)
          ✓ balances (196ms)
      [3] contribute
        ✓ authorization signature (99ms)
        ✓ run
        ✓ [TX] contribute (180ms)
        ✓ task (54ms)
        ✓ balances (187ms)
        checks
          ✓ contribution (45ms)
      [4] reveal
        ✓ [TX] reveal (94ms)
        checks
          ✓ task (81ms)
          ✓ balances (193ms)
      [5] finalization
        ✓ [TX] finalize (133ms)
        checks
          ✓ task (54ms)
          ✓ balances (187ms)
    → summary
```

```
      ✓ balances (180ms)
      ✓ balances - extra (577ms)
      ✓ score (97ms)
matchOrders            705431
initialize             171160
contribute             282612
contribute             304185
reveal                  79662
reveal                  45462
finalize               251584
Total gas             1840096
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (106ms)
      assets
        app
          ✓ create (101ms)
        dataset
          ✓ create (90ms)
        workerpool
          ✓ create (81ms)
          ✓ change policy (43ms)
      tokens
        ✓ balances before (193ms)
        ✓ deposit (300ms)
        ✓ balances after (191ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (196ms)
        checks
          ✓ deal
          ✓ balances (184ms)
      [2] initialization
        ✓ [TX] initialize (58ms)
        checks
          ✓ task (50ms)
          ✓ balances (200ms)
      [3] contribute
        ✓ authorization signature (128ms)
        ✓ run
        worker 1
          ✓ [TX] contribute (101ms)
          ✓ task (74ms)
          ✓ balances (248ms)
          checks
            ✓ contribution
        worker 2 - TEE
          ✓ [TX] contribute (142ms)
          ✓ task (70ms)
          ✓ balances (239ms)
          checks
            ✓ contribution
      [4] reveal
        ✓ [TX] reveal (88ms)
        checks
          ✓ task (54ms)
          ✓ balances (181ms)
      [5] finalization
        ✓ [TX] finalize (118ms)
        checks
          ✓ task (55ms)
          ✓ balances (180ms)
    → summary
      ✓ balances (175ms)
      ✓ balances - extra (599ms)
      ✓ score (141ms)
matchOrders            705443
initialize             171160
contribute             282624
contribute (TEE)       304197
reveal                  79650
reveal                  45450
finalize               251572
Total gas             1840096
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (134ms)
      assets
        app
          ✓ create (136ms)
        dataset
```

```
          ✓ create (136ms)
        workerpool
          ✓ create (93ms)
          ✓ change policy (43ms)
      tokens
        ✓ balances before (180ms)
        ✓ deposit (279ms)
        ✓ balances after (181ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (198ms)
      [2] initialization
        ✓ [TX] initialize (55ms)
      [3] contribute
        ✓ authorization signature (68ms)
        ✓ run
        ✓ [TX] contribute (99ms)
      [4] reveal
        ✓ [TX] reveal (49ms)
      [5] finalization
        ✓ [TX] finalize (109ms)
    → summary
      ✓ task (52ms)
      ✓ balances (182ms)
      ✓ balances - extra (587ms)
      ✓ score (100ms)
matchOrders             705449
initialize              171160
contribute              357273
reveal                   79662
finalize                184778
Total gas              1498322
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
```

```
       setup
      ✓ score (96ms)
      assets
        app
          ✓ create (97ms)
        dataset
          ✓ create (101ms)
        workerpool
          ✓ create (85ms)
          ✓ change policy (41ms)
      tokens
        ✓ balances before (182ms)
        ✓ deposit (285ms)
        ✓ balances after (184ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (189ms)
      [2] initialization
        ✓ [TX] initialize (56ms)
      [3] contribute
        ✓ authorization signature (128ms)
        ✓ run
        ✓ [TX] contribute (169ms)
      [4] reveal
        ✓ [TX] reveal (82ms)
      [5] finalization
        ✓ [TX] finalize (113ms)
    → summary
      ✓ task (50ms)
      ✓ balances (188ms)
      ✓ balances - extra (547ms)
      ✓ score (101ms)
matchOrders             705414
initialize              171160
contribute              282636
contribute              331957
reveal                   79662
reveal                   45462
reveal                  45462
finalize                251584
Total gas              1867875
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (101ms)
      assets
        app
          ✓ create (109ms)
        dataset
          ✓ create (85ms)
        workerpool
          ✓ create (79ms)
          ✓ change policy (39ms)
      tokens
        ✓ balances before (180ms)
        ✓ deposit (277ms)
        ✓ balances after (199ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (179ms)
      [2] initialization
        ✓ [TX] initialize (54ms)
      [3] contribute
        ✓ authorization signature (180ms)
        ✓ run
        ✓ [TX] contribute (242ms)
      [4] reveal
        ✓ [TX] reveal (122ms)
      [5] finalization
        ✓ [TX] finalize (124ms)
    → summary
      ✓ task (50ms)
      ✓ balances (181ms)
      ✓ balances - extra (553ms)
      ✓ score (100ms)
matchOrders            705429
initialize             171148
contribute             282636
contribute             252606
contribute             336572
reveal                  79662
reveal                  45462
reveal                  45462
finalize               295794
Total gas             2214771
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (100ms)
      assets
        app
          ✓ create (90ms)
        dataset
          ✓ create (80ms)
        workerpool
          ✓ create (77ms)
          ✓ change policy (41ms)
      tokens
        ✓ balances before (242ms)
        ✓ deposit (286ms)
        ✓ balances after (186ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (177ms)
      [2] initialization
        ✓ [TX] initialize (55ms)
      [3] contribute
        ✓ authorization signature (241ms)
        ✓ run
        ✓ [TX] contribute (335ms)
      [4] reveal
        ✓ [TX] reveal (170ms)
      [5] finalization
        ✓ [TX] finalize (141ms)
    → summary
      ✓ task (51ms)
      ✓ balances (183ms)
      ✓ balances - extra (567ms)
      ✓ score (113ms)
matchOrders            705419
initialize             171160
contribute             282624
contribute             252640
contribute             252611
contribute             341267
reveal                  79662
reveal                  45462
reveal                  45462
reveal                  45462
finalize               340004
Total gas             2561773
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (97ms)
      assets
        app
          ✓ create (89ms)
        dataset
          ✓ create (84ms)
        workerpool
          ✓ create (75ms)
          ✓ change policy (39ms)
      tokens
        ✓ balances before (177ms)
        ✓ deposit (276ms)
        ✓ balances after (185ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
```

