CONSENSYS Diligence

rICO Audit

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

1 Executive Summary

This report presents the results of our engagement with **Lukso rICO** to review the *Reversible Initial Coin Offering*, a version of an ICO that gives investors the ability to reverse their investment in different stages.

The review was conducted over the course of two weeks, from **April 13th, 2020** to **April 27th, 2020** by Shayan Eskandari and Gonçalo Sá. A total of 15 person-days were spent.

During the first week, we reviewed the documentation and attended several code walkthrough sessions with the developers. Initial issues were discussed and resulted in a new commit to be the base of the audit by mid-week. In an effort to understand the system, we produced several ancillary visualizations (that can be seen throughout the audit report) over the course of the week.

During the second week we reviewed the codebase with the aid of the aforementioned visualizations and looked attentively for breaches of the invariants described in the Security Properties section.

2 Scope

Our review focused on the commit hash ~~**de6b22ba8991d77560e574eae7f4f1e17f643115**~~ **77517a4dceed53ff7c5a7f7580cb805831a7f8d5** (tree/audit). The list of files in scope can be found in the Appendix.

2.1 Documentations

The following documentation was provided by the client:

- rICO — The Reversible ICO
  - RICO - Making ICOs Fair, By Making Them Reversible by Fabian Vogelsteller (Devcon4)
- Inline comments and Github README
- Code walk through meeting

2.2 Objectives

Together with the **Lukso rICO** team, we identified the following priorities for our review

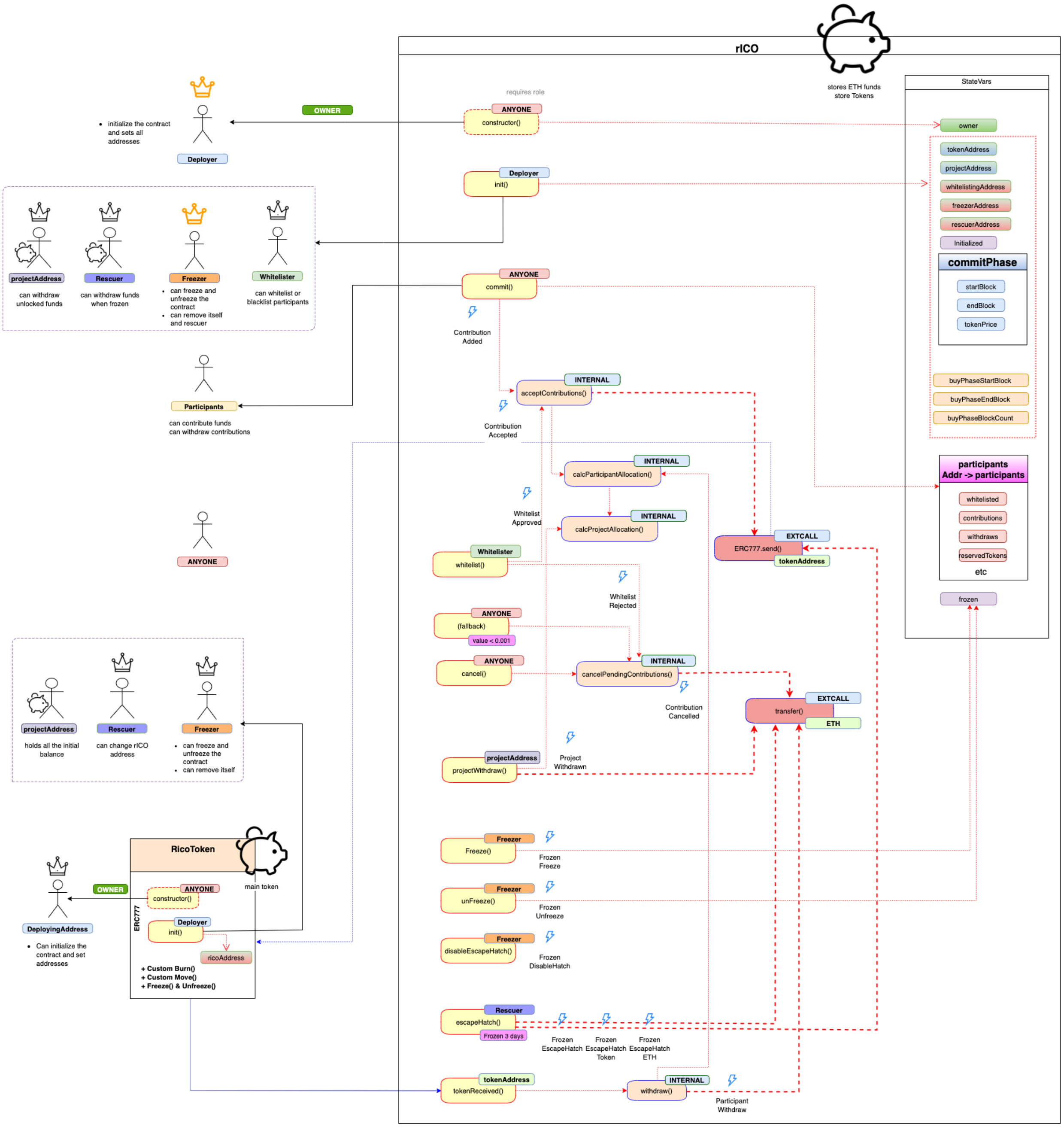
1. Ensure that the system is implemented consistently with the intended functionality, and without unintended edge cases, according to the specification derived from the documentation that was provided to us.
2. Identify known vulnerabilities particular to smart contract systems, as outlined in our Smart Contract Best Practices, and the Smart Contract Weakness Classification Registry.
3. The implementation of the mathematical relationships in the rICO smart contract corresponds to the specification in the documentation.
4. The flow of funds occurs as specified in the documentation. No undocumented flow of native or ERC20 tokens exists.

3 System Overview

The Reversible Initial Coin Offering, or rICO, for short, has two main contracts:

- ReversibleICO
  - Main functionality for swapping ETH with Token, and the other way around
- RicoToken
  - ERC777 with modified functions to consider the available unlocked balance in the rICO

Bellow you can see the visualization of the rICO system.



UPDATE: The above chart has been updated to reflect the new changes in the mitigation phase to the Token contract. However, it might lack some details, such as proper visualization of freezing functionality and the new roles.

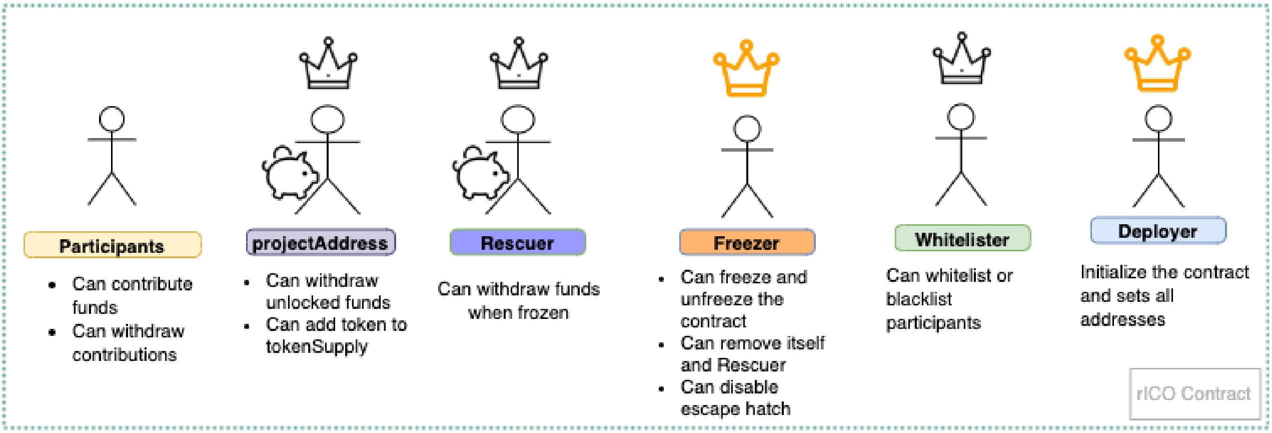
More details about the Actors and their permissions can be found in Actors.

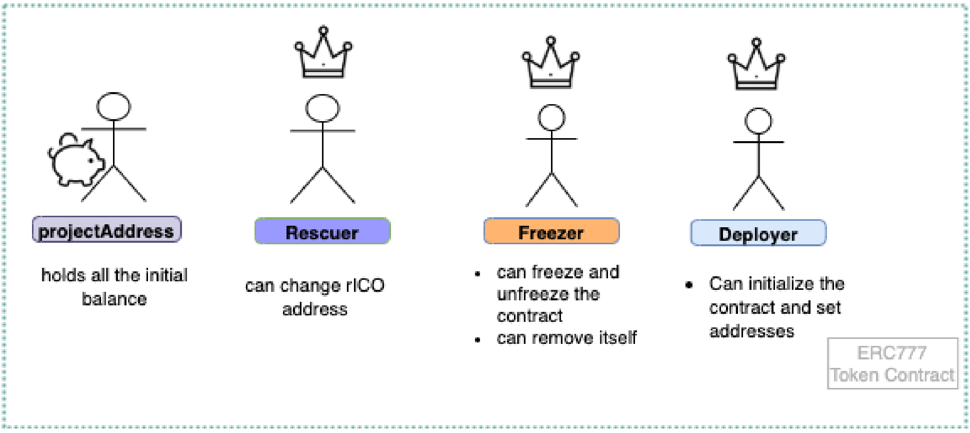
4 Security Specification

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.

4.1 Actors

The relevant actors are listed below with their respective abilities:


Participants
Can contribute funds
Can withdraw contributions
projectAddress
Can withdraw unlocked funds
Can add token to tokenSupply
Rescuer
Can withdraw funds when frozen
Freezer
Can freeze and unfreeze the contract
Can remove itself and Rescuer
Can disable escape hatch
Whitelister
Can whitelist or blacklist participants
Deployer
Initialize the contract and sets all addresses
rICO Contract


projectAddress
holds all the initial balance
Rescuer
can change rICO address
Freezer
can freeze and unfreeze the contract
can remove itself
Deployer
Can initialize the contract and set addresses
ERC777 Token Contract

rICO

- **deployingAddress** : Only this address is allowed to **set all other addresses and stage** details when initializing the rICO contract. after the initial setup the details of the rICO cannot be changed by any actor.

- **whitelistingAddress** : Only this address can **whitelist or blacklist participants** in the rICO.

- **freezerAddress**: Freezer address is designed for emergency scenarios, when the rICO must be frozen. This address can:

  - **Freeze the contract** to stop all functionalities in the contract, such as:
    - *Receiving Eth or Tokens*
    - *canceling* pending contributions
    - *accepting* pending contributions
    - withdrawing any tokens or contributions by either participants or project address

    - whitelisting addresses
  - **Unfreeze the contract** to resume all functionalities
    - As mentioned in issue 6.2 this results in extension to the rICO time frame
  - **Disable Escape hatch**: to remove *freezerAddress* and *rescuerAddress* from the system. This is design to be called when the smart contract is presumably secure. The smart contract cannot be frozen if this function is used.

- **rescuerAddress** : This address based on client discussion, will be held by a *trusted third party*, and only will be used in case of emergency. *After the contract has been frozen for 3 days *(18000 blocks), this address can **transfer all the funds and tokens** to the specified address.

- **Participant** : Any entity sending more than `minContribution` (0.001 ether) to the rICO smart contract, while the rICO is running, will be added as participants. The purchase of the committed tokens, however, depends if the participant is whitelisted or not.

  - Participants can also withdraw their contributions by returning the purchased tokens

- **projectAddress**: The project wallet

  - Can *withdraw ETH* contributions (Unlocked ETH)
  - *Add tokens to tokenSupply* of the rICO by sending tokens to rICO contract
  - Holds all the initial balance of the token

- **tokenAddress**: The address of the ERC777 token used in the rICO

  - ~~**manager**: is the address deploying the RicoToken (`LYXeToken`) contract.~~
  - **UPDATE:**: TokenManager has been removed and its permissions has been separated into the new roles, described below.

