

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.



Our review focused on the commit hash

dc6b22ba8991d77560e574eac7f4f1e17f643115

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:

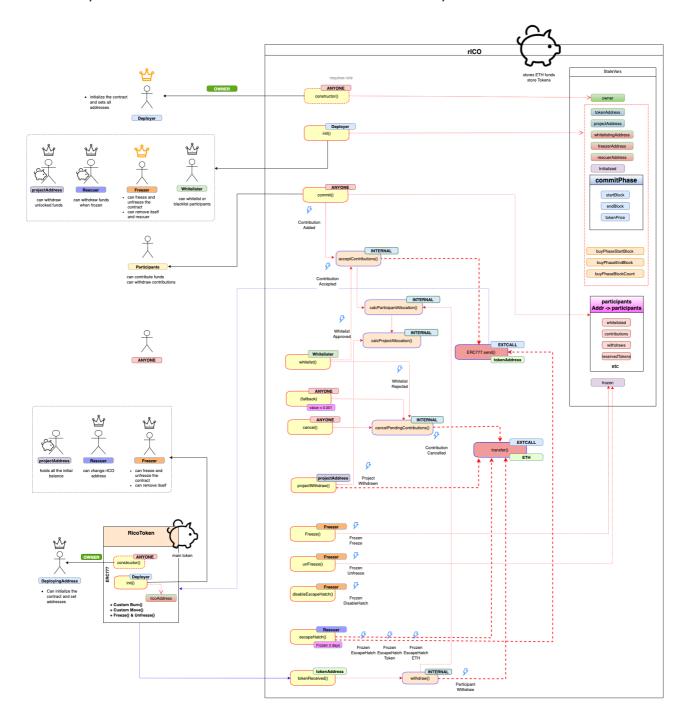
ReversibleICO



 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.

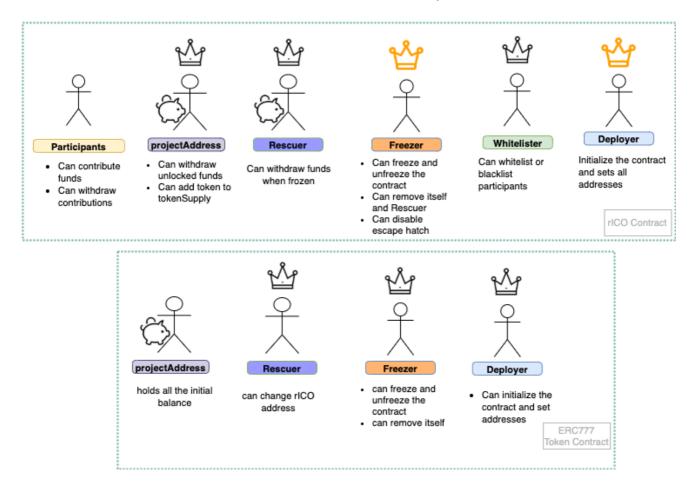
re details about the Actors and their permissions can be found in Actors.

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:



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 wing 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 <code>escapeHatch()</code> 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.



- 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 <code>getCurrentBlockNumber()</code> for actual current block number, and <code>getCurrentEffectiveBlockNumber()</code> for effective block number (deducting <code>frozenPeriod</code>).

UPDATE: The new function <code>getCurrentEffectiveBlockNumber()</code> was added in <code>lukso-network/rICO-smart-contracts@_e4c9ed5</code> .

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 luksonetwork/rICO-smart-contracts@ e4c9ed5.



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,

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

ያያት 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 loyment 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



Found in parallel to the audit team and has been mitigated in luksonetwork/rICO-smart-contracts@ ebc4bce . The issue was further simplified by adding <code>getCurrentEffectiveBlockNumber()</code> 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 calculat
}
```

code/contracts/ReversibleICO.sol:L654-L656

```
function getStageAtBlock(uint256 _blockNumber) public view returns (uint8) {
    uint256 blockNumber = _blockNumber.sub(frozenPeriod); // adjust the block
```

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

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:</pre>

```
uint256 blockNumber = _blockNumber.sub(frozenPeriod); // adjust the block by
require(blockNumber >= commitPhaseStartBlock && blockNumber <= buyPhaseEndBl</pre>
```

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 canno
```

The check in the <code>getStageAtBlock()</code> can be removed. However this is assuming that the correct calculation of the <code>currentEffectiveBlockNumber</code> 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 e 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 preexisting 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 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.

Blocks since the start of the commit phase

7 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.s ol	3d5bf2c18b1ffa10b50eaac4cc62eaf43a40b 6c2
contracts/RicoToken.sol	7d500809f2d14e4ea728ae126d4711239dffc4 22

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
 485:8 warning Call with hardcoded gas amount
 712:23 warning Potential use of a weak source of randomness "block.numbe
 848:12 warning Local variable shadows a state variable
 869:8 warning Call with hardcoded gas amount
/code/contracts/mocks/reversibleicomock.sol
  5:42 warning A floating pragma is set
                                                          SWC-103
       warning The state variable visibility is not set SWC-108
 9:9
/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
X 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/GnosisSafo col

```
CUITET ac (5/0110515/01105155ale.501
  427:4
           warning
                      Line contains trailing whitespace
                                                                  no-trailing-
  480:2
                      Only use indent of 4 spaces.
                                                                  indentation
           error
  485:6
                      Only use indent of 8 spaces.
                                                                  indentation
           error
  489:4
                      Provide an error message for require()
                                                                  error-reasor
           warning
  492:0
                      Only use indent of 4 spaces.
                                                                  indentation
           error
  497:2
           error
                      Only use indent of 4 spaces.
                                                                  indentation
  498:4
                      Provide an error message for require()
                                                                  error-reasor
           warning
                      Only use indent of 4 spaces.
  503:0
                                                                  indentation
           error
  508:2
                      Only use indent of 4 spaces.
                                                                  indentation
           error
  509:4
                      Provide an error message for require()
           warning
                                                                  error-reasor
  513:0
           error
                      Only use indent of 4 spaces.
                                                                  indentation
  518:2
                      Only use indent of 4 spaces.
                                                                  indentation
           error
                      Provide an error message for require()
  520:4
           warning
                                                                  error-reasor
                      Only use indent of 4 spaces.
                                                                  indentation
  523:0
           error
  529:2
                      Only use indent of 4 spaces.
                                                                  indentation
           error
  530:4
           warning
                      Provide an error message for require()
                                                                  error-reasor
                      Only use indent of 4 spaces.
  532:0
                                                                  indentation
           error
  739:1
                      Line contains trailing whitespace
                                                                  no-trailing-
           warning
contracts/ReversibleICO.sol
  313:45
            error
                       String literal must be quoted with double quotes.
  542:67
                       String literal must be quoted with double quotes.
            error
  680:23
                       There should be no whitespace or comments between arc
            warning
                       Only use indent of 12 spaces.
  681:10
            error
  771:12
                       String literal must be quoted with double quotes.
            error
  777:12
                       String literal must be quoted with double quotes.
            error
  793:12
                        String literal must be quoted with double quotes.
            error
  979:42
                       String literal must be quoted with double quotes.
            error
contracts/mocks/ERC777Mock.sol
                  "../zeppelin/token/ERC777/ERC777.sol": Import statements n
  3:7
         error
contracts/mocks/ERC777SenderRecipientMock.sol
  9:7
                       "../zeppelin/token/ERC777/ERC777.sol": Import statemer
           error
  54:12
           warning
                      Provide an error message for revert()
  85:12
                      Provide an error message for revert()
           warning
  143:8
                      Consider using 'transfer' in place of 'send'.
           warning
contracts/mocks/MathMock.sol
                  "../zeppelin/math/Math.sol": Import statements must use do
contracts/mocks/ReversibleICOMock.sol
                   ".../ReversibleICO.sol": Import statements must use double
  11:7
          error
contracts/mocks/ReversibleICOMock777.sol
  11:7
          error
                   "./ReversibleICOMock.sol": Import statements must use dou
     acts/mocks/SafeMathMock.sol
                  "../zeppelin/math/SafeMath.sol": Import statements must us
```