```
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (191ms)
      [2] initialization
        ✓ [TX] initialize (133ms)
      [3] contribute
        ✓ authorization signature (342ms)
        ✓ run
        ✓ [TX] contribute (402ms)
      [4] reveal
        ✓ [TX] reveal (166ms)
      [5] finalization
        ✓ [TX] finalize (150ms)
    → summary
      ✓ task (54ms)
      ✓ balances (189ms)
      ✓ balances - extra (569ms)
      ✓ score (98ms)
matchOrders            705441
initialize             171160
contribute             282636
contribute             267641
contribute             252594
contribute             252616
contribute             344833
reveal                  79662
reveal                  45462
reveal                  45462
reveal                  45462
finalize               345320
Total gas             2838289
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (100ms)
      assets
        app
          ✓ create (96ms)
        dataset
          ✓ create (87ms)
        workerpool
          ✓ create (158ms)
          ✓ change policy (45ms)
      tokens
```

```
        ✓ balances before (180ms)
        ✓ deposit (315ms)
        ✓ balances after (285ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (241ms)
      [2] initialization
        ✓ [TX] initialize task (231ms)
      [3] contribute
        ✓ authorization signature (395ms)
        ✓ run
        ✓ [TX] contribute (904ms)
      [4] reveal
        ✓ [TX] reveal (489ms)
      [5] finalization
        task 1
          ✓ [TX] finalize (163ms)
          checks
            ✓ task (64ms)
            ✓ balances (309ms)
            ✓ score (145ms)
        task 2
          ✓ [TX] finalize (172ms)
          checks
            ✓ task (72ms)
            ✓ balances (259ms)
            ✓ score (120ms)
        task 3
          ✓ [TX] finalize (155ms)
          checks
            ✓ task (51ms)
            ✓ balances (173ms)
            ✓ score (97ms)
    → summary
  tchOrders             705443
initialize              171148
initialize              190360
initialize              190360
initialize              190360
contribute              254893
contribute              304209
contribute              267653
contribute              331940
contribute              239922
contribute              224922
contribute              237623
contribute              252611
contribute              344838
reveal                   79662
reveal                   45462
reveal                   79662
reveal                   45462
reveal                   79662
reveal                   45462
reveal                   45462
reveal                   45462
finalize                326608
finalize                281608
finalize                274589
Total gas              5065023
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (95ms)
      assets
        app
          ✓ create (86ms)
        dataset
          ✓ create (87ms)
        workerpool
          ✓ create (75ms)
          ✓ change policy (39ms)
      tokens
        ✓ balances before (179ms)
        ✓ deposit (266ms)
        ✓ balances after (179ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
```

```
          ✓ sign (50ms)
          ✓ verify (54ms)
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (468ms)
      [2] initialization
        ✓ [TX] initialize task (154ms)
      [3] contribute
        ✓ authorization signature (316ms)
        ✓ run
        ✓ [TX] contribute (704ms)
      [4] reveal
        ✓ [TX] reveal (334ms)
      [5] finalization
        task 1
          ✓ [TX] finalize (116ms)
          checks
            ✓ task (54ms)
            ✓ balances (182ms)
            ✓ score (101ms)
        task 2
          ✓ [TX] finalize (115ms)
          checks
            ✓ task (54ms)
            ✓ balances (179ms)
            ✓ score (98ms)
        task 3
          ✓ [TX] finalize (157ms)
          checks
            ✓ task (53ms)
            ✓ balances (182ms)
            ✓ score (98ms)
    → summary
matchOrders            705423
matchOrders            634624
initialize             171160
initialize             190372
initialize             190372
contribute             254922
contribute             304197
contribute             267624
contribute             331940
contribute             239898
contribute             224893
contribute             237594
contribute             252611
contribute             344821
reveal                  79662
reveal                  45462
reveal                  79662
reveal                  45462
reveal                  79662
reveal                  45462
reveal                  45462
reveal                  45462
finalize               326608
finalize               281608
finalize               274589
Total gas             5699552
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (95ms)
      assets
        app
          ✓ create (89ms)
        dataset
          ✓ create (77ms)
        workerpool
          ✓ create (79ms)
          ✓ change policy (40ms)
      tokens
        ✓ balances before (176ms)
        ✓ deposit (276ms)
        ✓ balances after (177ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (199ms)
      [2] initialization
        ✓ [TX] initialize (56ms)
      [3] contribute
        ✓ [TX] contribute (225ms)
        check
```

```
          ✓ balances (184ms)
      [4] no reveal
        ✓ clock fast forward
      [5] reopen
        ✓ [TX] reopen (63ms)
      [6] contribute
        ✓ [TX] contribute (401ms)
        check
          ✓ balances (186ms)
      [7] reveal
        ✓ [TX] reveal (91ms)
      [8] finalization
        ✓ [TX] finalize (128ms)
    → summary
      ✓ balances (183ms)
      ✓ balances - extra (633ms)
      ✓ score (97ms)
matchOrders            705443
initialize             171148
contribute             254910
contribute             331940
contribute             267583
contribute             341063
reveal                  79650
reveal                  45450
finalize               262204
Total gas             2459391
      ✓ gas used