Token

- **deployingAddress** : Only this address is allowed to **set all other addresses** when initializing the token contract.

- **freezerAddress**: Freezer address is designed for emergency scenarios, when the token must be frozen. This address can:

  - **Freeze the contract** to stop all functionalities in the contract, such as:
    - *Burn Tokens*
    - *Move Tokens* All token transfers will be frozen
  - **Unfreeze the contract** to resume all functionalities
    - As mentioned in issue 6.2 this results in extension to the rICO time frame
  - **Remove Freezer Address**: to remove *freezerAddress* from the system. This is design to be called when the smart contract is presumably secure. The smart contract cannot be frozen if this function is used.

- **rescuerAddress** : This address based on client discussion, will be held by a *trusted third party*, and only will be used in case of emergency. This address can change the rICO address when the token is frozen. No grace period is implemented for this functionality.

Note: The addresses with the same name in rICO and Token contract can be different entities. However, as for Lukso rICO, it is assumed that they will be deployed and initialized for the same addresses.

4.2 Trust Model

In any smart contract system, it's important to identify what trust is expected/required between various actors. For this audit, we established the following trust model:

- **deployingAddress** is initially in full control of setting the actors in the system. However after the initialization, the deployer does not have any special access.
- **freezerAddress** has the most control over the rICO system, although no ability to withdraw or steal funds. freezerAddress can freeze and unfreeze the contract, resulting in total system halt or restore.
  - It should be noted that this entity can completely deny itself and **rescuerAddress** the opportunity to withdraw funds.
- **rescuerAddress** after the contract has been frozen for more than 3 days (18000 blocks), rescuerAddress can withdraw the funds and tokens to any address of choosing.
- Manager of the token (ERC777), can also freeze the underlying token.
- Due to ERC777 callbacks (e.g. tokenReceived) must be verified in order to consider the rICO to be safe to be used in DeFi.

4.3 Important Security Properties

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

Rico Token Flow

- During the commit and buy phases of the reversible ICO, locked tokens cannot be transferred by participants unless the receiver is the Reversible ICO contract address itself.
- With the exception of the privileged actors described above, no other actor should be able to withdraw ETH from the Reversible ICO contract.

ETH Flow

- No participant can withdraw other participant's committed ETH.
- With the exception of the privileged actors described above, no other actor should be able to withdraw ETH from the Reversible ICO contract.

Lockup Conditions

- No lockup conditions arise from incorrect usage of SafeMath.
  - *Note*: The obvious exception to this being the issue reported regarding the, incorrectly, unchecked subtraction of the frozen period, which the audit team expects to be resolved ASAP. (issue 6.4)
- No lockup condition arises from the incorrect calculation of a stage number.

Reentrancy Instances

- Both the reentrancy instances accessible by participants pose no problem to the correct functioning of the rICO. The only and obvious exception to this being the transfer of tokens present in the `escapeHatch()` method (this last one is called by a privileged actor that has the ability to drain the contract at any point in time as per the specification).

5 Recommendations

5.1 Sanity check for addresses

Even though the `init` function is called by the address deployer and possibly using scripts, it is recommended to have sanity checks inside the function to prevent some common mistakes, such as :

```
require(tokenAddress != address(0));
require(whitelistingAddress != address(0));
require(projectAddress != address(0));
require(freezerAddress != address(0));
require(rescuerAddress != address(0));
```

These checks can be extended to other security specifications such as to prevent *projectAddress* and *freezerAddress* to be the same, and so on.

Update: The proper checks were added in lukso-network/rICO-smart-contracts@ `edb880c` .

5.2 Separate currentBlock from currentEffectiveBlock

In rICO contract, the current block number is gotten from `getCurrentBlockNumber()` and the context it is used might mean different block numbers.

It is used to get *actual current block* in the following functions:

- `init()`
- The first time `freeze()` and `unfreeze()` are called

However, it is used to get the *effective block number* (currentBlock - frozenPeriod) in the following functions:

- `getCurrentStage()` (adds frozenPeriod for fixing the math)
- `getCurrentPrice()` (adds frozenPeriod for fixing the math)
- The second+ time `freeze()` and `unfreeze()` are called
- Other functions

The point is, even though, the mathematics behind the stages (e.g. multiple frozen periods) works out, it adds unnecessary complexity to the code and makes future updates and modifications tricky. It is suggested (similar to issue 6.3), to define two different functions, for example `getCurrentBlockNumber()` for actual current block number, and `getCurrentEffectiveBlockNumber()` for effective block number (deducting `frozenPeriod`).

UPDATE: The new function `getCurrentEffectiveBlockNumber()` was added in lukso-network/rICO-smart-contracts@ `e4c9ed5` .

5.3 Shadowed variable `stages`

In the `acceptContributions()` a variable is defined as `stages` that shadows a global variable with the same name. It is verified that within the scope of this function, there are no issues with this shadowing, however it might result in confusion or possible bugs in future updates. It is suggested to use a new name for the variable to prevent shadowing global variables.

```
mapping(uint8 => Stage) public stages;
```

```
ParticipantStageDetails storage stages = participantStats.stages[stageId];
```

UPDATE: The shadowed variable was renamed to `byStage` in lukso-network/rICO-smart-contracts@ `e4c9ed5` .

5.4 Limit the length of the stages

Currently there are no limits in how many stages can there be in a given rICO instance. Given that any participant can contribute in every stage, and there are many functions that iterate through the stages each participant has contributed in (e.g. `cancelPendingContributions()` and `acceptContributions()`), there must be an upper limit to the number of stages before it reaches the gasBlockLimit. It is recommended to calculate and add such a limit to `init()` function.

UPDATE: This limitation has been acknowledged by Lukso team. The number of stages are limited for Lukso rICO, however for future reference a note was added to the README file and an inline comment (in lukso-network/rICO-smart-contracts@ `e4c9ed5`) as a warning for future deployemnets.

```
**NOTE** Its not recommended to choose more than 50 stages!
9 stages require ~650k GAS when whitelisting contributions,
the whitelisting function could run out of gas with a high number of stages,
preventing accepting contributions.

Test before using the `/test/solc_tests/flows/random_tests.js`
```

5.5 Usage of variables under 32 bytes in size

Variable types smaller than 32 bytes in size are almost always (and also counterintuitively!) more gas intensive than 32-bytes-sized ones.

The audit team therefore recommends the sole use of 32-byte-sized variables (i.e. uint256) except in the situations where these can be tightly packed, like in the `Participant` or `Stage` struct, illustrated below.

```
//ReversibleICO.sol#L139-L140
    struct Stage {
        uint128 startBlock;
        uint128 endBlock;
        uint256 tokenPrice;
    }
```

6 Issues

Each issue has an assigned severity:

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

6.1 Test code present in the code base Medium ✓ Fixed

Resolution

Fixed in lukso-network/rICO-smart-contracts@ `edb880c` .

Description

Test code are present in the code base. This is mainly a reminder to fix those before production.

Examples

`rescuerAddress` and `freezerAddress` are not even in the function arguments.

code/contracts/ReversibleICO.sol:L243-L247

```
whitelistingAddress = _whitelistingAddress;
projectAddress = _projectAddress;
freezerAddress = _projectAddress; // TODO change, here only for testing
rescuerAddress = _projectAddress; // TODO change, here only for testing
```

Recommendation

Make sure all the variable assignments are ready for production before deployment to production.

6.2 `FreezerAddress` has more power than required Medium Acknowledged

Resolution

This issue is acknowledged by the client and the behaviour has been documented in security measurements.

Description

FreezerAddress is designed to have the ability of freezing the contract in case of emergency. However, indirectly, there are other changes in the system that can result from the freeze.

Examples

1. FreezerAddress can extend the rICO time frame. Given that the `frozenPeriod` is deducted from the blockNumber in stage calculations, the `buyPhaseEndBlock` is technically equals to `buyPhaseEndBlock + frozenPeriod`
2. FreezerAddress can call `disableEscapeHatch()`, which disables the escape hatch and rendering `RescuerAddress` useless.

Recommendation

If these behaviors are intentional they should be well documented and specified. If not, they should be removed.

In the case they are, indeed, intentional the audit team believes that, for *Example 1.*, there should be some event fired to serve as notification for the participants (possibly followed by off-chain infrastructure to warn them through email or other communication channel).

6.3 `frozenPeriod` is subtracted twice for calculating the current price

Medium **✓ Fixed**

Resolution

Found in parallel to the audit team and has been mitigated in lukso-network/rICO-smart-contracts@`ebc4bce`. The issue was further simplified by adding `getCurrentEffectiveBlockNumber()` in lukso-network/rICO-smart-contracts@`e4c9ed5` to remove ambiguity when calculating current block number.

Description

If the contract had been frozen, the current stage price will calculate the price by subtracting the `frozenPeriod` twice and result in wrong calculation.

`getCurrentBlockNumber()` subtracts `frozenPeriod` once, and then `getStageAtBlock()` will also subtract the same number again.

Examples

code/contracts/ReversibleICO.sol:L617-L619

```
function getCurrentStage() public view returns (uint8) {
    return getStageAtBlock(getCurrentBlockNumber());
}
```

code/contracts/ReversibleICO.sol:L711-L714

```
function getCurrentBlockNumber() public view returns (uint256) {
    return uint256(block.number)
    .sub(frozenPeriod); // make sure we deduct any frozenPeriod from calculations
}
```

code/contracts/ReversibleICO.sol:L654-L656

```
function getStageAtBlock(uint256 _blockNumber) public view returns (uint8) {

    uint256 blockNumber = _blockNumber.sub(frozenPeriod); // adjust the block by the
frozen period
```

Recommendation

Make sure `frozenPeriod` calculation is done correctly. It could be solved by renaming `getCurrentBlockNumber()` to reflect the calculation done inside the function.

e.g. :

- `getCurrentBlockNumber()` : gets current block number
- `getCurrentEffectiveBlockNumber()` : calculates the effective block number deducting `frozenPeriod`

6.4 Lockup condition in `getStageAtBlock()` Minor ✓ Fixed

Resolution

Even though the freeze pattern does indeed create a lot of additional complexity to the protocol, the particular `require` mentioned in the issue corpus by the audit team was found to never be triggered in a harmful way by rICO's development team.

In the light of this new discovery, we are greatly reducing the severity of the issue to "Minor". The reason why it is still kept as an issue is that the implementation of the freezing mechanism could still be greatly improved as we saw in the presented fixes here:

lukso-network/rICO-smart-contracts@ `e4c9ed5`

The changes resulted in a much more resilient rICO implementation.

Description

Given that the contract has been frozen at least once, if the `frozenPeriod` is longer than the period before the freeze event (starting from `commitPhaseStartBlock` till the `freezeStart`), the following require in `getStageAtBlock()` will revert due to the fact that `blockNumber < commitPhaseStartBlock`:

```
uint256 blockNumber = _blockNumber.sub(frozenPeriod); // adjust the block by the
frozen period

require(blockNumber >= commitPhaseStartBlock && blockNumber <= buyPhaseEndBlock,
"Block outside of rICO period.");
```

Note that the issue here is also related to the way currentBlockNumber is calculated (See issue 6.3 and Separate currentBlock from currentEffectiveBlock.

`getCurrentStage()` is called for every accept or cancelation of contributions and this lockup can result in total system halt.

Recommendation

Given that in the `init` function, the following condition is checked:

```
require(_commitPhaseStartBlock > getCurrentBlockNumber(), "Start block cannot be set
in the past.");
```

The check in the `getStageAtBlock()` can be removed. However this is assuming that the correct calculation of the `currentEffectiveBlockNumber` is used.