https://consensys.net/diligence/audits/2020/04/rico/

```
contracts/zeppelin/crowdsale/Crowdsale.sol
 149:89
           warning
                      Code contains empty block
                                                   no-empty-blocks
 179:85
                      Code contains empty block
                                                   no-empty-blocks
           warning
contracts/zeppelin/crowdsale/distribution/FinalizableCrowdsale.sol
          warning Code contains empty block no-empty-blocks
contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol
                   Only use indent of 12 spaces.
                                                  indentation
contracts/zeppelin/crowdsale/price/IncreasingPriceCrowdsale.sol
 64:30
          warning
                     Avoid using 'block.timestamp'.
                                                     security/no-block-me
contracts/zeppelin/crowdsale/validation/TimedCrowdsale.sol
                    Avoid using 'block.timestamp'.
 38:31
          warning
                                                      security/no-block-me
 65:15
                   Avoid using 'block.timestamp'. security/no-block-me
          warning
 65:50
          warning
                    Avoid using 'block.timestamp'.
                                                     security/no-block-me
 74:15
                     Avoid using 'block.timestamp'.
                                                     security/no-block-me
          warning
contracts/zeppelin/cryptography/ECDSA.sol
                 Avoid using Inline Assembly. security/no-inline-assembly.
 42:8
         error
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-m
                     Avoid using 'block.timestamp'.
 166:12
           warning
                                                       security/no-block-m
                     Avoid using 'block.timestamp'.
 168:19
           warning
                                                       security/no-block-m
                      Avoid using 'block.timestamp'.
 171:36
                                                        security/no-block-m
           warning
contracts/zeppelin/introspection/ERC165Checker.sol
                   Avoid using Inline Assembly. security/no-inline-assem
 102:8
          error
contracts/zeppelin/token/ERC20/SafeERC20.sol
 33:16
          error
                     Only use indent of 12 spaces.
                                                              indentation
 67:65
                     Avoid using low-level function 'call'.
          warning
                                                              security/no-
contracts/zeppelin/token/ERC20/TokenTimelock.sol
                     Avoid using 'block.timestamp'.
 29:30
          warning
                                                     security/no-block-me
 61:16
          warning
                     Avoid using 'block.timestamp'. security/no-block-me
contracts/zeppelin/token/ERC721/ERC721.sol
 91:16
                   Only use indent of 12 spaces.
          error
                                                   indentation
contracts/zeppelin/token/ERC721/IERC721.sol
                   Line contains trailing whitespace
                                                        no-trailing-whites
         warning
```