  Contract: Fullchain
# web3 version: 1.2.1
    → setup
      ✓ score (114ms)
      assets
        app
          ✓ create (91ms)
        dataset
          ✓ create (89ms)
        workerpool
          ✓ create (77ms)
          ✓ change policy (40ms)
      tokens
        ✓ balances before (177ms)
        ✓ deposit (269ms)
        ✓ balances after (188ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          ✓ sign
          ✓ verify
      [1] order matching
        ✓ [TX] match (176ms)
      [2] initialization
        ✓ [TX] initialize (55ms)
      [3] contributeAndFinalize
        ✓ authorization signature (64ms)
        ✓ run
        ✓ [TX] contributeAndFinalize (121ms)
    → summary
      ✓ task (61ms)
      ✓ balances (179ms)
      ✓ balances - extra (584ms)
      ✓ score (101ms)
matchOrders                 705374
initialize                  171160
contributeAndFinalize       399604
Total gas                  1276138
      ✓ gas used

  Contract: ENSIntegration
# web3 version: 1.2.1
    Initial state (migration)
      ✓ lookup (204ms)
      ✓ resolve (222ms)
    Reverse register
      unauthorized
        ✓ reverts (44ms)
      authorized
        ✓ success (60ms)
        ✓ lookup (43ms)

  Contract: Accessors
# web3 version: 1.2.1
    checking constant view methods
      escrow
        ✓ token
      ERC20 metadata
        ✓ name (46ms)
        ✓ symbol
        ✓ decimals
      Registries
      Registries
        ✓ AppRegistry
        ✓ DatasetRegistry
        ✓ AppRegistry

  Contract: CategoryManager
# web3 version: 1.2.1
    view
      invalid index
        ✓ reverts (77ms)
    create
      unauthorized create
        ✓ reverts (95ms)
      authorized
        ✓ success (69ms)
        ✓ emits event
        ✓ count update
        ✓ view newly created category

  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
        when the sender transfers all balance
          ✓ transfers the requested amount (75ms)
          ✓ emits a transfer event (38ms)
        when the sender transfers zero tokens
          ✓ transfers the requested amount (74ms)
          ✓ emits a transfer event
      when the recipient is the zero address
        ✓ reverts
    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 (78ms)
              ✓ decreases the spender allowance (58ms)
              ✓ emits a transfer event (42ms)
              ✓ emits an approval event (56ms)
            when the token owner does not have enough balance
              ✓ reverts (38ms)
              ✓ reverts (38ms)
          when the spender does not have enough approved balance
            when the token owner has enough balance
              ✓ reverts (50ms)
            when the token owner does not have enough balance
              ✓ reverts (39ms)
        when the recipient is the zero address
          ✓ reverts
      when the token owner is the zero address
        ✓ reverts (38ms)
    approve
      when the spender is not the zero address
        when the sender has enough balance
          ✓ emits an approval event
          when there was no approved amount before
            ✓ approves the requested amount (52ms)
          when the spender had an approved amount
            ✓ approves the requested amount and replaces the previous one (5
        when the sender does not have enough balance
          ✓ emits an approval event
          when there was no approved amount before
            ✓ approves the requested amount (53ms)
          when the spender had an approved amount
            ✓ approves the requested amount and replaces the previous one (5
      when the spender is the zero address
        ✓ reverts (42ms)
    decrease allowance
      when the spender is not the zero address
        when the sender has enough balance
          when there was no approved amount before
            ✓ reverts (40ms)
          when the spender had an approved amount
            ✓ emits an approval event (39ms)
            ✓ decreases the spender allowance subtracting the requested amou
            ✓ sets the allowance to zero when all allowance is removed (58ms
            ✓ reverts when more than the full allowance is removed (40ms)
        when the sender does not have enough balance
          when there was no approved amount before
            ✓ reverts (41ms)
          when the spender had an approved amount
            ✓ emits an approval event
            ✓ decreases the spender allowance subtracting the requested amou
            ✓ sets the allowance to zero when all allowance is removed (56ms
            ✓ reverts when more than the full allowance is removed (38ms)
      when the spender is the zero address
        ✓ reverts
    increase allowance
      when the spender is not the zero address
        when the sender has enough balance
          ✓ emits an approval event (39ms)
```

```
          when there was no approved amount before
            ✓ approves the requested amount (55ms)
          when the spender had an approved amount
            ✓ increases the spender allowance adding the requested amount (
        when the sender does not have enough balance
          ✓ emits an approval event
          when there was no approved amount before
            ✓ approves the requested amount (55ms)
          when the spender had an approved amount
            ✓ increases the spender allowance adding the requested amount (
      when the spender is the zero address
        ✓ reverts
    approveAndCall
      ✓ accepted by spender (39ms)
      ✓ rejected by spender (45ms)

  Contract: EscrowToken
# web3 version: 1.2.1
    fallback
      ✓ success
    deposit
      no tokens
        ✓ reverts (170ms)
      not approved
        ✓ reverts (176ms)
      approved
        ✓ success (148ms)
        ✓ emit events
    depositFor
      no tokens
        ✓ reverts (111ms)
      not approved
        ✓ reverts (148ms)
      approved
        ✓ success (321ms)
        ✓ emit events
    depositForArray
      no tokens
        ✓ reverts (284ms)
      not approved
        ✓ reverts (324ms)
      approved
        length missmatch
          amounts.length > target.length
            ✓ reverts (359ms)
          amounts.length > target.length
            ✓ reverts (274ms)
        length match
          ✓ success (306ms)
          ✓ emit events
    ApproveAndCall
      ✓ success (179ms)
      wrong token protection
        ✓ create dummy token (82ms)
        ✓ reverts (188ms)
    withdraw
      empty balance
        ✓ reverts (166ms)
      insufficient balance
        ✓ reverts (154ms)
      sufficient balance
        ✓ success (155ms)
        ✓ emit events
    recover
      unauthorized access
        ✓ reverts (54ms)
      no locked funds
        ✓ success (59ms)
        ✓ emit events
      locked funds
        ✓ locking funds (47ms)
        ✓ success (60ms)
        ✓ emit events