6.5 emit events for significant state changes Minor ✓ Fixed

Resolution

This issue was discussed in the code walk through meeting and was fixed, by adding proper events to the code base in lukso-network/rICO-smart-contracts@ `77517a4`, before the end of the audit.

Description

Events are useful for UI changes and user notifications. The code base overall can use more use of events to update the UI and participants.

One of the most important aspects that must emit events, are when system state and functionality are changed. These functions require to emit events for better visibility to the participants:

- `freeze()`
- `unfreeze()`
- `disableEscapeHatch()`
- `escapeHatch()`

Recommendation

emit events when system state is changed.

Appendix 1 - Agent-based Tests

Agent-based testing of the platform based on a modified version of the pre-existing random tests produced by the development team was ran. The results were adapted into graphs constructed with d3.js and were used to validate both the implementation of the mathematical models being used and their implementations, and the presence of subtle and nuanced nefarious effects coming from the interactions in an environment with many non-rational actors.

Presented below is a summarized version of the full graph. Please find the full, interactive version here.

The data presented in the charts stems from a simulation with the following parameters:

- Total participants: **20**
- Blocks per day: **25**
- Number of days of the *Commit* stage: **3**
- Number of days of each *Buy Phase* stage: **5**
- Total number of stages (including the *Commit* stage): **10**
- Price of token in the *Commit* stage: **0.002 ETH**
- Price increment per stage: **0.0001 ETH**

The ***project*** address agent withdraws ETH as often as it cans and the ***whitelister*** agent whitelists and blacklists randomly.

The ***participant*** agents have a total random strategy within the domain of valid actions (i.e., *valid* in this context means a transaction that won't revert). There are also two flavors of the *commit ETH* action being randomized. Sending the full ETH balance or sending half of it.

The code was adapted from the, already well-constructed, random tests present in the rICO repository.

A second test, with a different strategy for participants, was ran and can be found here.

In this version, the participants can commit any amount of their available balance and not just half or all of it. The number of days per stage also changed from *5* to **3**.

Note: The chart is zoomable. If there are ratio problems with the *iframe* below, please refresh the page.

Document Change Log

Version	Date	Description
1.0	2020-04-27	Initial report
1.1	2020-05-09	Reflect fixes

Appendix 2 - Files in Scope

This audit covered the following files:

File	SHA-1 hash
contracts/ReversibleICO.sol	3d5bf2c18b1ffa10b50eaac4cc62eaf43a40b6c2
contracts/RicoToken.sol	7d500809f2d14e4ea728ae126d4711239dffc422

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 raw output of the MythX vulnerability scan:

```
/code/contracts/mocks/erc777mock.sol
  1:0  warning  A floating pragma is set  SWC-103

/code/contracts/mocks/emptyreceiver.sol
  9:0  warning  A floating pragma is set  SWC-103

/code/contracts/reversibleico.sol
    9:0   warning  A floating pragma is set                                      SWC-
103
  485:8   warning  Call with hardcoded gas amount                                SWC-
134
  712:23  warning  Potential use of a weak source of randomness "block.number"  SWC-
120
  848:12  warning  Local variable shadows a state variable                       SWC-
119
  869:8   warning  Call with hardcoded gas amount                                SWC-
134

/code/contracts/mocks/reversibleicomock.sol
  5:42  warning  A floating pragma is set                  SWC-103
  9:9   warning  The state variable visibility is not set  SWC-108

/code/contracts/mocks/reversibleicomock777.sol
   5:42  warning  A floating pragma is set                  SWC-103
  24:15  warning  Unused function parameter "operator"      SWC-131
  24:41  warning  Unused function parameter "from"          SWC-131
  24:63  warning  Unused function parameter "to"            SWC-131
  25:9   warning  Unused function parameter "amount"        SWC-131
  25:33  warning  Unused function parameter "userData"      SWC-131
  25:66  warning  Unused function parameter "operatorData"  SWC-131

/code/contracts/ricotoken.sol
  1:0  warning  A floating pragma is set  SWC-103
```

```
/code/contracts/mocks/safemathmock.sol
  1:0  warning  A floating pragma is set  SWC-103

✖ 18 problems (0 errors, 18 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:

```
contracts/Gnosis/CreateCall.sol
  23:9    error    Only use indent of 8 spaces.    indentation

contracts/Gnosis/GnosisSafe.sol
  427:4    warning    Line contains trailing whitespace         no-trailing-
whitespace
  480:2    error      Only use indent of 4 spaces.              indentation
  485:6    error      Only use indent of 8 spaces.              indentation
  489:4    warning    Provide an error message for require()    error-reason
  492:0    error      Only use indent of 4 spaces.              indentation
  497:2    error      Only use indent of 4 spaces.              indentation
  498:4    warning    Provide an error message for require()    error-reason
  503:0    error      Only use indent of 4 spaces.              indentation
  508:2    error      Only use indent of 4 spaces.              indentation
  509:4    warning    Provide an error message for require()    error-reason
  513:0    error      Only use indent of 4 spaces.              indentation
  518:2    error      Only use indent of 4 spaces.              indentation
  520:4    warning    Provide an error message for require()    error-reason
  523:0    error      Only use indent of 4 spaces.              indentation
  529:2    error      Only use indent of 4 spaces.              indentation
  530:4    warning    Provide an error message for require()    error-reason
  532:0    error      Only use indent of 4 spaces.              indentation
  739:1    warning    Line contains trailing whitespace         no-trailing-
whitespace

contracts/ReversibleICO.sol
  313:45    error      String literal must be quoted with double quotes.
quotes
  542:67    error      String literal must be quoted with double quotes.
quotes
  680:23    warning    There should be no whitespace or comments between argument and
the comma following it.    comma-whitespace
  681:10    error      Only use indent of 12 spaces.
indentation
  771:12    error      String literal must be quoted with double quotes.
quotes
```

```
  777:12    error      String literal must be quoted with double quotes.
quotes
  793:12    error      String literal must be quoted with double quotes.
quotes
  979:42    error      String literal must be quoted with double quotes.
quotes

contracts/mocks/ERC777Mock.sol
  3:7    error    "../zeppelin/token/ERC777/ERC777.sol": Import statements must use
double quotes only.    quotes

contracts/mocks/ERC777SenderRecipientMock.sol
  9:7      error      "../zeppelin/token/ERC777/ERC777.sol": Import statements must
use double quotes only.    quotes
  54:12    warning    Provide an error message for revert()
error-reason
  85:12    warning    Provide an error message for revert()
error-reason
  143:8    warning    Consider using 'transfer' in place of 'send'.
security/no-send

contracts/mocks/MathMock.sol
  3:7    error    "../zeppelin/math/Math.sol": Import statements must use double
quotes only.    quotes

contracts/mocks/ReversibleICOMock.sol
  11:7    error    "../ReversibleICO.sol": Import statements must use double quotes
only.    quotes

contracts/mocks/ReversibleICOMock777.sol
  11:7    error    "./ReversibleICOMock.sol": Import statements must use double
quotes only.    quotes

contracts/mocks/SafeMathMock.sol
  3:7    error    "../zeppelin/math/SafeMath.sol": Import statements must use double
quotes only.    quotes

contracts/zeppelin/crowdsale/Crowdsale.sol
  149:89    warning    Code contains empty block    no-empty-blocks
  179:85    warning    Code contains empty block    no-empty-blocks

contracts/zeppelin/crowdsale/distribution/FinalizableCrowdsale.sol
  48:38    warning    Code contains empty block    no-empty-blocks

contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol
  21:16    error    Only use indent of 12 spaces.    indentation

contracts/zeppelin/crowdsale/price/IncreasingPriceCrowdsale.sol
  64:30    warning    Avoid using 'block.timestamp'.    security/no-block-members

contracts/zeppelin/crowdsale/validation/TimedCrowdsale.sol
  38:31    warning    Avoid using 'block.timestamp'.    security/no-block-members
  65:15    warning    Avoid using 'block.timestamp'.    security/no-block-members
  65:50    warning    Avoid using 'block.timestamp'.    security/no-block-members
  74:15    warning    Avoid using 'block.timestamp'.    security/no-block-members

contracts/zeppelin/cryptography/ECDSA.sol
  42:8    error    Avoid using Inline Assembly.    security/no-inline-assembly

contracts/zeppelin/drafts/SignatureBouncer.sol
  46:28    warning    Code contains empty block    no-empty-blocks

contracts/zeppelin/drafts/TokenVesting.sol
  55:38     warning    Avoid using 'block.timestamp'.    security/no-block-members
  166:12    warning    Avoid using 'block.timestamp'.    security/no-block-members
  168:19    warning    Avoid using 'block.timestamp'.    security/no-block-members
  171:36    warning    Avoid using 'block.timestamp'.    security/no-block-members

contracts/zeppelin/introspection/ERC165Checker.sol
  102:8    error    Avoid using Inline Assembly.    security/no-inline-assembly

contracts/zeppelin/token/ERC20/SafeERC20.sol
  33:16    error      Only use indent of 12 spaces.             indentation
  67:65    warning    Avoid using low-level function 'call'.    security/no-low-
level-calls

contracts/zeppelin/token/ERC20/TokenTimelock.sol
  29:30    warning    Avoid using 'block.timestamp'.    security/no-block-members
  61:16    warning    Avoid using 'block.timestamp'.    security/no-block-members

contracts/zeppelin/token/ERC721/ERC721.sol
  91:16    error    Only use indent of 12 spaces.    indentation

contracts/zeppelin/token/ERC721/IERC721.sol
  27:1    warning    Line contains trailing whitespace    no-trailing-whitespace

contracts/zeppelin/token/ERC721/IERC721Full.sol
  11:68    warning    Code contains empty block    no-empty-blocks

contracts/zeppelin/token/ERC721/IERC721Receiver.sol
  24:0    error    Only use indent of 4 spaces.    indentation

contracts/zeppelin/token/ERC777/ERC777.sol
  44:0      error      Only use indent of 4 spaces.
indentation
  48:0      error      Only use indent of 4 spaces.
indentation
  471:12    warning    Error message exceeds max length of 76 characters    error-
reason

contracts/zeppelin/utils/Address.sol
  21:8    warning    Line contains trailing whitespace    no-trailing-whitespace
  28:8    error      Avoid using Inline Assembly.         security/no-inline-assembly
```

```
✖ 34 errors, 31 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 a complete list of functions with their visibility and modifiers:

Sūrya's Description Report

File Name	
contracts/Gnosis/CreateCall.sol	e33c0ec5bcbe
contracts/Gnosis/GnosisSafe.sol	af2dbf4f80b6
contracts/Migrations.sol	6eddef3c09c6
contracts/ReversibleICO.sol	b40a2464c0f
contracts/RicoToken.sol	7d500809f2d
contracts/mocks/ERC777Mock.sol	679dfee5742c
contracts/mocks/ERC777SenderRecipientMock.sol	990ec041972
contracts/mocks/EmptyReceiver.sol	f4f7155b6c24
contracts/mocks/MathMock.sol	147138b16a7e
contracts/mocks/ReversibleICOMock.sol	8e15fa7194b6
contracts/mocks/ReversibleICOMock777.sol	87c2bf80a0fd
contracts/mocks/SafeMathMock.sol	906a40c436b
contracts/zeppelin/access/Roles.sol	2c85acf184ae
contracts/zeppelin/access/roles/CapperRole.sol	c5b388b4165
contracts/zeppelin/access/roles/MinterRole.sol	81ba1a5f8f35
contracts/zeppelin/access/roles/PauserRole.sol	eac20163f361
contracts/zeppelin/access/roles/SignerRole.sol	0d6c043d90f
contracts/zeppelin/access/roles/WhitelistAdminRole.sol	db13ff3d51ba
contracts/zeppelin/access/roles/WhitelistedRole.sol	adf6a7f1fc136