contracts/zeppelin/token/ERC721/IERC721Full.sol

```
11:68 warning Code contains empty block
                                                 no-empty-blocks
contracts/zeppelin/token/ERC721/IERC721Receiver.sol
                  Only use indent of 4 spaces. indentation
         error
contracts/zeppelin/token/ERC777/ERC777.sol
           error
                      Only use indent of 4 spaces.
 48:0
                      Only use indent of 4 spaces.
           error
 471:12
           warning
                      Error message exceeds max length of 76 characters
contracts/zeppelin/utils/Address.sol
                   Line contains trailing whitespace no-trailing-whites
 21:8
 28:8
                    Avoid using Inline Assembly.
                                                         security/no-inline
X 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	SHA-1 Hash
contracts/Gnosis/CreateCall.sol	e33c0ec5bcbeeb3ea22107 3e37b594a490863679
contracts/Gnosis/GnosisSafe.sol	af2dbf4f80b63f0edf1ebab a8c632fa2cc0c8e74
contracts/Migrations.sol	6eddef3c09c6eae904260 0a1e73310183e0c6f5d
contracts/ReversibleICO.sol	b40a2464c0fc24a5c1b8d5 9eb2e5f344f5618211
contracts/RicoToken.sol	7d500809f2d14e4ea728ae 126d4711239dffc422

File Name	SHA-1 Hash
contracts/mocks/ERC777Mock.sol	679dfee5742c44d8c2bc4b b3da866f5f89b51af5
contracts/mocks/ERC777SenderRecipientMock.sol	990ec041972850ba2fc1cd de3fad10cb442d6557
contracts/mocks/EmptyReceiver.sol	f4f7155b6c24f385be55da6 7f84840bb60d5cb25
contracts/mocks/MathMock.sol	147138b16a7e5fa032f92cc 53e73ff0d1cc6cb9e
contracts/mocks/ReversibleICOMock.sol	8e15fa7194b65d306183d5 af996d4c6c09b2598f
contracts/mocks/ReversibleICOMock777.so	87c2bf80a0fdd630995c3b 7f48892c19726133aa
contracts/mocks/SafeMathMock.sol	906a40c436b2315f8204f9 9896503c87e1ee5c7a
contracts/zeppelin/access/Roles.sol	2c85acf184ae36f96ebafd8 f6e26232ea459a711
contracts/zeppelin/access/roles/CapperRol e.sol	c5b388b416565361625c86 a41d14c4148053be2b
contracts/zeppelin/access/roles/MinterRole .sol	81ba1a5f8f3585e6fd7da0b c520cbb61d1ba96f9
contracts/zeppelin/access/roles/PauserRol e.sol	eac20163f361a7362b520d1 b0da3e638cf19b63b
contracts/zeppelin/access/roles/SignerRol e.sol	0d6c043d90f3b47361c169 947c1cd7bf5842ea73
contracts/zeppelin/access/roles/WhitelistAdminRole.sol	db13ff3d51ba7d7055bdad6 30e7c7677a3592c77
contracts/zeppelin/access/roles/Whiteliste dRole.sol	adf6a7f1fc136aa63e0d31a2 c36422d540b0c65f
ntracts/zeppelin/crowdsale/Crowdsale.s	9b929f34f8c7db0b20d528 c8fee2ca5d66502d9a

File Name	SHA-1 Hash
contracts/zeppelin/crowdsale/distribution/ FinalizableCrowdsale.sol	d4edf528c6aa439a08a5a0 e0f92463c0662b8538
contracts/zeppelin/crowdsale/distribution/ PostDeliveryCrowdsale.sol	c2ea0fe336ddd0b66803d 0dd2849cbd6020f64d6
contracts/zeppelin/crowdsale/distribution/ RefundableCrowdsale.sol	34f79575607b323d9e773d b58b83efa233b653a0
contracts/zeppelin/crowdsale/distribution/ RefundablePostDeliveryCrowdsale.sol	a46bf27427e2f2821925f810 7731f5a20f2c5642
contracts/zeppelin/crowdsale/emission/All owanceCrowdsale.sol	3eef5da8f50519e61c4a688 a65ebce5d4197932e
contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol	6e9c7fae7f84ecb25eda1f4 874db98cd2ce622c1
contracts/zeppelin/crowdsale/price/Increa singPriceCrowdsale.sol	323bf9fee7e541f27bc3dd6 802b501cffe2f6875
contracts/zeppelin/crowdsale/validation/C appedCrowdsale.sol	bac0582e3d142ab6bcd262 1394c7c39d9deee338
contracts/zeppelin/crowdsale/validation/In dividuallyCappedCrowdsale.sol	1475fb9401a71f65e06e0a0 b6874aa52f001b8f3
contracts/zeppelin/crowdsale/validation/PausableCrowdsale.sol	f363c66635ca748b976a57 72503c83ce2220b7d3
contracts/zeppelin/crowdsale/validation/Ti medCrowdsale.sol	3348207385ff898a06f73c 90719c6cb94eaa5616
contracts/zeppelin/crowdsale/validation/W hitelistCrowdsale.sol	54e5b7619d2f5f532ce2ada 4b9cfdb81926fbef3
contracts/zeppelin/cryptography/ECDSA.s ol	76a85bee5b53d94cbbb27 cf2e64d093e63fbf383
contracts/zeppelin/cryptography/MerklePr oof.sol	9cf3346b959339f76bbedf 4fdd7eb4c89f9d708b
ntracts/zeppelin/drafts/Counters.sol	9afb0abd3c2203bdebfb0 99ba312ae1aa3491ef1

File Name	SHA-1 Hash
contracts/zeppelin/drafts/ERC1046/ERC20 Metadata.sol	90bd87618009ef859d604 2e9f9652b7d381a88b6
contracts/zeppelin/drafts/ERC20Migrator.s ol	7b276d54e8b48abd3e6f6a 1dce3f2bc6dace7559
contracts/zeppelin/drafts/ERC20Snapshot.	2d87241a7d52337394b145f 0aa2e4492386e9353
contracts/zeppelin/drafts/SignatureBounce r.sol	8688cb091305ac4c9223d d0c279a193d415c19ae
contracts/zeppelin/drafts/SignedSafeMath.	cbb5a1dd1395fe442f1a65e 7ea363f59024bc568
contracts/zeppelin/drafts/Strings.sol	191552acdf0666a4d5a224 34618f604ac2e78f1a
contracts/zeppelin/drafts/TokenVesting.sol	aae2625bcc1061f910792d6 6448171854c10a12a
contracts/zeppelin/examples/SampleCrowdsale.sol	8a9795357ba9baddbdd08 f89ffa521e5dedb8c56
contracts/zeppelin/examples/SimpleToken. sol	b7cac40dfc7f81f4f3112bdc 05d70cf7f4109b22
contracts/zeppelin/introspection/ERC165.s ol	Offad990866bbae84334c1 99da3beac4b023c40b
contracts/zeppelin/introspection/ERC165C hecker.sol	70e4597cea01643d48b2c 4331a3a1a7ccb6312e5
contracts/zeppelin/introspection/ERC1820I mplementer.sol	ccdcb76ed593fed5d896d 80d5ce2d85494a21ce8
contracts/zeppelin/introspection/IERC165.s ol	3e4132a066a6508ca5d1bd ad1c6aefaf65f0f417
contracts/zeppelin/introspection/IERC1820 Implementer.sol	f5ed2d06bcd8e04750bc0 8298511e24a2c1b18e1
ntracts/zeppelin/introspection/IERC1820 Registry.sol	7043ec16917c1c320773519 e15c0a157b5eb622d

File Name	SHA-1 Hash
contracts/zeppelin/lifecycle/Pausable.sol	b0fa9243a2861ec124501a2 74ff27dc96d62045c
contracts/zeppelin/math/Math.sol	ab515a94d340aa89ddc03 c67e6fc2fdb4b6b3a18
contracts/zeppelin/math/SafeMath.sol	996fa9bc77d307e5841e95 836a6f3e70a47b56dc
contracts/zeppelin/ownership/Ownable.sol	52faef44a79929eb5829b4 4037bd7e6aeb5886a4
contracts/zeppelin/ownership/Secondary.s ol	effa2a1d4e5b89ca9ba0972 a1821efb7c6751301
contracts/zeppelin/payment/PaymentSplitt er.sol	cd09d63330e8fac61c3e31 977d74a62ec05f2b4b
contracts/zeppelin/payment/PullPayment.s ol	6de15ad8c8a87054c03cec 5c87c9ad9e3749b7dd
contracts/zeppelin/payment/escrow/ConditionalEscrow.sol	741bc063096b0d3fe7721d ac32cfcfdfe26bffec
contracts/zeppelin/payment/escrow/Escrow.sol	89814623bf0a582764a7ed 11aca0626bd0497469
contracts/zeppelin/payment/escrow/Refun dEscrow.sol	f356bb993dc108b56b22fb c198bfc1943b83a0c4
contracts/zeppelin/token/ERC20/ERC20.sol	090e794a02cb360fd29f4f ae86cc9beebe8c19fe
contracts/zeppelin/token/ERC20/ERC20Bu rnable.sol	53604981ed22f52fa49276 c7494a01fbd8b5cbba
contracts/zeppelin/token/ERC20/ERC20Ca pped.sol	bec55d19afae1b673fbfa89 a74e0c323d0ac9a65
contracts/zeppelin/token/ERC20/ERC20De tailed.sol	e87b9ea40a0fa3a6a3b61c 0d8b028dd50abd2c17
ntable.sol	9702a8bc622ecd20754103 e90f2624d69a657ff0

File Name	SHA-1 Hash
contracts/zeppelin/token/ERC20/ERC20Pa usable.sol	9c2bdb2452c4b5424cb55 278b87d2855dd1ab954
contracts/zeppelin/token/ERC20/IERC20.s ol	071386690ad9e56d7f22ec 461644611e9f46c531
contracts/zeppelin/token/ERC20/SafeERC2 0.sol	638ff9747c02c5a405a38c 53fcc627066146d5ba
contracts/zeppelin/token/ERC20/TokenTim elock.sol	56ff72e3930bc1ef6f949c5 be41a77b0b4c6f59a
contracts/zeppelin/token/ERC721/ERC721.s ol	14a1fd7b8f9aee634ea1b3d 550ae0f93a32452bf
contracts/zeppelin/token/ERC721/ERC721B urnable.sol	18e971a658a4ceed9f6cd4 aae2a62a19d15b7f21