  Contract: Poco
# web3 version: 1.2.1
    ✓ cannot reconfigure (41ms)
>>>>>>    domain.chainId: 1
>>>>>> web.eth.net.getId: 1589478046040
    ✓ domain
    ✓ updateChainId (45ms)

  Contract: OrderManagement
# web3 version: 1.2.1
    ✓ [Genesis] App Creation (89ms)
    ✓ [Genesis] Dataset Creation (88ms)
    ✓ [Genesis] Workerpool Creation (82ms)
    cancel apporder
      ✓ unauthorized sender (107ms)
      ✓ unauthorized signature (137ms)
      ✓ authorized signature (122ms)
      ✓ authorized sender (95ms)
    cancel datasetorder
      ✓ unauthorized sender (106ms)
      ✓ unauthorized signature (133ms)
      ✓ authorized signature (122ms)
      ✓ authorized sender (86ms)
    cancel workerpoolorder
      ✓ unauthorized sender (107ms)
      ✓ unauthorized signature (136ms)
      ✓ authorized signature (118ms)
      ✓ authorized sender (89ms)
    cancel requestorder
      ✓ unauthorized sender (122ms)
      ✓ unauthorized signature (128ms)
      ✓ authorized signature (120ms)
      ✓ authorized sender (85ms)

  Contract: OrderManagement
# web3 version: 1.2.1
    ✓ [Genesis] deposit (262ms)
    ✓ [Genesis] App Creation (90ms)
    ✓ [Genesis] Dataset Creation (85ms)
    ✓ [Genesis] Workerpool Creation (82ms)
    apporder
      ✓ valid operation - sign (57ms)
      ✓ invalid operation (50ms)
      ✓ invalid operation (44ms)
    datasetorder
      ✓ valid operation - sign (53ms)
      ✓ invalid operation (49ms)
      ✓ invalid operation (40ms)
    workerpoolorder
      ✓ valid operation - sign (76ms)
      ✓ invalid operation (46ms)
      ✓ invalid operation (45ms)
    requestorder
      ✓ valid operation - sign (79ms)
      ✓ invalid operation (67ms)
      ✓ invalid operation (51ms)

  Contract: OrderManagement
# web3 version: 1.2.1
    ✓ [Genesis] deposit (254ms)
    ✓ [Genesis] App Creation (88ms)
    ✓ [Genesis] Dataset Creation (80ms)
    ✓ [Genesis] Workerpool Creation (75ms)
    sign apporder
      ✓ unauthorized sender (193ms)
      ✓ unauthorized signature (242ms)
      ✓ authorized signature (211ms)
      ✓ authorized sender (170ms)
    sign datasetorder
      ✓ unauthorized sender (192ms)
      ✓ unauthorized signature (227ms)
      ✓ authorized signature (227ms)
      ✓ authorized sender (175ms)
    sign workerpoolorder
      ✓ unauthorized sender (214ms)
      ✓ unauthorized signature (219ms)
      ✓ unauthorized signature (219ms)
      ✓ authorized signature (205ms)
      ✓ authorized sender (193ms)
    sign requestorder
      ✓ unauthorized sender (185ms)
      ✓ unauthorized signature (215ms)
      ✓ authorized signature (198ms)
      ✓ authorized sender (162ms)
    matching presigned orders
      ✓ match (364ms)

  Contract: Poco
# web3 version: 1.2.1
    ✓ [Genesis] deposit (254ms)
    ✓ [Genesis] App Creation (91ms)
    ✓ [Genesis] Dataset Creation (85ms)
    ✓ [Genesis] Workerpool Creation (74ms)
    ✓ [Genesis] Workerpool configuration (43ms)
    ✓ [Match - app-dataset-workerpool-user] (353ms)
    ✓ [Match - app-workerpool-user] (330ms)
    ✓ [Match - app-dataset-workerpool-user BOT] (351ms)
    ✓ [Match - Error - category] (155ms)
    ✓ [Match - Error - trust] (154ms)
    ✓ [Match - Error - appprice] (155ms)
    ✓ [Match - Error - datasetprice] (177ms)
    ✓ [Match - Error - workerpoolprice] (153ms)
    ✓ [Match - Error - apptag] (157ms)
    ✓ [Match - Error - datasettag] (158ms)
    ✓ [Match - Ok - workerpooltag] (281ms)
    ✓ [Match - Error - usertag] (176ms)
    ✓ [Match - Error - requested app] (153ms)
    ✓ [Match - Error - requested dataset] (154ms)
    ✓ [Match - Error - workerpoolrequest] (156ms)
    ✓ [Match - Error - app-datasetrestrict] (159ms)
    ✓ [Match - Ok - app-datasetrestrict] (271ms)
    ✓ [Match - Error - app-workerpoolrestrict] (176ms)
    ✓ [Match - Ok - app-workerpoolrestrict] (275ms)
    ✓ [Match - Error - app-requesterrestrict] (155ms)
    ✓ [Match - Ok - app-requesterrestrict] (270ms)
    ✓ [Match - Error - dataset-apprestrict] (155ms)
    ✓ [Match - Ok - dataset-apprestrict] (295ms)
    ✓ [Match - Error - app-workerpoolrestrict] (155ms)
    ✓ [Match - Ok - app-workerpoolrestrict] (273ms)
    ✓ [Match - Error - app-requesterrestrict] (158ms)
    ✓ [Match - Ok - app-requesterrestrict] (277ms)
    ✓ [Match - Error - workerpool-apprestrict] (160ms)
    ✓ [Match - Ok - workerpool-apprestrict] (268ms)
    ✓ [Match - Error - workerpool-datasetrestrict] (155ms)
    ✓ [Match - Ok - workerpool-datasetrestrict] (264ms)
    ✓ [Match - Error - workerpool-requesterrestrict] (176ms)
    ✓ [Match - Ok - workerpool-requesterrestrict] (276ms)
    ✓ [Match - Ok - workerpool-requesterrestrict] (276ms)
    ✓ [Match - Error - volume null] (283ms)