File Name	
contracts/zeppelin/crowdsale/Crowdsale.sol	9b929f34f8c7
contracts/zeppelin/crowdsale/distribution/FinalizableCrowdsale.sol	d4edf528c6aa
contracts/zeppelin/crowdsale/distribution/PostDeliveryCrowdsale.sol	c2ea0fe336dd
contracts/zeppelin/crowdsale/distribution/RefundableCrowdsale.sol	34f79575607b
contracts/zeppelin/crowdsale/distribution/RefundablePostDeliveryCrowdsale.sol	a46bf27427e2
contracts/zeppelin/crowdsale/emission/AllowanceCrowdsale.sol	3eef5da8f505
contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol	6e9c7fae7f84
contracts/zeppelin/crowdsale/price/IncreasingPriceCrowdsale.sol	323bf9fee7e5
contracts/zeppelin/crowdsale/validation/CappedCrowdsale.sol	bac0582e3d1
contracts/zeppelin/crowdsale/validation/IndividuallyCappedCrowdsale.sol	1475fb9401a7
contracts/zeppelin/crowdsale/validation/PausableCrowdsale.sol	f363c66635ca
contracts/zeppelin/crowdsale/validation/TimedCrowdsale.sol	3348207385f
contracts/zeppelin/crowdsale/validation/WhitelistCrowdsale.sol	54e5b7619d2f
contracts/zeppelin/cryptography/ECDSA.sol	76a85bee5b5
contracts/zeppelin/cryptography/MerkleProof.sol	9cf3346b959
contracts/zeppelin/drafts/Counters.sol	9afb0abd3c2
contracts/zeppelin/drafts/ERC1046/ERC20Metadata.sol	90bd876180
contracts/zeppelin/drafts/ERC20Migrator.sol	7b276d54e8b
contracts/zeppelin/drafts/ERC20Snapshot.sol	2d87241a7d5
contracts/zeppelin/drafts/SignatureBouncer.sol	8688cb09130
contracts/zeppelin/drafts/SignedSafeMath.sol	cbb5a1dd1395
contracts/zeppelin/drafts/Strings.sol	191552acdf06
contracts/zeppelin/drafts/TokenVesting.sol	aae2625bcc10
contracts/zeppelin/examples/SampleCrowdsale.sol	8a9795357ba
contracts/zeppelin/examples/SimpleToken.sol	b7cac40dfc7f
contracts/zeppelin/introspection/ERC165.sol	0ffad990866
contracts/zeppelin/introspection/ERC165Checker.sol	70e4597cea01

File Name	
contracts/zeppelin/introspection/ERC1820Implementer.sol	ccdcb76ed593
contracts/zeppelin/introspection/IERC165.sol	3e4132a066a6
contracts/zeppelin/introspection/IERC1820Implementer.sol	f5ed2d06bcd8
contracts/zeppelin/introspection/IERC1820Registry.sol	7043ec16917c
contracts/zeppelin/lifecycle/Pausable.sol	b0fa9243a286
contracts/zeppelin/math/Math.sol	ab515a94d34
contracts/zeppelin/math/SafeMath.sol	996fa9bc77d3
contracts/zeppelin/ownership/Ownable.sol	52faef44a799
contracts/zeppelin/ownership/Secondary.sol	effa2a1d4e5b8
contracts/zeppelin/payment/PaymentSplitter.sol	cd09d63330e
contracts/zeppelin/payment/PullPayment.sol	6de15ad8c8a8
contracts/zeppelin/payment/escrow/ConditionalEscrow.sol	741bc063096
contracts/zeppelin/payment/escrow/Escrow.sol	89814623bf0
contracts/zeppelin/payment/escrow/RefundEscrow.sol	f356bb993dc1
contracts/zeppelin/token/ERC20/ERC20.sol	090e794a02c
contracts/zeppelin/token/ERC20/ERC20Burnable.sol	53604981ed2
contracts/zeppelin/token/ERC20/ERC20Capped.sol	bec55d19afae
contracts/zeppelin/token/ERC20/ERC20Detailed.sol	e87b9ea40a0
contracts/zeppelin/token/ERC20/ERC20Mintable.sol	9702a8bc622
contracts/zeppelin/token/ERC20/ERC20Pausable.sol	9c2bdb2452c
contracts/zeppelin/token/ERC20/IERC20.sol	071386690ad
contracts/zeppelin/token/ERC20/SafeERC20.sol	638ff9747c02
contracts/zeppelin/token/ERC20/TokenTimelock.sol	56ff72e3930b
contracts/zeppelin/token/ERC721/ERC721.sol	14a1fd7b8f9a
contracts/zeppelin/token/ERC721/ERC721Burnable.sol	18e971a658a4
contracts/zeppelin/token/ERC721/ERC721Enumerable.sol	5d56a89a03a
contracts/zeppelin/token/ERC721/ERC721Full.sol	004e3919a168

File Name	
contracts/zeppelin/token/ERC721/ERC721Holder.sol	9ae70830aa2
contracts/zeppelin/token/ERC721/ERC721Metadata.sol	f15e429094d7
contracts/zeppelin/token/ERC721/ERC721MetadataMintable.sol	d79b2f03279
contracts/zeppelin/token/ERC721/ERC721Mintable.sol	3e7f86143285
contracts/zeppelin/token/ERC721/ERC721Pausable.sol	5781706f3e6
contracts/zeppelin/token/ERC721/IERC721.sol	a031de37de0
contracts/zeppelin/token/ERC721/IERC721Enumerable.sol	d68cee9914f8
contracts/zeppelin/token/ERC721/IERC721Full.sol	d383b8f1941
contracts/zeppelin/token/ERC721/IERC721Metadata.sol	8be425d35ab
contracts/zeppelin/token/ERC721/IERC721Receiver.sol	259fda3fb13a
contracts/zeppelin/token/ERC777/ERC777.sol	4f6d1ba8747
contracts/zeppelin/token/ERC777/IERC777.sol	31e168dfd70
contracts/zeppelin/token/ERC777/IERC777Recipient.sol	e5cc170671b1
contracts/zeppelin/token/ERC777/IERC777Sender.sol	05af02d35e3
contracts/zeppelin/utils/Address.sol	5e025b5b324
contracts/zeppelin/utils/Arrays.sol	3487917d053
contracts/zeppelin/utils/ReentrancyGuard.sol	b419b7ac132

Contract	Type	
└	**Function Name**	
CreateCall	Implementation	
└	performCreate2	
└	performCreate	
Executor	Implementation	
└	execute	
└	executeCall	
└	executeDelegateCall	

Contract	Type	
Enum	Implementation	
SecuredTokenTransfer	Implementation	
└	transferToken	
SelfAuthorized	Implementation	
FallbackManager	Implementation	
└	internalSetFallbackHandler	
└	setFallbackHandler	
└		
ModuleManager	Implementation	Self
└	setupModules	
└	enableModule	
└	disableModule	
└	execTransactionFromModule	
└	getModules	
OwnerManager	Implementation	
└	setupOwners	
└	addOwnerWithThreshold	
└	removeOwner	
└	swapOwner	
└	changeThreshold	
└	getThreshold	
└	isOwner	
└	getOwners	
MasterCopy	Implementation	
└	changeMasterCopy	

Contract	Type	
Module	Implementation	
└	setManager	
SignatureDecoder	Implementation	
└	recoverKey	
└	signatureSplit	
SafeMath	Library	
└	mul	
└	div	
└	sub	
└	add	
└	mod	
ISignatureValidatorConstants	Implementation	
GnosisSafe	Implementation	Master S Sec ISigna
└	setup	
└	execTransaction	
└	handlePayment	
└	checkSignatures	
└	requiredTxGas	
└	approveHash	
└	signMessage	
└	isValidSignature	
└	getMessageHash	

Contract	Type	
└	encodeTransactionData	
└	getTransactionHash	
ISignatureValidator	Implementation	ISigna
└	isValidSignature	
Migrations	Implementation	
ReversibleICO	Implementation	I
└		
└	init	
└		
└	tokensReceived	
└	commit	
└	cancel	
└	whitelist	
└	projectWithdraw	
└	freeze	
└	unfreeze	
└	disableEscapeHatch	
└	escapeHatch	
└	getUnlockedProjectETH	
└	getAvailableProjectETH	

Contract	Type	
└	getParticipantReservedTokens	
└	getParticipantUnlockedTokens	
└	getCurrentStage	
└	getCurrentPrice	
└	getPriceAtBlock	
└	getPriceAtStage	
└	getStageAtBlock	
└	committableEthAtStage	
└	getTokenAmountForEthAtStage	
└	getEthAmountForTokensAtStage	
└	getCurrentBlockNumber	
└	calcUnlockedAmount	
└	sanityCheckProject	
└	sanityCheckParticipant	
└	calcProjectAllocation	
└	calcParticipantAllocation	
└	cancelPendingContributions	
└	acceptContributions	
└	withdraw	
ReversibleICO	Interface	
└	getParticipantReservedTokens	
RicoToken	Implementation	
└		
└	setup	

Contract	Type	
└	changeManager	
└	setFrozen	
└	getLockedBalance	
└	getUnlockedBalance	
└	_burn	
└	_move	
ERC777Mock	Implementation	
└		
└	mintInternal	
ERC777SenderRecipientMock	Implementation	I EF
└	tokensToSend	
└	tokensReceived	
└	senderFor	
└	registerSender	
└	recipientFor	
└	registerRecipient	
└	setShouldRevertSend	
└	setShouldRevertReceive	
└	send	
└	burn	
EmptyReceiver	Implementation	
MathMock	Implementation	
└	max	

Contract	Type	
└	min	
└	average	
ReversibleICOMock	Implementation	
└	getCurrentBlockNumber	
└	increaseCurrentBlockNumber	
└	jumpToBlockNumber	
ReversibleICOMock777	Implementation	R
└	setreservedTokenAmount	
└	getParticipantReservedTokens	
└	tokensReceived	
SafeMathMock	Implementation	
└	mul	
└	div	
└	sub	
└	add	
└	mod	
Roles	Library	
└	add	
└	remove	
└	has	
CapperRole	Implementation	
└		
└	isCapper	
└	addCapper	
└	renounceCapper	

Contract	Type	
└	_addCapper	
└	_removeCapper	
MinterRole	Implementation	
└		
└	isMinter	
└	addMinter	
└	renounceMinter	
└	_addMinter	
└	_removeMinter	
PauserRole	Implementation	
└		
└	isPauser	
└	addPauser	
└	renouncePauser	
└	_addPauser	
└	_removePauser	
SignerRole	Implementation	
└		
└	isSigner	
└	addSigner	
└	renounceSigner	
└	_addSigner	
└	_removeSigner	
WhitelistAdminRole	Implementation	
└		

Contract	Type	
└	isWhitelistAdmin	
└	addWhitelistAdmin	
└	renounceWhitelistAdmin	
└	_addWhitelistAdmin	
└	_removeWhitelistAdmin	
WhitelistedRole	Implementation	W
└	isParticipantWhitelisted	
└	addWhitelisted	
└	removeWhitelisted	
└	renounceWhitelisted	
└	_addWhitelisted	
└	_removeWhitelisted	
Crowdsale	Implementation	
└		
└		
└	token	
└	wallet	
└	rate	
└	weiRaised	
└	buyTokens	
└	_preValidatePurchase	
└	_postValidatePurchase	
└	_deliverTokens	
└	_processPurchase	
└	_updatePurchasingState	
└	_getTokenAmount	

Contract	Type	
└	_forwardFunds	
FinalizableCrowdsale	Implementation	
└		
└	finalized	
└	finalize	
└	_finalization	
PostDeliveryCrowdsale	Implementation	
└		
└	withdrawTokens	
└	balanceOf	
└	_processPurchase	
unstableTokenVault	Implementation	
└	transfer	
RefundableCrowdsale	Implementation	Fi
└		
└	goal	
└	claimRefund	
└	goalReached	
└	_finalization	
└	_forwardFunds	
RefundablePostDeliveryCrowdsale	Implementation	Re Po
└	withdrawTokens	
AllowanceCrowdsale	Implementation	
└		