contracts/zeppelin/token/ERC721/ERC721E numerable.sol	5d56a89a03af60edce202 0f9b5babc35d94a96e9
contracts/zeppelin/token/ERC721/ERC721F ull.sol	004e3919a168f167a21724e 367b14062a80fcce5
contracts/zeppelin/token/ERC721/ERC721H older.sol	9ae70830aa2c02885b90f 254821ba87544b70f51
contracts/zeppelin/token/ERC721/ERC721M etadata.sol	f15e429094d7331c5c83e4 3c919d2b9ac16f994f
contracts/zeppelin/token/ERC721/ERC721M etadataMintable.sol	d79b2f0327909f36781705 3002557994a644d7c8
contracts/zeppelin/token/ERC721/ERC721M intable.sol	3e7f8614328532a74bf7e18 89df0f5f94598ad12
contracts/zeppelin/token/ERC721/ERC721P ausable.sol	5781706f3e601b9dd04e89 b036980438e0e1c000
contracts/zeppelin/token/ERC721/IERC721.s ol	a031de37de0bdcd6f65244 2f6d5a98e28ad0bc7b
ntracts/zeppelin/token/ERC721/IERC721E	d68cee9914f8b5b1a6d756 5d77c63d21008ffc0f

File Name			SHA-1	Hash	
contracts/zeppelin/token/ERC721/IERC721F ull.sol			d383b8f1941b7c768ded74 4aa22f1283a82fc0f1		
contracts/zeppelin/token/ERC721/IERC721 Metadata.sol			8be425d35abba3b557053 5d7c517035e001c012d		
contracts/zeppelin/token/ERC721/IERC721R eceiver.sol		259fda3fb13a4dbcde0821e c6f17dd98311486f1			
contracts/ze ol	ppelin/token/E	ERC777/ERC777.s		4f6d1ba87477d5fe7dae32b afe26ff93a140d883	
contracts/zeppelin/token/ERC777/IERC777.			31e168dfd70b2c8d2682cc ed1b204c0a89cd7aa9		
contracts/zeppelin/token/ERC777/IERC777R ecipient.sol			e5cc170671b166d18dad33 6cf09df5dba734c803		
contracts/zeppelin/token/ERC777/IERC777S ender.sol		05af02d35e333afc31602d 0a85d965386b63c06d			
contracts/zeppelin/utils/Address.sol		5e025b5b3244d65ad36df dceca7b968b012a76ed			
contracts/zeppelin/utils/Arrays.sol			3487917d053c7fb108d5e5 de9972dff52405a385		
contracts/ze	ppelin/utils/Re	entrancyGuard.	b419b7ac13283 e269947340ee		
Contract	Туре	Bases			
L	Function Name	Visibility	Mutability	Modifiers	
CreateCall	Implement ation				
L	performCr eate2	Public !		NO	
ldh r	performCr eate	Public .		NO.	

		1100 Conscileys E	9	
Contract	Туре	Bases		
Executor	Implement ation			
L	execute	Internal 🦲		
L	executeCa 	Internal 🦲		
L	executeDe legateCall	Internal 🦲		
Enum	Implement ation			
SecuredT okenTrans fer	Implement ation			
L	transferTo ken	Internal 🦲		
SelfAutho rized	Implement ation			
FallbackM anager	Implement ation	SelfAuthorized		
L	internalSet FallbackHa ndler	Internal 🦲		
L	setFallbac kHandler	Public !		authorized
L		External J	ED	NO.
ModuleMa nager	Implement ation	SelfAuthorized, Executor		
JŶÞ L	setupMod ules	Internal 🦰		

Contract	Туре	Bases	
L	enableMo dule	Public !	authorized
L	disableMo dule	Public !	authorized
L	execTrans actionFro mModule	Public !	NO.
L	getModule s	Public !	NO.
OwnerMa nager	Implement ation	SelfAuthorized	
L	setupOwn ers	Internal 🦲	
L	addOwner WithThres hold	Public !	authorized
L	removeOw ner	Public !	authorized
L	swapOwn er	Public !	authorized
L	changeThr eshold	Public !	authorized
L	getThresh old	Public !	NO.
L	isOwner	Public 🌡	NO
L	getOwner s	Public !	NO
MasterCo py	Implement ation	SelfAuthorized	

		nco consensys i	-	
Contract	Туре	Bases		
L	changeMa sterCopy	Public		authorized
Module	Implement ation	MasterCopy		
L	setManage r	Internal 🦲		
Signature Decoder	Implement ation			
L	recoverKe y	Internal 🦰		
L	signatureS plit	Internal 🦲		
SafeMath	Library			
L	mul	Internal 🦰		
L	div	Internal 🦲		
L	sub	Internal 🦲		
L	add	Internal 🦲		
L	mod	Internal 🦰		
ISignature ValidatorC onstants	Implement ation			



Contract	Туре	Bases	
GnosisSaf e	Implement ation	MasterCopy, ModuleManager, OwnerManager, SignatureDecod er, SecuredTokenTr ansfer, ISignatureValidat orConstants, FallbackManager	
L	setup	External J	NO
L	execTrans action	External .	NO.
L	handlePay ment	Private 🖺	
L	checkSign atures	Internal 🦲	
L	requiredTx Gas	External J	authorized
L	approveHa sh	External J	NO.
L	signMessa ge	External J	authorized
L	isValidSign ature	External J	NO
L	getMessag eHash	Public	NO.
L	encodeTra nsactionD ata	Public !	NO.

Sign

Contract	Туре	Bases		
L	getTransa ctionHash	Public		NO
ISignature Validator	Implement ation	ISignatureValidat orConstants		
L	isValidSign ature	Public		NO
Migration s	Implement ation			
Reversible ICO	Implement ation	IERC777Recipien t		
L		Public		NO
L	init	Public [onlyDeplo yingAddre ss isNotInitial ized
L		External J	UD	isInitialize d isNotFroze n
L	tokensRec eived	External J		isInitialize d isNotFroze n
L	commit	External !	uъ	isInitialize d isNotFroze n isRunning

Jih

Contract	Туре	Bases		
L	cancel	External J	uр	isInitialize d isNotFroze n
L	whitelist	External J		onlyWhitel istingAddr ess isInitialize d isNotFroze n isRunning
L	projectWit hdraw	External J		onlyProjec tAddress isInitialize d isNotFroze n
L	freeze	External J		onlyFreeze rAddress isNotFroze n
L	unfreeze	External J		onlyFreeze rAddress isFrozen
L	disableEsc apeHatch	External J		onlyFreeze rAddress isNotFroze n
L	escapeHat ch	External .		onlyRescu erAddress isFrozen

Contract	Туре	Bases	
L	getUnlock edProjectE TH	Public !	NO.
L	getAvailab leProjectE TH	Public !	NO.
L	getParticip antReserv edTokens	Public !	NO.
L	getParticip antUnlock edTokens	Public !	NO.
L	getCurrent Stage	Public	NO.
L	getCurrent Price	Public	NO
L	getPriceAt Block	Public	NO.
L	getPriceAt Stage	Public	NO
L	getStageA tBlock	Public	NO.
L	committab leEthAtSta ge	Public !	NO.
L	getTokenA mountForE thAtStage	Public !	NO.



Contract	Туре	Bases	
L	getEthAm ountForTo kensAtSta ge	Public !	NO.
L	getCurrent BlockNum ber	Public !	NO.
L	calcUnlock edAmount	Public !	NO.
L	sanityChe ckProject	Internal 🦲	
L	sanityChe ckParticip ant	Internal 🦲	
L	calcProjec tAllocation	Internal 🦲	
L	calcPartici pantAlloca tion	Internal 🦲	
L	cancelPen dingContri butions	Internal 🦲	isInitialize d isNotFroze n
L	acceptCon tributions	Internal 🦲	isInitialize d isNotFroze n isRunning



	_		
Contract	Туре	Bases	
L	withdraw	Internal 🦲	isInitialize d isNotFroze n isRunning
Reversible ICO	Interface		
L	getParticip antReserv edTokens	External J	NO.
RicoToken	Implement ation	ERC777	
L		Public	ERC777
L	setup	Public !	requireNot Initialized onlyManag er
L	changeMa nager	Public [onlyManag er
L	setFrozen	Public !	onlyManag er
L	getLocked Balance	Public	NO.
L	getUnlock edBalance	Public !	NO.
L	_burn	Internal 🦲	requireNot Frozen



Contract	Туре	Bases	
L	_move	Internal 🦲	requireNot Frozen requireIniti alized
ERC777M ock	Implement ation	ERC777	
L		Public	ERC777
L	mintIntern al	Public [NO.
ERC777Se nderRecip ientMock	Implement ation	IERC777Sender, IERC777Recipien t, ERC1820Implem enter	
L	tokensToS end	External J	NO
L	tokensRec eived	External J	NO
L	senderFor	Public	NO
L	registerSe nder	Public	NO.
L	recipientF or	Public	NO
L	registerRe cipient	Public	NO.
L	setShould RevertSen d	Public !	NO.



Contract	Туре	Bases	
L	setShould RevertRec eive	Public !	NO.
L	send	Public !	NO
L	burn	Public	NO
EmptyRec eiver	Implement ation		
MathMock	Implement ation		
L	max	Public .	NO
L	min	Public !	NO
L	average	Public	NO
Reversible ICOMock	Implement ation	ReversibleICO	
L	getCurrent BlockNum ber	Public !	NO.
L	increaseC urrentBloc kNumber	Public !	NO.
L	jumpToBlo ckNumber	Public	NO.
Reversible ICOMock7 77	Implement ation	ReversibleICOM ock	
JÅ L	setreserve dTokenAm ount	External J	NO.

Contract	Туре	Bases	
L	getParticip antReserv edTokens	Public [NO.
L	tokensRec eived	External J	NO.
SafeMath Mock	Implement ation		