  Contract: Poco
# web3 version: 1.2.1
    ✓ [Setup] deposit (266ms)
    ✓ [Setup] (843ms)
    ✓ [1.1] Initialization - Correct (56ms)
    ✓ [1.2] Initialization - Error (low id) (47ms)
    ✓ [1.3] Initialization - Error (high id) (49ms)
    ✓ [1.4] Initialization - Error (already initialized) (51ms)

  Contract: Poco
# web3 version: 1.2.1
    ✓ [Setup] deposit (253ms)
    ✓ [Setup] (810ms)
    ✓ [setup] Initialization (293ms)
    ✓ [2.1][TAG] Contribute - Error (missing sgx) (58ms)
    ✓ [2.2][TAG] Contribute - Correct (sgx) (86ms)
    ✓ [2.3][TAG] Contribute - Error (unset) (65ms)
    ✓ [2.4][TAG] Contribute - Error (duplicate) (134ms)
    ✓ [2.5][TAG] Contribute - Error (authorization) (113ms)
    ✓ [2.6][TAG] Contribute - Error (enclave signature) (66ms)
    ✓ clock fast forward
    ✓ [2.7][TAG] Contribute - Late (59ms)

  Contract: Poco
# web3 version: 1.2.1
    ✓ [Setup] deposit (257ms)
    1) [Setup]

    Events emitted during test:
    ---------------------------

    IERC721.Transfer(
      from: <indexed> 0x0000000000000000000000000000000000000000 (type: addr
      to: <indexed> 0xB3c79F718589D834aF279981a633A2dA116Ac718 (type: addres
      tokenId: <indexed> 31374211685551723035548226552043074335477672O2 (typ
    )

    IERC721.Transfer(
      from: <indexed> 0x0000000000000000000000000000000000000000 (type: addr
      to: <indexed> 0xc50A09736Ad7C6f0331Cb5E5582339A1fF7B3e6e (type: addres
      tokenId: <indexed> 1430053037958512563531366597552228675841918792505 (
    )

    IERC721.Transfer(
      from: <indexed> 0x0000000000000000000000000000000000000000 (type: addr
      to: <indexed> 0x6Ee95a4B8417eD1D83F46B1632ba051d03CAC476 (type: addres
      tokenId: <indexed> 621472623740660239675733564111685551416607383546 (t
    )

    Warning: Could not decode event!

    Warning: Could not decode event!

    Warning: Could not decode event!

    Warning: Could not decode event!

    Warning: Could not decode event!

    Warning: Could not decode event!

    Warning: Could not decode event!


    ---------------------------
    2) [setup] Initialization
    > No events were emitted
    3) [2.1] Contribute - Correct
    > No events were emitted
    4) [2.2] Contribute - Correct (sgx)
    > No events were emitted
    5) [2.3] Contribute - Error (unset)
    > No events were emitted
    6) [2.4] Contribute - Error (duplicate)
    > No events were emitted
    7) [2.5] Contribute - Error (authorization)
    > No events were emitted
    8) [2.6] Contribute - Error (enclave signature)
    > No events were emitted
    9) clock fast forward
    > No events were emitted
    10) [2.7] Contribute - Late
    > No events were emitted

  Contract: Poco
# web3 version: 1.2.1
    ✓ [Setup] deposit (266ms)
    ✓ [Setup] (848ms)
    ✓ [setup] Initialization (295ms)
    ✓ [setup] Contribute (1072ms)
    ✓ [3.1] Reveal - Correct (41ms)
    ✓ [3.2] Reveal - Error (unset) (39ms)
    ✓ [3.3] Reveal - Error (no consensus) (39ms)
    ✓ [3.4] Reveal - Error (contribution value) (160ms)
    ✓ [3.6] Reveal - Error .hash) (43ms)
    ✓ [3.6] Reveal - Error .seal) (90ms)
    ✓ clock fast forward
```

```
      ✓ [3.7] Reveal - Error (late for reveal) (38ms)

    Contract: Poco
  # web3 version: 1.2.1
      ✓ [Setup] deposit (250ms)
      ✓ [Setup] (835ms)
      ✓ [setup] Initialization (308ms)
      ✓ [setup] Contribute (885ms)
      ✓ [setup] Reveal (227ms)
      ✓ [4.1] Finalize - Correct (full) (113ms)
      ✓ [4.2] Finalize - Error (partial - soon) (66ms)
      ✓ clock fast forward (38ms)
      ✓ [4.3] Finalize - Correct (partial - wait) (130ms)
      ✓ [4.4] Finalize - Error (no contribution) (66ms)
      ✓ [4.5] Finalize - Error (no consensus) (99ms)
      ✓ [4.6] Finalize - Error (no reveal) (52ms)
      ✓ clock fast forward
      ✓ [4.7] Finalize - Error (late) (50ms)