Contract	Type	
└	tokenWallet	
└	remainingTokens	
└	_deliverTokens	
MintedCrowdsale	Implementation	
└	_deliverTokens	
IncreasingPriceCrowdsale	Implementation	
└		
└	rate	
└	initialRate	
└	finalRate	
└	getCurrentRate	
└	_getTokenAmount	
CappedCrowdsale	Implementation	
└		
└	cap	
└	capReached	
└	_preValidatePurchase	
IndividuallyCappedCrowdsale	Implementation	Cro
└	setCap	
└	getCap	
└	getContribution	
└	_preValidatePurchase	
└	_updatePurchasingState	
PausableCrowdsale	Implementation	C
└	_preValidatePurchase	

Contract	Type	
TimedCrowdsale	Implementation	
└		
└	openingTime	
└	closingTime	
└	isOpen	
└	hasClosed	
└	_preValidatePurchase	
└	_extendTime	
WhitelistCrowdsale	Implementation	Whit
└	_preValidatePurchase	
ECDSA	Library	
└	recover	
└	toEthSignedMessageHash	
MerkleProof	Library	
└	verify	
Counters	Library	
└	current	
└	increment	
└	decrement	
ERC20Metadata	Implementation	
└		
└	tokenURI	
└	_setTokenURI	
ERC20Migrator	Implementation	
└		

Contract	Type
└	legacyToken
└	newToken
└	beginMigration
└	migrate
└	migrateAll
ERC20Snapshot	Implementation
└	snapshot
└	balanceOfAt
└	totalSupplyAt
└	_transfer
└	_mint
└	_burn
└	_valueAt
└	_updateAccountSnapshot
└	_updateTotalSupplySnapshot
└	_updateSnapshot
└	_lastSnapshotId
SignatureBouncer	Implementation
└	
└	_isValidSignature
└	_isValidSignatureAndMethod
└	_isValidSignatureAndData
└	_isValidDataHash
SignedSafeMath	Library
└	mul
└	div

Contract	Type	
└	sub	
└	add	
Strings	Library	
└	fromUint256	
TokenVesting	Implementation	
└		
└	beneficiary	
└	cliff	
└	start	
└	duration	
└	revocable	
└	released	
└	revoked	
└	release	
└	revoke	
└	_releasableAmount	
└	_vestedAmount	
SampleCrowdsaleToken	Implementation	
└		
SampleCrowdsale	Implementation	(Re
└		

Contract	Type	
SimpleToken	Implementation	ER
└		
ERC165	Implementation	
└		
└	supportsInterface	
└	_registerInterface	
ERC165Checker	Library	
└	_supportsERC165	
└	_supportsInterface	
└	_supportsAllInterfaces	
└	_supportsERC165Interface	
└	_callERC165SupportsInterface	
ERC1820Implementer	Implementation	IEI
└	canImplementInterfaceForAddress	
└	_registerInterfaceForAddress	
IERC165	Interface	
└	supportsInterface	
IERC1820Implementer	Interface	
└	canImplementInterfaceForAddress	
IERC1820Registry	Interface	
└	setManager	
└	getManager	
└	setInterfaceImplementer	
└	getInterfaceImplementer	
└	interfaceHash	

Contract	Type	
└	updateERC165Cache	
└	implementsERC165Interface	
└	implementsERC165InterfaceNoCache	
Pausable	Implementation	
└		
└	paused	
└	pause	
└	unpause	
Math	Library	
└	max	
└	min	
└	average	
SafeMath	Library	
└	add	
└	sub	
└	mul	
└	div	
└	mod	
Ownable	Implementation	
└		
└	owner	
└	isOwner	
└	renounceOwnership	
└	transferOwnership	
└	_transferOwnership	

Contract	Type
Secondary	Implementation
└	
└	primary
└	transferPrimary
PaymentSplitter	Implementation
└	
└	
└	totalShares
└	totalReleased
└	shares
└	released
└	payee
└	release
└	_addPayee
PullPayment	Implementation
└	
└	withdrawPayments
└	payments
└	_asyncTransfer
ConditionalEscrow	Implementation
└	withdrawalAllowed
└	withdraw
Escrow	Implementation
└	depositsOf
└	deposit

Contract	Type	
└	withdraw	
RefundEscrow	Implementation	C
└		
└	state	
└	beneficiary	
└	deposit	
└	close	
└	enableRefunds	
└	beneficiaryWithdraw	
└	withdrawalAllowed	
ERC20	Implementation	
└	totalSupply	
└	balanceOf	
└	transfer	
└	allowance	
└	approve	
└	transferFrom	
└	increaseAllowance	
└	decreaseAllowance	
└	_transfer	
└	_mint	
└	_burn	
└	_approve	
└	_burnFrom	
ERC20Burnable	Implementation	
└	burn	

Contract	Type	
└	burnFrom	
ERC20Capped	Implementation	
└		
└	cap	
└	_mint	
ERC20Detailed	Implementation	
└		
└	name	
└	symbol	
└	decimals	
ERC20Mintable	Implementation	E
└	mint	
ERC20Pausable	Implementation	
└	transfer	
└	transferFrom	
└	approve	
└	increaseAllowance	
└	decreaseAllowance	
IERC20	Interface	
└	totalSupply	
└	balanceOf	
└	transfer	
└	allowance	
└	approve	
└	transferFrom	

Contract	Type	
SafeERC20	Library	
└	safeTransfer	
└	safeTransferFrom	
└	safeApprove	
└	safeIncreaseAllowance	
└	safeDecreaseAllowance	
└	callOptionalReturn	
TokenTimelock	Implementation	
└		
└	token	
└	beneficiary	
└	releaseTime	
└	release	
ERC721	Implementation	
└		
└	balanceOf	
└	ownerOf	
└	approve	
└	getApproved	
└	setApprovalForAll	
└	isApprovedForAll	
└	transferFrom	
└	safeTransferFrom	
└	safeTransferFrom	
└	_exists	
└	_isApprovedOrOwner	

Contract	Type	
└	_mint	
└	_burn	
└	_burn	
└	_transferFrom	
└	_checkOnERC721Received	
└	_clearApproval	
ERC721Burnable	Implementation	
└	burn	
ERC721Enumerable	Implementation	II
└		
└	tokenOfOwnerByIndex	
└	totalSupply	
└	tokenByIndex	
└	_transferFrom	
└	_mint	
└	_burn	
└	_tokensOfOwner	
└	_addTokenToOwnerEnumeration	
└	_addTokenToAllTokensEnumeration	
└	_removeTokenFromOwnerEnumeration	
└	_removeTokenFromAllTokensEnumeration	
ERC721Full	Implementation	ERC72
└		
ERC721Holder	Implementation	

Contract	Type	
└	onERC721Received	
ERC721Metadata	Implementation	
└		
└	name	
└	symbol	
└	tokenURI	
└	_setTokenURI	
└	_burn	
ERC721MetadataMintable	Implementation	ERC
└	mintWithTokenURI	
ERC721Mintable	Implementation	E
└	mint	
ERC721Pausable	Implementation	
└	approve	
└	setApprovalForAll	
└	transferFrom	
IERC721	Implementation	
└	balanceOf	
└	ownerOf	
└	safeTransferFrom	
└	transferFrom	
└	approve	
└	getApproved	
└	setApprovalForAll	

Contract	Type	
└	isApprovedForAll	
└	safeTransferFrom	
IERC721Enumerable	Implementation	
└	totalSupply	
└	tokenOfOwnerByIndex	
└	tokenByIndex	
IERC721Full	Implementation	IE
IERC721Metadata	Implementation	
└	name	
└	symbol	
└	tokenURI	
IERC721Receiver	Implementation	
└	onERC721Received	
ERC777	Implementation	
└		
└	name	
└	symbol	
└	decimals	
└	granularity	
└	totalSupply	
└	balanceOf	
└	send	
└	transfer	
└	burn	

Contract	Type	
└	isOperatorFor	
└	authorizeOperator	
└	revokeOperator	
└	defaultOperators	
└	operatorSend	
└	operatorBurn	
└	allowance	
└	approve	
└	transferFrom	
└	_mint	
└	_send	
└	_burn	
└	_move	
└	_approve	
└	_callTokensToSend	
└	_callTokensReceived	
IERC777	Interface	
└	name	
└	symbol	
└	granularity	
└	totalSupply	
└	balanceOf	
└	send	
└	burn	
└	isOperatorFor	
└	authorizeOperator	

Contract	Type
└	revokeOperator
└	defaultOperators
└	operatorSend
└	operatorBurn
IERC777Recipient	Interface
└	tokensReceived
IERC777Sender	Interface
└	tokensToSend
Address	Library
└	isContract
└	toPayable
Arrays	Library
└	findUpperBound
ReentrancyGuard	Implementation
└	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