L	mul	Public 🛭	NO
L	div	Public 🛭	NO
L	sub	Public 🛭	NO
L	add	Public 🛭	NO
L	mod	Public 🛚	NO
Roles	Library		
L	add	Internal 🦲	
L	remove	Internal 🦲	
L	has	Internal 🦲	
CapperRol e	Implement ation		
L		Internal 🦲	
L	isCapper	Public 🌡	NO
L	addCappe r	Public	onlyCappe r
L	renounce Capper	Public [NO.
L JŶ	_addCapp er	Internal 🦲	

Contract	Туре	Bases	
L	_removeC apper	Internal 🦺	
MinterRol e	Implement ation		
L		Internal 🦲	
L	isMinter	Public .	NO
L	addMinter	Public .	onlyMinter
L	renounce Minter	Public !	NO
L	_addMinte r	Internal 🖲	
L	_removeMi nter	Internal 🦺	
PauserRol e	Implement ation		
L		Internal 🦲	
L	isPauser	Public	NO
L	addPauser	Public .	onlyPauser
L	renounceP auser	Public !	NO
L	_addPause r	Internal 🖲	
L	_removePa user	Internal 🦺	
SignerRol e	Implement ation		
J L		Internal 🦲	

Contract	Туре	Bases	
L	isSigner	Public 🌡	NO
L	addSigner	Public 🌡	onlySigner
L	renounceS igner	Public .	NO
L	_addSigne r	Internal 🦲	
L	_removeSi gner	Internal 🦲	
WhitelistA dminRole	Implement ation		
L		Internal 🦲	
L	isWhitelist Admin	Public	NO
L	addWhiteli stAdmin	Public	onlyWhitel istAdmin
L	renounce WhitelistA dmin	Public !	NO
L	_addWhitel istAdmin	Internal 🦲	
L	_removeW hitelistAd min	Internal 🦰	
Whiteliste dRole	Implement ation	WhitelistAdminR ole	
L	isParticipa ntWhitelist ed	Public	NO

Contract	Туре	Bases		
L	addWhiteli sted	Public		onlyWhitel istAdmin
L	removeWh itelisted	Public !		onlyWhitel istAdmin
L	renounce Whiteliste d	Public !		NO.
L	_addWhitel isted	Internal 🦲		
L	_removeW hitelisted	Internal 🦰		
Crowdsale	Implement ation	ReentrancyGuar d		
L		Public 🌡		NO
L		External J	SP	NO
L	token	Public		NO
L	wallet	Public 🌡		NO
L	rate	Public 🌡		NO.
L	weiRaised	Public 🌡		NO.
L	buyTokens	Public .	<u>u</u> D	nonReentr ant
L	_preValidat ePurchase	Internal 🦲		
L	_postValid atePurcha se	Internal 🦲		
L JŶ	_deliverTok ens	Internal 🦲		

Contract	Туре	Bases	
L	_processP urchase	Internal 🦲	
L	_updatePu rchasingSt ate	Internal 🦲	
L	_getToken Amount	Internal 🦲	
L	_forwardFu nds	Internal 🦲	
Finalizable Crowdsale	Implement ation	TimedCrowdsale	
L		Internal 🦲	
L	finalized	Public [NO
L	finalize	Public	NO
L	_finalizatio n	Internal 🦲	
PostDelive ryCrowds ale	Implement ation	TimedCrowdsale	
L		Public !	NO
L	withdrawT okens	Public	NO.
L	balanceOf	Public [NO
L	_processP urchase	Internal 🦰	
unstableT kenVault	Implement ation	Secondary	

Contract	Туре	Bases	
L	transfer	Public !	onlyPrimar y
Refundabl eCrowdsal e	Implement ation	FinalizableCrowd sale	
L		Public 🌡	NO
L	goal	Public 🌡	NO
L	claimRefu nd	Public .	NO.
L	goalReach ed	Public	NO.
L	_finalizatio n	Internal 🦰	
L	_forwardFu nds	Internal 🦰	
Refundabl ePostDeliv eryCrowd sale	Implement ation	RefundableCrow dsale, PostDeliveryCro wdsale	
L	withdrawT okens	Public 【	NO.
Allowance Crowdsale	Implement ation	Crowdsale	
L		Public	NO
L	tokenWalle t	Public	NO.
J P L	remaining Tokens	Public	NO

NO
NO.
NO
NO
NO
NO.
NO.
NO.



Contract	Туре	Bases	
Individuall yCappedC rowdsale	Implement ation	Crowdsale, CapperRole	
L	setCap	External J	onlyCappe r
L	getCap	Public 🌡	NO
L	getContrib ution	Public	NO.
L	_preValidat ePurchase	Internal 🦲	
L	_updatePu rchasingSt ate	Internal 🦲	
PausableC rowdsale	Implement ation	Crowdsale, Pausable	
L	_preValidat ePurchase	Internal 🦲	whenNotP aused
TimedCro wdsale	Implement ation	Crowdsale	
L		Public 🌡	NO
L	openingTi me	Public !	NO.
L	closingTim e	Public !	NO.
L	isOpen	Public 🌡	NO
L	hasClosed	Public 🌡	NO
L JŶ	_preValidat ePurchase	Internal 🦰	onlyWhile Open

// 10 Z0:04		1100 Consciloys L	3	
Contract	Туре	Bases		
L	_extendTi me	Internal 🦲		
WhitelistC rowdsale	Implement ation	WhitelistedRole, Crowdsale		
L	_preValidat ePurchase	Internal 🦲		
ECDSA	Library			
L	recover	Internal 🦲		
L	toEthSigne dMessage Hash	Internal 🦰		
MerklePro of	Library			
L	verify	Internal 🦲		
Counters	Library			
L	current	Internal 🦲		
L	increment	Internal 🦲		
L	decrement	Internal 🦰		
ERC20Me tadata	Implement ation			
L		Public .		NO
L	tokenURI	External J		NO
L	_setToken URI	Internal 🦰		
C20Mig rator	Implement ation			

Contract	Туре	Bases	
L		Public 🌡	NO
L	legacyTok en	Public	NO.
L	newToken	Public [NO
L	beginMigr ation	Public .	NO
L	migrate	Public 🛭	NO
L	migrateAll	Public .	NO
ERC20Sna pshot	Implement ation	ERC20	
L	snapshot	Public !	NO
L	balanceOf At	Public	NO
L	totalSuppl yAt	Public	NO
L	_transfer	Internal 🦲	
L	_mint	Internal 🦲	
L	_burn	Internal 🦲	
L	_valueAt	Private 😷	
L	_updateAc countSnap shot	Private 傄	
L	_updateTot alSupplyS napshot	Private 傄	
L SP\$	_updateSn apshot	Private 傄	

			_	
Contract	Туре	Bases		
L	_lastSnaps hotId	Private 🖺		
Signature Bouncer	Implement ation	SignerRole		
L		Internal 🦲		
L	_isValidSig nature	Internal 🦲		
L	_isValidSig natureAnd Method	Internal 🦲		
L	_isValidSig natureAnd Data	Internal 🦲		
L	_isValidDat aHash	Internal 🦰		
SignedSaf eMath	Library			
L	mul	Internal 🦲		
L	div	Internal 🦲		
L	sub	Internal 🦲		
L	add	Internal 🦲		
Strings	Library			
L	fromUint2 56	Internal 🦲		
TokenVest ing	Implement ation	Ownable		
β [†] Γ		Public 🌡		NO

Contract	Type	Bases	
L	beneficiar y	Public	NO
L	cliff	Public	NO
L	start	Public	NO
L	duration	Public	NO
L	revocable	Public	NO
L	released	Public	NO
L	revoked	Public .	NO
L	release	Public	NO
L	revoke	Public	onlyOwner
L	_releasable Amount	Private 😷	
L	_vestedAm ount	Private 🖺	
SampleCr owdsaleTo ken	Implement ation	ERC20Mintable, ERC20Detailed	
L		Public	ERC20Det ailed
SampleCr owdsale	Implement ation	CappedCrowdsa le, RefundableCrow dsale, MintedCrowdsal e	



Contract	Туре	Bases	
L		Public !	Crowdsale CappedCr owdsale TimedCro wdsale Refundabl eCrowdsal e
SimpleTok en	Implement ation	ERC20, ERC20Detailed	
L		Public	ERC20Det ailed
ERC165	Implement ation	IERC165	
L		Internal 🦲	
L	supportsIn terface	External J	NO
L	_registerIn terface	Internal 🦲	
ERC165Ch ecker	Library		
L	_supportsE RC165	Internal 🦰	
L	_supportsl nterface	Internal 🦰	
L	_supports AllInterfac es	Internal 🦰	



		1100 Consciloys E	•	
Contract	Туре	Bases		
L	_supportsE RC165Inter face	Private 傄		
L	_callERC16 5Supportsl nterface	Private 傄		
ERC1820I mplement er	Implement ation	IERC1820Implem enter		
L	canImple mentInterf aceForAdd ress	External J		NO.
L	_registerIn terfaceFor Address	Internal 🦰		
IERC165	Interface			
L	supportsIn terface	External J		NO
IERC1820I mplement er	Interface			
L	canImple mentInterf aceForAdd ress	External J		NO I
IERC1820 Registry	Interface			
JŶÞ L	setManage r	External J		NO.

Contract	Туре	Bases	
L	getManag er	External J	NO
L	setInterfac eImpleme nter	External J	NO.
L	getInterfa ceImplem enter	External J	NO.
L	interfaceH ash	External .	NO.
L	updateER C165Cach e	External J	NO.
L	implement sERC165In terface	External J	NO.
L	implement sERC165In terfaceNo Cache	External J	NO
Pausable	Implement ation	PauserRole	
L		Internal 🦲	
L	paused	Public [NO
L	pause	Public <mark>.</mark>	onlyPauser whenNotP aused
L JŶ	unpause	Public !	onlyPauser whenPaus ed

Contract	Туре	Bases	
Math	Library		
L	max	Internal 🦲	
L	min	Internal 🦲	
L	average	Internal 🦰	
SafeMath	Library		
L	add	Internal 🦲	
L	sub	Internal 🦲	
L	mul	Internal 🦲	
L	div	Internal 🦲	
L	mod	Internal 🦰	
Ownable	Implement ation		
L		Internal 🦲	
L	owner	Public	NO
L	isOwner	Public	NO
L	renounce Ownership	Public .	onlyOwner
L	transferO wnership	Public .	onlyOwner
L	_transferO wnership	Internal 🦰	
Secondar y	Implement ation		
L		Internal 🦲	
JŶ\$ L	primary	Public .	NO