    Contract: Poco
  # web3 version: 1.2.1
      ✓ [Setup] deposit (279ms)
      ✓ [Setup] (951ms)
      ✓ [setup] Initialization (240ms)
      ✓ [setup] Contribute (779ms)
      ✓ [setup] Reveal (41ms)
      ✓ [5.1] Reopen - Error (early) (43ms)
      ✓ clock fast forward
      ✓ [5.2] Reopen - Correct (79ms)
      ✓ [5.3] Reopen - Error (status #1 - currently unset) (42ms)
      ✓ [5.4] Reopen - Error (status #2 - currently active) (40ms)
      ✓ [5.5] Reopen - Error (counter) (42ms)
      ✓ clock fast forward
      ✓ [5.6] Reopen - Error (late) (41ms)

    Contract: Poco
  # web3 version: 1.2.1
      ✓ [Setup] deposit (262ms)
      ✓ [Setup] (768ms)
      ✓ [setup] Initialization (239ms)
      ✓ [setup] Contribute (534ms)
      ✓ [setup] Reveal (121ms)
      ✓ [setup] Finalize (107ms)
      ✓ [6.1a] Claim - Error (soon #1) (39ms)
      ✓ [6.2a] Claim - Error (soon #2) (39ms)
      ✓ [6.3a] Claim - Error (soon #3) (39ms)
      ✓ [6.4a] Claim - Error (soon #4) (39ms)
      ✓ [6.5a] Claim - Error (soon #5) (38ms)
      ✓ [6.6a] Claim - Error (soon & finalized) (39ms)
      ✓ clock fast forward
      ✓ [6.1b] Claim - Correct (#1) (109ms)
      ✓ [6.2b] Claim - Correct (#2) (57ms)
      ✓ [6.3b] Claim - Correct (#3) (61ms)
      ✓ [6.4b] Claim - Correct (#4) (68ms)
      ✓ [6.5b] Claim - Correct (#5) (67ms)
      ✓ [6.6b] Claim - Error (finalized #7) (40ms)

    Contract: Poco
  # web3 version: 1.2.1
      ✓ [Setup] deposit (250ms)
      ✓ [Setup] (777ms)
      ✓ [setup] Initialization (126ms)
      ✓ [setup] Contribute (550ms)
      ✓ [setup] Reveal (114ms)
      ✓ [setup] Finalize (109ms)
      ✓ [7.1a] Claim - Error (soon #1) (40ms)
      ✓ [7.2a] Claim - Error (soon #2) (39ms)
      ✓ [7.3a] Claim - Error (soon #3)
      ✓ [7.4a] Claim - Error (soon #4) (39ms)
      ✓ [7.5a] Claim - Error (soon #5) (39ms)
      ✓ [7.6a] Claim - Error (soon & finalized) (49ms)
      ✓ [7.7a] Claim - Error (soon #6) (91ms)
      ✓ clock fast forward
      ✓ [7.1b] Claim - Correct (242ms)
      ✓ [7.6b] Claim - Error (finalized #7)
      ✓ [7.7a] Claim - Correct (143ms)

    Contract: Poco
  # web3 version: 1.2.1
      → setup
        tokens
          ✓ distribute (249ms)
          ✓ balances (161ms)
        assets
          app
            ✓ create (88ms)
          dataset
            ✓ create (79ms)
          workerpool
            ✓ create (77ms)
            ✓ change policy (41ms)
        orders
          ✓ app (43ms)
          ✓ workerpool
          ✓ requester (48ms)
      → fill Kitty
        ✓ [8.1a] match order (147ms)
        ✓ [8.2a] initialize (49ms)
        ✓ wait
        ✓ [8.3a] claim (58ms)
        ✓ [8.6a] claim (35ms)
        ✓ kitty balance (39ms)
        ✓ balances (130ms)
      → drain Kitty
        ✓ [8.1b] match order (149ms)
        ✓ [8.2b] initialize (52ms)
        ✓ [8.3b] contribute (80ms)
        ✓ [8.4b] reveal (41ms)
        ✓ [8.5b] finalize (87ms)
        ✓ kitty balance (52ms)
        ✓ balances (154ms)

    Contract: Poco
  # web3 version: 1.2.1
      ✓ check signature mechanism (278ms)
      ✓ [Genesis] App Creation (83ms)
      ✓ [Genesis] Dataset Creation (79ms)
      ✓ [Genesis] Workerpool Creation (73ms)
      ✓ check app hash (311ms)
      ✓ check dataset hash (304ms)
      ✓ check workerpool hash (328ms)
      ✓ check request hash (477ms)

    Contract: Relay
  # web3 version: 1.2.1
      → setup
        assets
          app
            ✓ create (84ms)
          dataset
            ✓ create (78ms)
          workerpool
            ✓ create (72ms)
            ✓ change policy (38ms)
        orders
          app
            ✓ sign
            ✓ verify
          dataset
            ✓ sign
            ✓ verify
          workerpool
            ✓ sign (38ms)
            ✓ verify
          request
            ✓ sign
            ✓ verify
      braodcasting
        broadcastAppOrder
          ✓ success (39ms)
          ✓ emit events
          ✓ emit events
        broadcastDatasetOrder
          ✓ success (38ms)
          ✓ emit events
        broadcastWorkerpoolOrder
          ✓ success
          ✓ emit events
        broadcastRequestOrder
          ✓ success (38ms)
          ✓ emit events