A.3.4 Tests Suite

Below is the output generated by running the test suite:

```
> ricopoc@0.0.1 test /Users/gnsps/lukso-rico-audit-2020-04/code
> npm run test-validator && npm run test-solc
> ricopoc@0.0.1 test-validator /Users/gnsps/lukso-rico-audit-2020-04/code
> scripts/run_js.sh all refresh js

Connection to localhost port 8545 [tcp/*] succeeded!
Killing existing ganache-cli instance at port 8545
Starting new ganache-cli instance at port 8545
exchange neither monster ethics bless cancel ghost excite business record warfare
invite

-------------------------------------------------------------------
 Running all tests in "test/js_validator_tests" folder:
-------------------------------------------------------------------
You can improve web3's peformance when running Node.js versions older than 10.5.0 by
installing the (deprecated) scrypt package in your project
  ---------------------------------------------------------------
  Step 1 - Setting up helpers and globals
  ---------------------------------------------------------------
  ---------------------------------------------------------------
  Step 2 - Run tests
  ---------------------------------------------------------------


  Javascript Validator - Tests
    Integrity checking
      Settings are assigned correctly
        ✓ commitPhaseStartBlock is correct
        ✓ commitPhaseBlockCount is correct
        ✓ commitPhaseEndBlock is correct
        ✓ buyPhaseStartBlock is correct
        ✓ buyPhaseEndBlock is correct
        ✓ buyPhaseBlockCount is correct
        ✓ blocksPerDay is correct
        ✓ commitPhaseDays is correct
        ✓ stageDays is correct
        ✓ commitPhasePrice is 0.002
        ✓ stagePriceIncrease is 0.0001
      getCurrentBlockNumber()
        ✓ returns default block correctly
      setBlockNumber()
        ✓ sets block correctly
    Initialization
      stage generation
        ✓ stageCount is correct
        ✓ pricing increases by 10% for each stage
    Stage Methods
      getStageAtBlock(_blockNumber)
        stage 0
          ✓ should return correct stageId using startBlock
          ✓ should return correct stageId using endBlock
        stage 1
          ✓ should return correct stageId using startBlock
          ✓ should return correct stageId using endBlock
        stage 6
          ✓ should return correct stageId using startBlock
          ✓ should return correct stageId using endBlock
        last stage
          ✓ should return correct stageId using startBlock
          ✓ should return correct stageId using endBlock
        1 block before 0
          ✓ should throw "Block outside of rICO period."
        1 block after last stage
          ✓ should throw "Block outside of rICO period."
    Price Methods
      getPriceAtBlock(_blockNumber)
        edge of commit and buy block range
          before commitPhaseStartBlock
            ✓ should throw "Block outside of rICO period."
          at commitPhaseStartBlock
            ✓ should return commitPhasePrice
          at buyPhaseEndBlock
            ✓ should return commitPhasePrice
          after buyPhaseEndBlock
            ✓ should throw "Block outside of rICO period."
        first stage
          startBlock
            ✓ should return commitPhasePrice
          endBlock
            ✓ should return commitPhasePrice
          StartBlock price and EndBlock price
            ✓ should be higher than 0 and match
        stage 6
          startBlock
            ✓ should return stage tokenPrice
          endBlock
            ✓ should return stage tokenPrice
          StartBlock price and EndBlock price
            ✓ should be higher than 0 and match
        last stage
          startBlock
            ✓ should return stage tokenPrice
          endBlock
            ✓ should return stage tokenPrice
          StartBlock price and EndBlock price
            ✓ should be higher than 0 and match
      getTokenAmountForEthAtStage()
        1 eth
          stage 0
            ✓ should return 500 tokens
          stage 1
            ✓ should return 476.190476190476190476 tokens
          stage 6
            ✓ should return 384.615384615384615384 tokens
          last stage
            ✓ should return 312.5 tokens
      getEthAmountForTokensAtStage()
        1 eth worth of tokens
          stage 0
            ✓ should return 1 eth
          stage 1
            ✓ should return 1 eth minus 1 wei
          stage 6
            ✓ should return 1 eth minus 1 wei
          last stage
            ✓ should return 1 eth
      getUnlockPercentage(_currentBlock, _startBlock, _endBlock, precisionPow)
        precisionPow = 2 ( 10 ** 2 => 100 )
          _currentBlock in range
            _currentBlock = 1, _startBlock = 1, _endBlock = 100
              ✓ should return 0.01
            _currentBlock = 101, _startBlock = 101, _endBlock = 200
              ✓ should return 0.01
            _currentBlock = 2, _startBlock = 1, _endBlock = 100
              ✓ should return 0.02
            _currentBlock = 102, _startBlock = 101, _endBlock = 200
              ✓ should return 0.02
            _currentBlock = 50, _startBlock = 1, _endBlock = 100
              ✓ should return 0.5
            _currentBlock = 100, _startBlock = 1, _endBlock = 100
              ✓ should return 1
          _currentBlock ouside range
            before range => _currentBlock = 0, _startBlock = 1, _endBlock = 100
              ✓ should return 0
            after range => _currentBlock = 101, _startBlock = 1, _endBlock = 100
              ✓ should return 1
        precisionPow = 20 ( 10 ** 20 => 100000000000000000000 )
          _currentBlock in range
            _currentBlock = 1, _startBlock = 1, _endBlock = 100
              ✓ should return 0.01
            _currentBlock = 101, _startBlock = 101, _endBlock = 200
              ✓ should return 0.01
            _currentBlock = 2, _startBlock = 1, _endBlock = 100
              ✓ should return 0.02
            _currentBlock = 102, _startBlock = 101, _endBlock = 200
              ✓ should return 0.02
            _currentBlock = 50, _startBlock = 1, _endBlock = 100
              ✓ should return 0.5
            _currentBlock = 100, _startBlock = 1, _endBlock = 100
              ✓ should return 1
          _currentBlock ouside range
            before range => _currentBlock = 0, _startBlock = 1, _endBlock = 100
              ✓ should return 0
            after range => _currentBlock = 101, _startBlock = 1, _endBlock = 100
              ✓ should return 1
      getParticipantReservedTokensAtBlock(_tokenAmount, _blockNumber, precisionPow)
        _blockNumber in range
```

```
          _tokenAmount = 100, _blockNumber = startBlock
            ✓ should return 99
          _tokenAmount = 100, _blockNumber = (range * 0.25) - 1
            ✓ should return 75
          _tokenAmount = 100, _blockNumber = (range * 0.50) - 1 ( middle of the range
)
            ✓ should return 50
          _tokenAmount = 100, _blockNumber = (range * 0.75) - 1
            ✓ should return 25
          _tokenAmount = 100, _blockNumber = endBlock
            ✓ should return 0
        _blockNumber outside range
          block before buyPhaseStartBlock
            ✓ should return full amount
          block after buyPhaseEndBlock
            ✓ should return 0
      getUnockedTokensForBoughtAmountAtBlock(_tokenAmount, _blockNumber,
precisionPow)
        _blockNumber in range
          _tokenAmount = 100, _blockNumber = startBlock
            ✓ should return 1
          _tokenAmount = 100, _blockNumber = (range * 0.25) - 1
            ✓ should return 25
          _tokenAmount = 100, _blockNumber = (range * 0.50) - 1 ( middle of the range
)
            ✓ should return 50
          _tokenAmount = 100, _blockNumber = (range * 0.75) - 1
            ✓ should return 75
          _tokenAmount = 100, _blockNumber = endBlock
            ✓ should return 100
        _blockNumber outside range
          block before buyPhaseStartBlock
            ✓ should return 0
          block after buyPhaseEndBlock
            ✓ should return full amount

  Javascript Validator - Tests
    Stage initialisation
      Settings:
       startBlock:       100
       startBlockDelay:  10
       blocksPerDay:     10
       commitPhaseDays:  10
       stageCount:       12
       stageDays:        10
      Stage[0]
        ✓ stage[0] startBlock is 110
        ✓ stage[0] duration is 99 ( endBlock - startBlock )
        ✓ stage[0] endBlock is 209 ( startBlock=110 + duration ) => 209
        ✓ stage[0] stagePriceIncrease is correct
      Stage[1]
        ✓ stage[1] startBlock is 210
        ✓ stage[1] duration is 99 ( endBlock - startBlock )
        ✓ stage[1] endBlock is 309 ( startBlock=110 + duration ) => 309
        ✓ stage[1] stagePriceIncrease is correct
      Stage[12]
        ✓ stage[12] startBlock is 1310
        ✓ stage[12] duration is 99 ( endBlock - startBlock )
        ✓ stage[12] endBlock is 1409 ( startBlock=110 + duration ) => 1409
        ✓ stage[12] stagePriceIncrease is correct
    Stage Methods
      ✓ stage count matches for both test instances
      getStageAtBlock(_blockNumber)
        stage 0
          ✓ should return 0 when called using using stage[0].startBlock
          ✓ should return 0 when called using using stage[0].endBlock
        stage 1
          ✓ should return 1 when called using using stage[1].startBlock
          ✓ should return 1 when called using using stage[1].endBlock
        stage 6
          ✓ should return 6 when called using using stage[6].startBlock
          ✓ should return 6 when called using using stage[6].endBlock
        last stage
          ✓ should return stageCount when called using using
stage[stageCount].startBlock
          ✓ should return stageCount when called using using
stage[stageCount].endBlock
        1 block before 0
          ✓ should throw "Block outside of rICO period."
        1 block after last stage
          ✓ should throw "Block outside of rICO period."

  Javascript Validator - Contract - commit()
    Participant - commits 1 eth
      State changes after first contribution by a Participant
        ✓ Contract.participantsById indexes the participant id => address
        ✓ Contract.participantCount increases by 1
        ParticipantRecord
          ✓ contributions is 1
      State changes after a new contribution
        ✓ Contract.totalSentETH increases by commited value
        ParticipantRecord
          ✓ contributions increases by 1
          ✓ totalSentETH increases by commited value
          ✓ returnedETH does not change
          ✓ withdrawnETH does not change
          ✓ allocatedETH does not change
          ✓ returnedTokens does not change
          ✓ committedETH does not change
          ✓ boughtTokens does not change
          ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
          currentStageRecord
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ committedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            ✓ boughtTokens does not change
            ✓ returnedTokens does not change
        ETH Balances:
          ✓ Contract ETH balance increases by commit value
          ✓ Participant ETH balance decreases by commit value
    Participant - commits 1 eth - second time
      Contract State changes after contribution from existing Participant
        ✓ Contract.participantCount does not change
      State changes after a new contribution
        ✓ Contract.totalSentETH increases by commited value
        ParticipantRecord
          ✓ contributions increases by 1
          ✓ totalSentETH increases by commited value
          ✓ returnedETH does not change
          ✓ withdrawnETH does not change
          ✓ allocatedETH does not change
          ✓ returnedTokens does not change
          ✓ committedETH does not change
          ✓ boughtTokens does not change
          ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
          currentStageRecord
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ committedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            ✓ boughtTokens does not change
            ✓ returnedTokens does not change
        ETH Balances:
          ✓ Contract ETH balance increases by commit value
          ✓ Participant ETH balance decreases by commit value
    Participant - commits 1 eth - third time
      Contract State changes after contribution from existing Participant
        ✓ Contract.participantCount does not change
      State changes after a new contribution
        ✓ Contract.totalSentETH increases by commited value
        ParticipantRecord
          ✓ contributions increases by 1
          ✓ totalSentETH increases by commited value
          ✓ returnedETH does not change
          ✓ withdrawnETH does not change
          ✓ allocatedETH does not change
          ✓ returnedTokens does not change
          ✓ committedETH does not change
          ✓ boughtTokens does not change
          ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
          currentStageRecord
```

```
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ committedETH does not change (5ms)
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            ✓ boughtTokens does not change
            ✓ returnedTokens does not change
        ETH Balances:
          ✓ Contract ETH balance increases by commit value
          ✓ Participant ETH balance decreases by commit value
    Participant 2 - commits 1 eth
      ✓ Contract.participantCount is 2
      State changes after first contribution by a Participant
        ✓ Contract.participantsById indexes the participant id => address
        ✓ Contract.participantCount increases by 1
        ParticipantRecord
          ✓ contributions is 1
      State changes after a new contribution
        ✓ Contract.totalSentETH increases by commited value
        ParticipantRecord
          ✓ contributions increases by 1
          ✓ totalSentETH increases by commited value
          ✓ returnedETH does not change
          ✓ withdrawnETH does not change
          ✓ allocatedETH does not change
          ✓ returnedTokens does not change
          ✓ committedETH does not change
          ✓ boughtTokens does not change
          ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
          currentStageRecord
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ committedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            ✓ boughtTokens does not change
            ✓ returnedTokens does not change
        ETH Balances:
          ✓ Contract ETH balance increases by commit value
          ✓ Participant ETH balance decreases by commit value

  Javascript Validator - Contract - whitelist()
    Scenario: Stage:0, Participant gets whitelisted then contributes
      - Participant gets whitelisted
        Contract State changes after whitelisting of Participant with no
contributions
          ParticipantRecord
            ✓ whitelisted is true
          ETH Balances:
            ✓ Contract ETH balance does not change
            ✓ Participant ETH balance does not change
      - Participant commits 1 eth
        State changes after first contribution by a Participant
          ✓ Contract.participantsById indexes the participant id => address
          ✓ Contract.participantCount increases by 1
          ParticipantRecord
            ✓ contributions is 1
        State changes after a new contribution
          ✓ Contract.totalSentETH increases by commited value
          ParticipantRecord
            ✓ contributions increases by 1
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ returnedTokens does not change
            ✓ committedETH increases by commit value
            ✓ pendingTokens is 0
            ✓ boughtTokens increases by getTokenAmountForEthAtStage(value)
            currentStageRecord
              ✓ totalSentETH increases by commited value
              ✓ returnedETH does not change
              ✓ committedETH increases by commit value
              ✓ withdrawnETH does not change
              ✓ allocatedETH does not change
              ✓ pendingTokens is 0
              ✓ boughtTokens increases by getTokenAmountForEthAtStage(value)
              ✓ returnedTokens does not change
          ETH Balances:
            ✓ Contract ETH balance increases by commit value
            ✓ Participant ETH balance decreases by commit value
    Scenario: Stage:0, Participant contributes then gets whitelisted
      - Participant commits 1 eth
        State changes after first contribution by a Participant
          ✓ Contract.participantsById indexes the participant id => address
          ✓ Contract.participantCount increases by 1
          ParticipantRecord
            ✓ contributions is 1
        State changes after a new contribution
          ✓ Contract.totalSentETH increases by commited value
          ParticipantRecord
            ✓ contributions increases by 1
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ returnedTokens does not change
            ✓ committedETH does not change
            ✓ boughtTokens does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            currentStageRecord
              ✓ totalSentETH increases by commited value
              ✓ returnedETH does not change
              ✓ committedETH does not change
              ✓ withdrawnETH does not change
              ✓ allocatedETH does not change
              ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