Contract	Туре	Bases		
L	transferPri mary	Public [onlyPrimar y
PaymentS plitter	Implement ation			
L		Public 🌡	S D	NO
L		External J	SP	NO
L	totalShare s	Public 【		NO.
L	totalReleas ed	Public 🛚		NO.
L	shares	Public 🌡		NO
L	released	Public 🌡		NO
L	payee	Public 🌡		NO
L	release	Public 🌡		NO
L	_addPayee	Private 🥙		
PullPayme nt	Implement ation			
L		Internal 🦲		
L	withdrawP ayments	Public		NO.
L	payments	Public 🌡		NO
L	_asyncTran sfer	Internal 🦰		
Condition alEscrow	Implement ation	Escrow		
JŶÞ L	withdrawal Allowed	Public 🌡		NO.

Contract	Туре	Bases		
L	withdraw	Public 🌡		NO
Escrow	Implement ation	Secondary		
L	depositsOf	Public 🛚		NO
L	deposit	Public !	яЪ	onlyPrimar y
L	withdraw	Public		onlyPrimar y
RefundEsc row	Implement ation	ConditionalEscro w		
L		Public 🛭		NO
L	state	Public !		NO
L	beneficiar y	Public 🌡		NO
L	deposit	Public	SP	NO
L	close	Public 🌡		onlyPrimar y
L	enableRef unds	Public !		onlyPrimar y
L	beneficiar yWithdraw	Public !		NO
L	withdrawal Allowed	Public !		NO.
ERC20	Implement ation	IERC20		
JÅ L	totalSuppl y	Public		NO.

0/19 23:34		rico Consensys L	
Contract	Туре	Bases	
L	balanceOf	Public 🌡	NO
L	transfer	Public 🌡	NO
L	allowance	Public 🌡	NO
L	approve	Public 🌡	NO
L	transferFro m	Public	NO.
L	increaseAll owance	Public	NO.
L	decreaseA Ilowance	Public .	NO.
L	_transfer	Internal 🦲	
L	_mint	Internal 🦲	
L	_burn	Internal 🦲	
L	_approve	Internal 🦲	
L	_burnFrom	Internal 🦲	
ERC20Bur nable	Implement ation	ERC20	
L	burn	Public 🌡	NO
L	burnFrom	Public 🛭	NO
ERC20Ca pped	Implement ation	ERC20Mintable	
L		Public 🌡	NO
L	cap	Public 🌡	NO
L	_mint	Internal 🦰	
RC20Det ailed	Implement ation	IERC20	

Contract	Туре	Bases	
L		Public 🛮	NO
L	name	Public 🌡	NO
L	symbol	Public	NO
L	decimals	Public .	NO
ERC20Min table	Implement ation	ERC20, MinterRole	
L	mint	Public !	onlyMinter
ERC20Pau sable	Implement ation	ERC20, Pausable	
L	transfer	Public	whenNotP aused
L	transferFro m	Public !	whenNotP aused
L	approve	Public	whenNotP aused
L	increaseAll owance	Public	whenNotP aused
L	decreaseA Ilowance	Public .	whenNotP aused
IERC20	Interface		
L	totalSuppl y	External J	NO.
L	balanceOf	External !	NO
L	transfer	External J	NO
L	allowance	External .	NO
JPP L	approve	External !	NO

		1100 Consency of	
Contract	Туре	Bases	
L	transferFro m	External J	NO
SafeERC2 0	Library		
L	safeTransf er	Internal 🦲	
L	safeTransf erFrom	Internal 🦲	
L	safeAppro ve	Internal 🦲	
L	safeIncrea seAllowan ce	Internal 🦲	
L	safeDecre aseAllowa nce	Internal 🦲	
L	callOption alReturn	Private 🤔	
TokenTim elock	Implement ation		
L		Public 🌡	NO
L	token	Public 🌡	NO
L	beneficiar y	Public [NO.
L	releaseTim e	Public 🛚	NO.
L	release	Public 🌡	NO
101			



Contract	Туре	Bases	
ERC721	Implement ation	ERC165, IERC721	
L		Public	NO
L	balanceOf	Public !	NO
L	ownerOf	Public !	NO
L	approve	Public !	NO
L	getApprov ed	Public .	NO.
L	setApprov alForAll	Public	NO.
L	isApprove dForAll	Public .	NO.
L	transferFro m	Public	NO.
L	safeTransf erFrom	Public	NO.
L	safeTransf erFrom	Public	NO.
L	_exists	Internal 🦲	
L	_isApprove dOrOwner	Internal 🦲	
L	_mint	Internal 🦲	
L	_burn	Internal 🦲	
L	_burn	Internal 🦲	
L	_transferFr om	Internal 🦲	



		·	
Contract	Туре	Bases	
L	_checkOn ERC721Rec eived	Internal 🦲	
L	_clearAppr oval	Private 🖺	
ERC721Bu rnable	Implement ation	ERC721	
L	burn	Public !	NO
ERC721En umerable	Implement ation	ERC165, ERC721, IERC721Enumera ble	
L		Public	NO
L	tokenOfO wnerByInd ex	Public !	NO.
L	totalSuppl y	Public	NO.
L	tokenByIn dex	Public	NO
L	_transferFr om	Internal 🦲	
L	_mint	Internal 🦲	
L	_burn	Internal 🦲	
L	_tokensOf Owner	Internal 🦲	
L	_addToken ToOwnerE numeratio n	Private 傄	

Contract	Туре	Bases	
L	_addToken ToAllToken sEnumerat ion	Private 傄	
L	_removeTo kenFromO wnerEnum eration	Private 🖺	
L	_removeTo kenFromAl ITokensEn umeration	Private 傄	
ERC721Ful	Implement ation	ERC721, ERC721Enumera ble, ERC721Metadata	
L		Public [ERC721Me tadata
ERC721Ho Ider	Implement ation	IERC721Receiver	
L	onERC721 Received	Public !	NO
ERC721Me tadata	Implement ation	ERC165, ERC721, IERC721Metadat a	
L		Public	NO.
L	name	External J	NO
L	symbol	External J	NO
lih r	tokenURI	External J	NO.

Contract	Туре	Bases	
L	_setToken URI	Internal 🦲	
L	_burn	Internal 🦰	
ERC721Me tadataMin table	Implement ation	ERC721, ERC721Metadata , MinterRole	
L	mintWithT okenURI	Public !	onlyMinter
ERC721Mi ntable	Implement ation	ERC721, MinterRole	
L	mint	Public !	onlyMinter
ERC721Pa usable	Implement ation	ERC721, Pausable	
L	approve	Public [whenNotP aused
L	setApprov alForAll	Public [whenNotP aused
L	transferFro m	Public	whenNotP aused
IERC721	Implement ation	IERC165	
L	balanceOf	Public 🛭	NO
L	ownerOf	Public [NO
L	safeTransf erFrom	Public !	NO
L JŶ	transferFro m	Public	NO

Contract	Туре	Bases	
L	approve	Public 🌡	NO
L	getApprov ed	Public [NO.
L	setApprov alForAll	Public .	NO.
L	isApprove dForAll	Public	NO.
L	safeTransf erFrom	Public !	NO.
IERC721En umerable	Implement ation	IERC721	
L	totalSuppl y	Public	NO.
L	tokenOfO wnerByInd ex	Public [NO
L	tokenByIn dex	Public !	NO
IERC721Fu II	Implement ation	IERC721, IERC721Enumera ble, IERC721Metadat a	
IERC721M etadata	Implement ation	IERC721	
L	name	External !	NO
L	symbol	External J	NO
JÅ L	tokenURI	External J	NO

Contract	Туре	Bases	
IERC721Re ceiver	Implement ation		
L	onERC721 Received	Public !	NO
ERC777	Implement ation	IERC777, IERC20	
L		Public	NO
L	name	Public [NO
L	symbol	Public [NO
L	decimals	Public .	NO
L	granularity	Public	NO
L	totalSuppl y	Public	NO.
L	balanceOf	Public [NO
L	send	External J	NO
L	transfer	External J	NO
L	burn	External .	NO
L	isOperator For	Public !	NO.
L	authorize Operator	External J	NO.
L	revokeOpe rator	External .	NO.
L	defaultOp erators	Public !	NO.
L IPI	operatorS end	External J	NO

Contract	Туре	Bases	
L	operatorB urn	External J	NO
L	allowance	Public	NO
L	approve	External J	NO
L	transferFro m	External J	NO.
L	_mint	Internal 🦲	
L	_send	Private 🦺	
L	_burn	Internal 🦲	
L	_move	Internal 🦲	
L	_approve	Private 🦺	
L	_callToken sToSend	Private 🖺	
L	_callToken sReceived	Private 🖺	
IERC777	Interface		
L	name	External J	NO
L	symbol	External J	NO
L	granularity	External J	NO
L	totalSuppl y	External J	NO
L	balanceOf	External J	NO
L	send	External !	NO
L	burn	External !	NO
L L	isOperator For	External J	NO

Contract	Туре	Bases	
L	authorize Operator	External J	NO
L	revokeOpe rator	External !	NO
L	defaultOp erators	External !	NO
L	operatorS end	External !	NO
L	operatorB urn	External [NO.
IERC777R ecipient	Interface		
L	tokensRec eived	External [NO
IERC777S ender	Interface		
L	tokensToS end	External [NO
Address	Library		
L	isContract	Internal 🦲	
L	toPayable	Internal 🦲	
Arrays	Library		
L	findUpper Bound	Internal 🦲	
Reentranc yGuard	Implement ation		
L		Internal 🦲	

Legend

Symbol	Meaning
	Function can modify state
54 1	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 wa
 Running all tests in "test/js_validator_tests" folder:
______
You can improve web3's peformance when running Node.js versions older than 1
  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

√ 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 476.190476190476 tokens

    stage 6

√ should return 384.615384615384 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, precisionPc
  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 =
        √ should return 0
      after range => _currentBlock = 101, _startBlock = 1, _endBlock =
```