    Contract: Registries
  # web3 version: 1.2.1
      Registry
        ✓ cannot reinitialize (93ms)
        ✓ baseURI (54ms)
      Apps
        app #0
          ✓ creation (122ms)
          ✓ content (122ms)
          ✓ token details (93ms)
          ✓ duplicate protection (59ms)
        app #1
          ✓ creation (118ms)
          ✓ content (123ms)
          ✓ token details (95ms)
          ✓ duplicate protection (59ms)
        app #2
          ✓ creation (120ms)
          ✓ content (122ms)
          ✓ token details (97ms)
          ✓ duplicate protection (57ms)
        app #3
          ✓ creation (119ms)
          ✓ content (125ms)
          ✓ token details (98ms)
          ✓ duplicate protection (55ms)
        app #4
          ✓ creation (117ms)
          ✓ content (124ms)
          ✓ token details (99ms)
          ✓ duplicate protection (56ms)
        app #5
          ✓ creation (121ms)
          ✓ content (123ms)
          ✓ token details (95ms)
          ✓ duplicate protection (57ms)
        app #6
          ✓ creation (122ms)
          ✓ content (128ms)
          ✓ token details (99ms)
          ✓ duplicate protection (60ms)
        app #7
          ✓ creation (122ms)
          ✓ content (125ms)
          ✓ token details (97ms)
          ✓ duplicate protection (55ms)
      Datasets
        dataset #0
          ✓ creation (114ms)
          ✓ content (88ms)
          ✓ token details (100ms)
          ✓ duplicate protection (57ms)
        dataset #1
          ✓ creation (110ms)
          ✓ content (91ms)
          ✓ token details (97ms)
          ✓ duplicate protection (56ms)
        dataset #2
          ✓ creation (143ms)
          ✓ content (89ms)
          ✓ token details (96ms)
          ✓ duplicate protection (54ms)
        dataset #3
          ✓ creation (113ms)
          ✓ content (92ms)
          ✓ token details (95ms)
          ✓ duplicate protection (56ms)
        dataset #4
          ✓ creation (111ms)
          ✓ content (96ms)
          ✓ token details (99ms)
          ✓ duplicate protection (58ms)
        dataset #5
          ✓ creation (114ms)
          ✓ content (90ms)
          ✓ token details (97ms)
          ✓ duplicate protection (57ms)
        dataset #6
          ✓ creation (116ms)
          ✓ content (89ms)
          ✓ token details (100ms)
          ✓ duplicate protection (59ms)
        dataset #7
          ✓ creation (123ms)
          ✓ content (88ms)
          ✓ token details (96ms)
          ✓ duplicate protection (55ms)
      Workerpools
        workerpool #0
```

```
        ✓ creation (106ms)
        ✓ content (90ms)
        ✓ token details (97ms)
        ✓ duplicate protection (49ms)
      workerpool #1
        ✓ creation (107ms)
        ✓ content (89ms)
        ✓ token details (96ms)
        ✓ duplicate protection (53ms)
      workerpool #2
        ✓ creation (106ms)
        ✓ content (91ms)
        ✓ token details (97ms)
        ✓ duplicate protection (52ms)
      workerpool #3
        ✓ creation (109ms)
        ✓ content (90ms)
        ✓ token details (97ms)
        ✓ duplicate protection (53ms)
      workerpool #4
        ✓ creation (108ms)
        ✓ content (90ms)
        ✓ token details (111ms)
        ✓ duplicate protection (52ms)
      workerpool #5
        ✓ creation (111ms)
        ✓ content (94ms)
        ✓ token details (100ms)
        ✓ duplicate protection (50ms)
      workerpool #6
        ✓ creation (110ms)
        ✓ content (90ms)
        ✓ token details (98ms)
        ✓ duplicate protection (54ms)
      workerpool #7
        ✓ creation (107ms)
        ✓ content (95ms)
        ✓ token details (99ms)
        ✓ duplicate protection (51ms)

  Contract: Ressources
# web3 version: 1.2.1
    Apps
      app #0
        ✓ creation (100ms)
        ✓ content (130ms)
        ✓ reverse registration (107ms)
      app #1
        ✓ creation (88ms)
        ✓ content (129ms)
        ✓ reverse registration (102ms)
      app #2
        ✓ creation (87ms)
        ✓ content (127ms)
        ✓ reverse registration (101ms)
      app #3
        ✓ creation (93ms)
        ✓ content (128ms)
        ✓ reverse registration (101ms)
      app #4
        ✓ creation (89ms)
        ✓ content (136ms)
        ✓ reverse registration (101ms)
      app #5
        ✓ creation (90ms)
        ✓ content (130ms)
        ✓ reverse registration (103ms)
      app #6
        ✓ creation (86ms)
        ✓ content (130ms)
        ✓ reverse registration (102ms)
      app #7
        ✓ creation (89ms)
        ✓ content (131ms)
        ✓ reverse registration (103ms)
    Datasets
      dataset #0
        ✓ creation (84ms)
        ✓ content (94ms)
        ✓ reverse registration (107ms)
      dataset #1
        ✓ creation (83ms)
        ✓ content (96ms)
        ✓ reverse registration (202ms)
      dataset #2
        ✓ creation (163ms)
        ✓ content (94ms)
        ✓ reverse registration (107ms)
      dataset #3
        ✓ creation (83ms)
        ✓ content (98ms)
        ✓ reverse registration (155ms)
      dataset #4
        ✓ creation (83ms)
        ✓ content (96ms)
        ✓ reverse registration (108ms)
      dataset #5
        ✓ creation (85ms)
        ✓ content (93ms)
        ✓ reverse registration (104ms)
      dataset #6
        ✓ creation (85ms)
        ✓ content (93ms)
        ✓ reverse registration (103ms)
      dataset #7
        ✓ creation (88ms)
        ✓ content (95ms)
        ✓ reverse registration (103ms)
    Workerpools
      workerpool #0
        ✓ creation (79ms)
        ✓ content (91ms)
        ✓ reverse registration (108ms)
      workerpool #1
        ✓ creation (76ms)
        ✓ content (90ms)
        ✓ reverse registration (115ms)
      workerpool #2
        ✓ creation (77ms)
        ✓ content (95ms)
        ✓ reverse registration (105ms)
      workerpool #3
        ✓ creation (76ms)
        ✓ content (94ms)
        ✓ reverse registration (112ms)
      workerpool #4
        ✓ creation (77ms)
        ✓ content (94ms)
        ✓ reverse registration (112ms)
      workerpool #5
        ✓ creation (78ms)
        ✓ content (93ms)
        ✓ reverse registration (107ms)
      workerpool #6
        ✓ creation (89ms)
        ✓ content (95ms)
        ✓ reverse registration (110ms)
      workerpool #7
        ✓ creation (85ms)
        ✓ content (93ms)
        ✓ reverse registration (112ms)
      configuration
        ✓ owner can configure (115ms)
        ✓ owner restriction apply (117ms)
        ✓ invalid configuration refused (114ms)