              ✓ boughtTokens does not change
              ✓ returnedTokens does not change
          ETH Balances:
            ✓ Contract ETH balance increases by commit value
            ✓ Participant ETH balance decreases by commit value
      - Participant gets whitelisted
        ✓ Participant token balance is 500
        State changes after whitelist mode: true
          ParticipantRecord
            ✓ whitelisted is true
          acceptContributions()
            Contract:
              ✓ returnedETH does not change
              ✓ committedETH increases by commit value
            ParticipantRecord:
              ✓ whitelisted is true
              ✓ ParticipantAvailableETH is commit value
              ✓ committedETH increases by commit value
            Tokens:
              ✓ Participant token balance is oldState.ParticipantRecord.pendingTokens
              ✓ ParticipantRecord.pendingTokens is 0
          ETH Balances:
            ✓ Contract ETH balance does not change
            ✓ Participant ETH balance does not change
    Scenario: Stage:6, Participant contributes then gets rejected
      - Participant commits 1 eth
        State changes after first contribution by a Participant
          ✓ Contract.participantsById indexes the participant id => address
          ✓ Contract.participantCount increases by 1
          ParticipantRecord
            ✓ contributions is 1
        State changes after a new contribution
          ✓ Contract.totalSentETH increases by commited value
          ParticipantRecord
            ✓ contributions increases by 1
            ✓ totalSentETH increases by commited value
            ✓ returnedETH does not change
            ✓ withdrawnETH does not change
            ✓ allocatedETH does not change
            ✓ returnedTokens does not change
            ✓ committedETH does not change
            ✓ boughtTokens does not change
            ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
            currentStageRecord
              ✓ totalSentETH increases by commited value
              ✓ returnedETH does not change
              ✓ committedETH does not change
              ✓ withdrawnETH does not change
              ✓ allocatedETH does not change
              ✓ pendingTokens increases by getTokenAmountForEthAtStage(value)
              ✓ boughtTokens does not change
              ✓ returnedTokens does not change
            Each Previous StageRecord (5)
              ✓ totalSentETH does not change
              ✓ returnedETH does not change
              ✓ committedETH does not change
              ✓ withdrawnETH does not change
              ✓ pendingTokens does not change
              ✓ boughtTokens does not change
              ✓ returnedTokens does not change
              ✓ allocatedETH does not change
          ETH Balances:
            ✓ Contract ETH balance increases by commit value
            ✓ Participant ETH balance decreases by commit value
      - Participant gets rejected
        State changes after whitelist mode: false
          ParticipantRecord
            ✓ whitelisted is false
          cancelContributionsForAddress()
            Contract:
              ✓ committedETH does not change
              ✓ returnedETH increases by oldState.ParticipantAvailableETH value
            ParticipantRecord:
              ✓ ParticipantAvailableETH is 0
              ✓ whitelisted is false
              ✓ pendingTokens is 0
              ✓ withdrawnETH increases by oldState.ParticipantAvailableETH
            Tokens:
              ✓ Participant token balance does not change
              ✓ ParticipantRecord.pendingTokens is 0
            ETH Balances:
              ✓ Contract ETH balance decreases by oldState.ParticipantAvailableETH
              ✓ Participant ETH balance increases by oldState.ParticipantAvailableETH


  290 passing (625ms)

Done
-------------------------------------------------------------------

Killing existing ganache-cli instance at pid 44589.


> ricopoc@0.0.1 test-solc /Users/gnsps/lukso-rico-audit-2020-04/code
> scripts/run_solc.sh all refresh

Starting new ganache-cli instance at port 8545
exchange neither monster ethics bless cancel ghost excite business record warfare
invite
```

```
--------------------------------------------------------------------
 Running all tests in "test" folder:
--------------------------------------------------------------------
You can improve web3's peformance when running Node.js versions older than 10.5.0 by
installing the (deprecated) scrypt package in your project
You can improve web3's peformance when running Node.js versions older than 10.5.0 by
installing the (deprecated) scrypt package in your project

Compiling your contracts...
===========================
✔ Fetching solc version list from solc-bin. Attempt #1
✔ Downloading compiler. Attempt #1.
> Compiling ./contracts/Gnosis/CreateCall.sol
> Compiling ./contracts/Gnosis/GnosisSafe.sol
> Compiling ./contracts/Migrations.sol
> Compiling ./contracts/ReversibleICO.sol
> Compiling ./contracts/RicoToken.sol
> Compiling ./contracts/mocks/ERC777Mock.sol
> Compiling ./contracts/mocks/ERC777SenderRecipientMock.sol
> Compiling ./contracts/mocks/EmptyReceiver.sol
> Compiling ./contracts/mocks/MathMock.sol
> Compiling ./contracts/mocks/ReversibleICOMock.sol
> Compiling ./contracts/mocks/ReversibleICOMock777.sol
> Compiling ./contracts/mocks/SafeMathMock.sol
> Compiling ./contracts/zeppelin/access/Roles.sol
> Compiling ./contracts/zeppelin/access/roles/CapperRole.sol
> Compiling ./contracts/zeppelin/access/roles/MinterRole.sol
> Compiling ./contracts/zeppelin/access/roles/PauserRole.sol
> Compiling ./contracts/zeppelin/access/roles/SignerRole.sol
> Compiling ./contracts/zeppelin/access/roles/WhitelistAdminRole.sol
> Compiling ./contracts/zeppelin/access/roles/WhitelistedRole.sol
> Compiling ./contracts/zeppelin/crowdsale/Crowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/distribution/FinalizableCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/distribution/PostDeliveryCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/distribution/RefundableCrowdsale.sol
> Compiling
./contracts/zeppelin/crowdsale/distribution/RefundablePostDeliveryCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/emission/AllowanceCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/price/IncreasingPriceCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/CappedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/IndividuallyCappedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/PausableCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/TimedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/WhitelistCrowdsale.sol
> Compiling ./contracts/zeppelin/cryptography/ECDSA.sol
> Compiling ./contracts/zeppelin/cryptography/MerkleProof.sol
> Compiling ./contracts/zeppelin/drafts/Counters.sol
> Compiling ./contracts/zeppelin/drafts/ERC1046/ERC20Metadata.sol
> Compiling ./contracts/zeppelin/drafts/ERC20Migrator.sol
> Compiling ./contracts/zeppelin/drafts/ERC20Snapshot.sol
> Compiling ./contracts/zeppelin/drafts/SignatureBouncer.sol
> Compiling ./contracts/zeppelin/drafts/SignedSafeMath.sol
> Compiling ./contracts/zeppelin/drafts/Strings.sol
> Compiling ./contracts/zeppelin/drafts/TokenVesting.sol
> Compiling ./contracts/zeppelin/examples/SampleCrowdsale.sol
> Compiling ./contracts/zeppelin/examples/SimpleToken.sol
> Compiling ./contracts/zeppelin/introspection/ERC165.sol
> Compiling ./contracts/zeppelin/introspection/ERC165Checker.sol
> Compiling ./contracts/zeppelin/introspection/ERC1820Implementer.sol
> Compiling ./contracts/zeppelin/introspection/IERC165.sol
> Compiling ./contracts/zeppelin/introspection/IERC1820Implementer.sol
> Compiling ./contracts/zeppelin/introspection/IERC1820Registry.sol
> Compiling ./contracts/zeppelin/lifecycle/Pausable.sol
> Compiling ./contracts/zeppelin/math/Math.sol
> Compiling ./contracts/zeppelin/math/SafeMath.sol
> Compiling ./contracts/zeppelin/ownership/Ownable.sol
> Compiling ./contracts/zeppelin/ownership/Secondary.sol
> Compiling ./contracts/zeppelin/payment/PaymentSplitter.sol
> Compiling ./contracts/zeppelin/payment/PullPayment.sol
> Compiling ./contracts/zeppelin/payment/escrow/ConditionalEscrow.sol
> Compiling ./contracts/zeppelin/payment/escrow/Escrow.sol
> Compiling ./contracts/zeppelin/payment/escrow/RefundEscrow.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20Burnable.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20Capped.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20Detailed.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20Mintable.sol
> Compiling ./contracts/zeppelin/token/ERC20/ERC20Pausable.sol
> Compiling ./contracts/zeppelin/token/ERC20/IERC20.sol
> Compiling ./contracts/zeppelin/token/ERC20/SafeERC20.sol
> Compiling ./contracts/zeppelin/token/ERC20/TokenTimelock.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Burnable.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Enumerable.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Full.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Holder.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Metadata.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721MetadataMintable.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Mintable.sol
> Compiling ./contracts/zeppelin/token/ERC721/ERC721Pausable.sol
> Compiling ./contracts/zeppelin/token/ERC721/IERC721.sol
> Compiling ./contracts/zeppelin/token/ERC721/IERC721Enumerable.sol
> Compiling ./contracts/zeppelin/token/ERC721/IERC721Full.sol
> Compiling ./contracts/zeppelin/token/ERC721/IERC721Metadata.sol
> Compiling ./contracts/zeppelin/token/ERC721/IERC721Receiver.sol
> Compiling ./contracts/zeppelin/token/ERC777/ERC777.sol
> Compiling ./contracts/zeppelin/token/ERC777/IERC777.sol
> Compiling ./contracts/zeppelin/token/ERC777/IERC777Recipient.sol
> Compiling ./contracts/zeppelin/token/ERC777/IERC777Sender.sol
> Compiling ./contracts/zeppelin/utils/Address.sol
> Compiling ./contracts/zeppelin/utils/Arrays.sol
> Compiling ./contracts/zeppelin/utils/ReentrancyGuard.sol
> Compilation warnings encountered:
,,
> Artifacts written to /Users/gnsps/lukso-rico-audit-2020-04/code/build/contracts
> Compiled successfully using:
   - solc: 0.5.17+commit.d19bba13.Emscripten.clang

You can improve web3's peformance when running Node.js versions older than 10.5.0 by
installing the (deprecated) scrypt package in your project
  ----------------------------------------------------------------
  Step 1 - Setting up helpers and globals
  ----------------------------------------------------------------
  ----------------------------------------------------------------
  Step 2 - Run tests
  ----------------------------------------------------------------
Current Block:  11
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  12
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  13
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block:  14
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  0
Current Block:  15
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: CONTRIBUTE 1
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3
Current Block:  16
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3
Current Block:  17
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  4
Current Block:  18
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
```

```
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  19
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: CONTRIBUTE 1
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  20
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  0
Current Block:  21
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  6
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3
Current Block:  22
Current Block:  23
Current Block:  24
Current Block:  25
Current Block:  26
Current Block:  27
Current Block:  28
Current Block:  29
Current Block:  30
Current Block:  31
Current Block:  32
Current Block:  33
Current Block:  34
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  35
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  9
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  36
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  5
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  6
Current Block:  37
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  38
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
```

```
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  39
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  8
Current Block:  40
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  8
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  41
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  8
Current Block:  42
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  43
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  9
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  4
Current Block:  44
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  45
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  46
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  8
Current Block:  47
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  48
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
```

```
Current Block:  49
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  5
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  50
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  51
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  9
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  52
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  53
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  54
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  6
Current Block:  55
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  56
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  9
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  0
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  4
Current Block:  57
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  6
Current Block:  58
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  59
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
```

```
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  6
Current Block:  60
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  4
Current Block:  61
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  62
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block:  63
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  64
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3
Current Block:  65
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  0
Current Block:  66
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  6
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  67
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  9
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  68
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  4
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  69
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
```

```
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block:  70
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  4
Current Block:  71
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  5
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: CONTRIBUTE 1
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  8
Current Block:  72
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  73
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  74
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  75
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  8
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  76
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  77
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  78
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: CONTRIBUTE 1
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  79
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: CONTRIBUTE 1
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  80
```

```
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  81
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  0
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  9
Current Block:  82
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  83
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  5
Current Block:  84
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block:  85
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  0
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  7
Current Block:  86
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:  8
Current Block:  87
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:  5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Number of Participants:  4


  SafeMath
    add
      ✓ adds correctly (93ms)
      ✓ reverts on addition overflow (110ms)
    sub
      ✓ subtracts correctly (52ms)
      ✓ reverts if subtraction result would be negative (40ms)
    mul
      ✓ multiplies correctly (52ms)
      ✓ multiplies by zero correctly (141ms)
      ✓ reverts on multiplication overflow (47ms)
    div
      ✓ divides correctly (32ms)
      ✓ divides zero correctly (26ms)
      ✓ returns complete number result on non-even division (32ms)
      ✓ reverts on division by zero (30ms)
    mod
      ✓ reverts with a 0 divisor (26ms)
      modulos correctly