ββ

```
√ should return 1
  _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 =
        √ should return 0
      after range => _currentBlock = 101, _startBlock = 1, _endBlock =
        √ should return 1
getParticipantReservedTokensAtBlock(_tokenAmount, _blockNumber, precis
  _blockNumber in range
    _tokenAmount = 100, _blockNumber = startBlock
      √ should return 99
    _{\text{tokenAmount}} = 100, _{\text{blockNumber}} = (range * 0.25) - 1
      √ should return 75
    _tokenAmount = 100, _blockNumber = (range * 0.50) - 1 ( middle of
      √ 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, pre
  _blockNumber in range
    _tokenAmount = 100, _blockNumber = startBlock
      √ should return 1
    _{\text{tokenAmount}} = 100, _{\text{blockNumber}} = (range * 0.25) - 1
      √ should return 25
    _tokenAmount = 100, _blockNumber = (range * 0.50) - 1 ( middle of
      √ should return 50
    _{\text{tokenAmount}} = 100, _{\text{blockNumber}} = (range * 0.75) - 1
      √ should return 75
    _tokenAmount = 100, _blockNumber = endBlock
      √ should return 100
```



```
_biockitaliber 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 )
      \sqrt{\text{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 )
      \sqrt{\text{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

        √ 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[stageCour]

√ should return stageCount when called using using stage[stageCour
      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 committed value

      ParticipantRecord

√ contributions increases by 1

√ totalSentETH increases by committed 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 committed 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 committed value

      ParticipantRecord
        √ contributions increases by 1

√ totalSentETH increases by committed 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 committed value

√ returnedETH does not change
```