  Contract: ERC1154: callback
web3 version: 1.2.1
    → setup
      ✓ score (96ms)
      ✓ score (96ms)
      assets
        app
          ✓ create (88ms)
        dataset
          ✓ create (93ms)
        workerpool
          ✓ create (75ms)
          ✓ change policy (53ms)
      tokens
        ✓ balances before (186ms)
        ✓ deposit (271ms)
        ✓ balances after (172ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify
        request
          no callback
            ✓ sign (41ms)
            ✓ verify
          invalid callback
            ✓ sign
            ✓ verify
          valid callback
            ✓ sign
            ✓ verify
          callback EOA
            ✓ sign
            ✓ verify
      [1] order matching
        ✓ [TX] match (656ms)
      [2] initialization
        ✓ [TX] initialize (169ms)
      [3] contribute
        ✓ [TX] contribute (318ms)
      [4] reveal
        ✓ [TX] reveal (162ms)
      [5] finalization
        no callback
          ✓ [TX] no call (89ms)
        invalid callback
          ✓ [TX] doesn't revert (91ms)
        valid callback
```

```
        valid callback
          ✓ [TX] call (117ms)
          ✓ check
        callback EOA
          ✓ [TX] doesn't revert (96ms)

  Contract: ERC1154: resultFor
# web3 version: 1.2.1
    → setup
      ✓ score (116ms)
      assets
        app
          ✓ create (102ms)
        dataset
          ✓ create (85ms)
        workerpool
          ✓ create (83ms)
          ✓ change policy (42ms)
      tokens
        ✓ balances before (183ms)
        ✓ deposit (278ms)
        ✓ balances after (185ms)
    → pipeline
      [0] orders
        app
          ✓ sign
          ✓ verify
        dataset
          ✓ sign
          ✓ verify
        workerpool
          ✓ sign
          ✓ verify (45ms)
        request
          ✓ sign
          ✓ verify (43ms)
      [1] order matching
        ✓ [TX] match (245ms)
      [2] initialization
        ✓ [TX] initialize (253ms)
      [3] contribute
        ✓ [TX] contribute (358ms)
      [4] reveal
        ✓ [TX] reveal (89ms)
      [5] finalization
        ✓ [TX] finalize (94ms)
    → result for
      uninitialized
        ✓ reverts
      initialized
```

```
        ✓ reverts
      contributed
        ✓ reverts
      consensus
        ✓ reverts
      reveal
        ✓ reverts
      finalized
        ✓ valid


  910 passing (3m)
  10 failing

  1) Contract: Poco
       [Setup]:
     Error: Returned error: VM Exception while processing transaction: rever
     at PromiEvent (node_modules/truffle/build/webpack:/packages/contract/li
      at TruffleContract.matchOrders (node_modules/truffle/build/webpack:/pa
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:217
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  2) Contract: Poco
       [setup] Initialization:
     Error: invalid bytes32 value (arg="", coderType="bytes32", value=undefi
     at PromiEvent (node_modules/truffle/build/webpack:/packages/contract/li
      at TruffleContract.initialize (node_modules/truffle/build/webpack:/pac
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:225
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  3) Contract: Poco
       [2.1] Contribute - Correct:
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/web
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:256
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  4) Contract: Poco
       [2.2] Contribute - Correct (sgx):
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/web
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:276
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  5) Contract: Poco
       [2.3] Contribute - Error (unset):
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/web
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:296
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  6) Contract: Poco
       [2.4] Contribute - Error (duplicate):
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/web
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:308
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  7) Contract: Poco
       [2.5] Contribute - Error (authorization):
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/web
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:337
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  8) Contract: Poco
       [2.6] Contribute - Error (enclave signature):
     TypeError: Cannot read property 'replace' of undefined
```

```
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/wet
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:352
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  9) Contract: Poco
       clock fast forward:
     Error: invalid bytes32 value (arg="", coderType="bytes32", value=undefi
     at PromiEvent (node_modules/truffle/build/webpack:/packages/contract/li
      at TruffleContract.viewTask (node_modules/truffle/build/webpack:/packa
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:359
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)

  10) Contract: Poco
       [2.7] Contribute - Late:
     TypeError: Cannot read property 'replace' of undefined
      at _solidityPack (node_modules/truffle/build/webpack:/node_modules/wet
      at _processSoliditySha3Args (node_modules/truffle/build/webpack:/node_
      at Function._.map._.collect (node_modules/truffle/build/webpack:/node_
      at Object.soliditySha3 (node_modules/truffle/build/webpack:/node_modul
      at sealByteResult (utils/odb-tools.js:202:22)
      at Object.sealResult (utils/odb-tools.js:214:9)
      at Context.<anonymous> (test/byContract/IexecPoco/02_contribute.js:373
      at runMicrotasks (<anonymous>)
      at processTicksAndRejections (internal/process/task_queues.js:97:5)



success
```

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.

Request a Security Review Today

Get in touch with our team to request a quote for a smart contract audit.

CONTACT US

AUDITS

FUZZING

SCRIBBLE

BLOG

TOOLS

RESEARCH

ABOUT

CONTACT

CAREERS

Subscribe to Our Newsletter

Stay up-to-date on our latest offerings, tools, and the world of blockchain security.

PRIVACY POLICY

Email*

e-mail address

→

POWERED BY CONSENSYS