        ✓ when the dividend is smaller than the divisor (28ms)
        ✓ when the dividend is equal to the divisor (27ms)
        ✓ when the dividend is larger than the divisor (24ms)
        ✓ when the dividend is a multiple of the divisor (24ms)

  ERC1820 - Token Registry
    Step 1 - Before deployment state
      ✓ Contract Code at address: 0x1820a4B7618BdE71Dce8cdc73aAB6C95905faD24 should
be 0x
      ✓ Deployer address: 0xa990077c3205cbDf861e17Fa532eeB069cE9fF96 balance should
be 0 eth (10ms)
      ✓ Funds Supplier address: 0xFE6B56FdCF920382Af1493828E79C017EE090F2a balance
should be at least 0.08 eth
    Step 2 - Deployment preparation
      New Account balances after Supplier sends value to SenderAddress
        ✓ FundsSupplier balance has deploymentCost + tx fee substracted
        ✓ SenderAddress balance is equal to deploymentCost
    Step 3 - ERC1820 Deployment
      Gas used for deployment: 711453
      Contract Address: 0x1820a4B7618BdE71Dce8cdc73aAB6C95905faD24

      Validation after ERC1820 Registry contract deployment
        Transaction
          ✓ status is true
          ✓ signature is valid
          ✓ from address is correct
          ✓ Contract address is 0x1820a4B7618BdE71Dce8cdc73aAB6C95905faD24
        Contract
          ✓ code at address exists (13ms)
          ✓ contract has the getManager method which can be called (51ms)
     * EVM snapshot[ERC1820_ready] saved

  ReversibleICO - Withdraw Token Balance
     * EVM snapshot[ERC1820_ready] restored
     * EVM snapshot[WithdrawTokenTests_Phase_2] start
      Contract deployed:   RicoToken
        Gas used:          4224630
        Contract Address:  0x88eC20080706B787C7BF684880f3d1899433f760
      Contract deployed:   ReversibleICOMock
        Gas used:          5661611
        Contract Address:  0x35C310d59E2b7f1F96A5e133Efb20538266e4053
     * EVM snapshot[WithdrawTokenTests_Phase_2] saved
    randomly contribute and exit
```

```
     * EVM snapshot[WithdrawTokenTests_Phase_2] restored
---> Project withdraw:  89207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (134ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (131ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 11 (142ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (46ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (44ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (125ms)
---> Contribution : 150777 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (295ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 12 (120ms)
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Return tokens (106ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 13 (115ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 14 (123ms)
---> Contribution : 120777 GAS
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (290ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (25ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (105ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 15 (145ms)
---> Contribution : 120777 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (250ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (105ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 16 (97ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (99ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 17 (97ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (113ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 18 (103ms)
---> Contribution : 65455 GAS
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (219ms)
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (17ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 19 (148ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 20 (221ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (116ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 21 (100ms)
      ✓ Freeze contract at block 22 (63ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 22 (99ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 23 (119ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 24 (98ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 25 (85ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 26 (86ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 27 (107ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 28 (130ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 29 (122ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 30 (113ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 31 (104ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 32 (109ms)
      ✓ Unfreeze contract at block 33 (65ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 33 (164ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 34 (125ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 35 (173ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 36 (145ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 37 (136ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (32ms)
Stage: 0, Price: 25000000000000000
      ✓ Jump to the next block: 38 (123ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (26ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 39 (131ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 40 (131ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 41 (130ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (26ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 42 (162ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (267ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 43 (166ms)
---> Contribution : 65455 GAS
```

```
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (515ms)
Stage: 1, Price: 28333333333333333
      ✓ Jump to the next block: 44 (180ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (37ms)
---> Project withdraw:  59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (214ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 45 (198ms)
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (21ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 46 (92ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 47 (89ms)
---> Whitelisting:  276818 GAS
---> Contribution with auto accepting : 185174 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (1166ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 48 (114ms)
---> Project withdraw:  98129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (105ms)
---> Whitelisting:  210967 GAS
---> Contribution with auto accepting : 185174 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (994ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 49 (89ms)
---> Contribution with auto accepting : 200351 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (490ms)
Stage: 2, Price: 31666666666666666
      ✓ Jump to the next block: 50 (87ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 51 (86ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 52 (91ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (85ms)
---> Contribution with auto accepting : 200709 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (492ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 53 (88ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (94ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 54 (78ms)
---> Withdraw:  171420 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (166ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 55 (87ms)
Stage: 3, Price: 34999999999999999
      ✓ Jump to the next block: 56 (86ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (16ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 57 (78ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (13ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 58 (154ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (18ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 59 (100ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 60 (82ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (90ms)
---> Contribution with auto accepting : 186126 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (455ms)
---> Contribution with auto accepting : 186126 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (474ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 61 (83ms)
---> Withdraw:  156420 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Return tokens (149ms)
Stage: 4, Price: 38333333333333332
      ✓ Jump to the next block: 62 (75ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (20ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (27ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 63 (81ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (13ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (162ms)
---> Project withdraw:  60858 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (100ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 64 (87ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (98ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 65 (103ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (98ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 66 (92ms)
---> Contribution with auto accepting : 186602 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (503ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 67 (88ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (14ms)
---> Contribution with auto accepting : 186602 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (512ms)
Stage: 5, Price: 41666666666666665
      ✓ Jump to the next block: 68 (89ms)
---> Withdraw:  156420 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Return tokens (228ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 69 (85ms)
```

```
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (81ms)
---> Project withdraw:  60858 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (87ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 70 (84ms)
---> Whitelisting:  52939 GAS
---> Contribution with auto accepting : 283023 GAS
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Buy tokens (543ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 71 (82ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 72 (83ms)
---> Contribution with auto accepting : 187019 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (515ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 73 (92ms)
---> Withdraw:  171420 GAS
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (175ms)
---> Project withdraw:  68070 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (99ms)
Stage: 6, Price: 44999999999999998
      ✓ Jump to the next block: 74 (80ms)
---> Contribution with auto accepting : 187019 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (590ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 75 (97ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 76 (99ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 77 (95ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (90ms)
---> Contribution with auto accepting : 187377 GAS
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Buy tokens (463ms)
---> Withdraw:  156297 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (159ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 78 (85ms)
---> Whitelisting:  235613 GAS
---> Contribution with auto accepting : 187259 GAS
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (1859ms)
---> Withdraw:  156361 GAS
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (257ms)
---> Contribution with auto accepting : 187377 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (730ms)
---> Contribution with auto accepting : 187377 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (799ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 79 (107ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (146ms)
```

```
---> Contribution with auto accepting : 187377 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (894ms)
Stage: 7, Price: 48333333333333331
      ✓ Jump to the next block: 80 (101ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 81 (98ms)
---> Withdraw:  156356 GAS
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (288ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 82 (97ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 83 (156ms)
---> Contribution with auto accepting : 187853 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (594ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 84 (89ms)
---> Project withdraw:  68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (92ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 85 (76ms)
---> Withdraw:  156356 GAS
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (173ms)
Stage: 8, Price: 51666666666666664
      ✓ Jump to the next block: 86 (144ms)
---> Contribution with auto accepting : 187853 GAS
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (706ms)
Stage: 9, Price: 54999999999999997
      ✓ Jump to the next block: 87 (101ms)
      ✓ rICO should be finished (37ms)
      ✓ rICO balance - getAvailableProjectETH should be 0 (25ms)
      ✓ rICO rest balance should be no more or less than 0% off to what was ever
committed ETH (57ms)
      ✓ rICO balance should have all getAvailableProjectETH still (25ms)
      ✓ Project balance + getAvailableProjectETH should be committedETH (46ms)
      ✓ Project should have all projectWithdrawnETH (14ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: compare full token balances
(18ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: reserved token balance should be
0 (21ms)
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: unlocked token balance should be
all bought tokens (26ms)
Participant Stats: 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Result {
  '0': true,
  '1': '3',
  '2': '0',
  '3': '62000000000000000000',
  '4': '2063333333333333282',
  '5': '0',
  '6': '62000000000000000000',
  '7': '0',
  '8': '67',
  whitelisted: true,
  contributions: '3',
  withdraws: '0',
  reservedTokens: '62000000000000000000',
  committedEth: '2063333333333333282',
  pendingEth: '0',
  _currentReservedTokens: '62000000000000000000',
  _unlockedTokens: '0',
  _lastBlock: '67' }
-------
Compare prices paid  33888888888888888
      ✓ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: compare price average, should be
0 (22ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: compare full token balances
(18ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: reserved token balance should be
0 (28ms)
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: unlocked token balance should be
all bought tokens (16ms)
Participant Stats: 0x10a0717595A97A777F51f3ae542d4312edfD20FA Result {
  '0': true,
  '1': '2',
  '2': '3',
  '3': '69935689161348817000',
  '4': '3276953567763392027',
  '5': '0',
  '6': '4700750087631469563',
  '7': '65234939073717347437',
  '8': '74',
  whitelisted: true,
  contributions: '2',
  withdraws: '3',
  reservedTokens: '69935689161348817000',
  committedEth: '3276953567763392027',
  pendingEth: '0',
  _currentReservedTokens: '4700750087631469563',
  _unlockedTokens: '65234939073717347437',
  _lastBlock: '74' }
-------
Compare prices paid  46666666666666664
Compare prices withdraw  46237780567259190
      ✓ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: compare price average, should be
0 (20ms)
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: compare full token balances
(24ms)
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: reserved token balance should be
0 (19ms)
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: unlocked token balance should be
all bought tokens (19ms)
Participant Stats: 0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Result {
  '0': true,
  '1': '7',
  '2': '3',
  '3': '109329431275414248000',
  '4': '3813784881602372481',
  '5': '0',
  '6': '15455486025207072261',
  '7': '93873945250207175739',
  '8': '70',
  whitelisted: true,
  contributions: '7',
  withdraws: '3',
  reservedTokens: '109329431275414248000',
  committedEth: '3813784881602372481',
  pendingEth: '0',
  _currentReservedTokens: '15455486025207072261',
  _unlockedTokens: '93873945250207175739',
  _lastBlock: '70' }
-------
Compare prices paid  35476190476190475
Compare prices withdraw  31705770993565596
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: compare price average, should be
0 (38ms)
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: compare full token balances
(19ms)
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: reserved token balance should be
0 (20ms)
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: unlocked token balance should be
all bought tokens (28ms)
Participant Stats: 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Result {
  '0': true,
  '1': '11',
  '2': '2',
  '3': '542031893923099250000',
  '4': '23555201231560275220',
  '5': '0',
  '6': '105489722069174269196',
  '7': '436542171853924980804',
  '8': '75',
  whitelisted: true,
  contributions: '11',
  withdraws: '2',
  reservedTokens: '542031893923099250000',
  committedEth: '23555201231560275220',
  pendingEth: '0',
  _currentReservedTokens: '105489722069174269196',
  _unlockedTokens: '436542171853924980804',
  _lastBlock: '75' }
-------
Compare prices paid  41666666666666665
Compare prices withdraw  33769882384568211
      ✓ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: compare price average, should be
0 (22ms)
```

```
  200 passing (33s)

Done
--------------------------------------------------------------------

Killing existing ganache-cli instance at pid 44604.
```

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.