 \checkmark 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 committed value

ParticipantRecord

- √ contributions increases by 1
- √ totalSentETH increases by committed 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 committed 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 committed value

ParticipantRecord

- \checkmark contributions increases by 1
- √ totalSentETH increases by committed value
- √ returnedETH does not change
- √ withdrawnETH does not change
- √ allocatedETH does not change



- rICO | ConsenSys Diligence √ returnedTokens does not change √ committedETH does not change √ boughtTokens does not change √ pendingTokens increases by getTokenAmountForEthAtStage(value) currentStageRecord √ totalSentETH increases by committed 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 cor 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 committed value ParticipantRecord √ contributions increases by 1 √ totalSentETH increases by committed 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 committed value √ returnedETH does not change √ committedETH increases by commit value √ withdrawnETH does not change
- Jih

- √ 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 committed value

ParticipantRecord

- √ contributions increases by 1
- √ totalSentETH increases by committed 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 committed 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
- √ committedFTH increases by commit value



Tokens:

- ✓ Participant token balance is oldState.ParticipantRecord.pend
- ✓ 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 committed value

ParticipantRecord

- √ contributions increases by 1
- √ totalSentETH increases by committed 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 committed 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

/ whitaliated in folia

```
    ∧ MIIITETIZIEN IZ LATZE

          cancelContributionsForAddress()
            Contract:

√ committedETH does not change

              √ returnedETH increases by oldState.ParticipantAvailableETH va
            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.ParticipantAvaila
              √ Participant ETH balance increases by oldState.ParticipantAva
  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 wa
 Running all tests in "test" folder:
You can improve web3's peformance when running Node.js versions older than 1
You can improve web3's peformance when running Node.js versions older than 1
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
```

```
rICO | ConsenSys Diligence
> 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
> Compiling ./contracts/zeppelin/crowdsale/distribution/PostDeliveryCrowdsal
> Compiling ./contracts/zeppelin/crowdsale/distribution/RefundableCrowdsale.
> Compiling ./contracts/zeppelin/crowdsale/distribution/RefundablePostDelive
> Compiling ./contracts/zeppelin/crowdsale/emission/AllowanceCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/emission/MintedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/price/IncreasingPriceCrowdsale.sc
> Compiling ./contracts/zeppelin/crowdsale/validation/CappedCrowdsale.sol
> Compiling ./contracts/zeppelin/crowdsale/validation/IndividuallyCappedCrow
> 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/cont
> Compiled successfully using:
   - solc: 0.5.17+commit.d19bba13.Emscripten.clang
You can improve web3's peformance when running Node.js versions older than 1
  _____
  Step 1 - Setting up helpers and globals
 Step 2 - Run tests
Current Block: 11
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
 10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
 xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
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:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block: 14
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 15
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: CONTRIBUTE 1
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3
Current Block: 16
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
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:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: 8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 19
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: CONTRIBUTE 1
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 20
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                  6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 21
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  6
  :10a0717595A97A777F51f3ae542d4312edfD20FA Task:
 xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
```

0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: PROJECT WITHDRAW 3

```
Current Block:
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:
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:
Current Block: 37
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  6
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 38
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  0
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
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
9x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
                                                  5
  rrent Block: 41
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0v10a0717505A07A777E51f2ac5A2dA212adfD20EA Tack.
```

```
UXIUdU/I/JYJAY/A///FJIIJdeJ4ZU4JIZEUIJZUFA Id5K.
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 8
Current Block: 42
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 43
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                9
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 4
Current Block: 44
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 7
0xeF6DCBB32a3263d35185993B608843F7A65e90f5 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:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 7
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 47
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                 8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                 a
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 48
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                 8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
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:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
 x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
  rrent Block: 51
```

```
Ux1UaU/1/595A9/A///F51t3ae542d4312edtD2UFA lask:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
                                                  9
Current Block: 52
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 53
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 9
Current Block: 54
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 6
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 6
Current Block: 55
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 56
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 57
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 58
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
                                                  7
Current Block: 59
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: 4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 60
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                  0
 k920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
 arrent Block: 61
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
```

```
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block: 62
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: 4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 4
0xeF6DCBB32a3263d35185993B608843F7A65e90f5 Task: 4
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block: 63
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843F7A65e90f5 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:
Current Block: 66
0x668d51FD53ee7d1dA66d8Cc9eB0274F0D9634C2F Task: 6
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: 8
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 67
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: CONTRIBUTE 1
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 68
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: WITHDRAW 2
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: 5
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block: 69
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: 7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: WITHDRAW 2
Current Block: 70
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: PROJECT WITHDRAW 3
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: 8
  (920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 4
 urrent Block: 71
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: 5
```

```
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: CONTRIBUTE 1
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: 9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 72
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                 7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                 a
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
                                                 9
Current Block: 73
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                 5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block: 74
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: PROJECT WITHDRAW 3
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: 5
Current Block: 75
0x668d51FD53ee7d1dA66d8Cc9eB0274F0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block: 76
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                 a
                                                 7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
                                                 9
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
                                                 5
Current Block: 77
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                 4
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
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:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
 urrent Block: 81
```

0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: 0

```
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 82
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  7
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task: WITHDRAW 2
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 83
0x668d51FD53ee7d1dA66d8Cc9eB0274F0D9634C2F Task:
                                                  0
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
                                                  5
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 84
0x668d51FD53ee7d1dA66d8Cc9eB0274F0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task: CONTRIBUTE 1
Current Block: 85
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task: PROJECT WITHDRAW 3
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: 0
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 86
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task: WITHDRAW 2
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c Task:
Current Block: 87
0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Task:
                                                  8
0x10a0717595A97A777F51f3ae542d4312edfD20FA Task:
0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Task:
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)

    mu1
      ✓ multiplies correctly (52ms)

√ multiplies by zero correctly (141ms)

√ reverts on multiplication overflow (47ms)
    div

√ divides correctly (32ms)

      ./ divides zero correctly (26ms)
```

```
A MINIMES VELO COLLECTTÀ (VOILS)
   √ 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
   ✓ Deployer address: 0xa990077c3205cbDf861e17Fa532eeB069cE9fF96 balance
   √ Funds Supplier address: 0xFE6B56FdCF920382Af1493828E79C017EE090F2a k
 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)

       \checkmark 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:
     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
   Project withdraw:
                     59207 GAS
```

```
√ UXFE6B56FdCF9ZU38ZATT4938Z8E/9CUT/EEU9UFZa Project: Withdraws EIH (
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 (**

---> Contribution : 150777 GAS

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (295ms)

Stage: 0, Price: 250000000000000000

√ Jump to the next block: 12 (120ms)

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Return tokens (106ms)

Stage: 0, Price: 250000000000000000
     ✓ Jump to the next block: 13 (115ms)
Stage: 0, Price: 250000000000000000

√ Jump to the next block: 14 (123ms)
---> Contribution : 120777 GAS
      \checkmark 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (290ms)

√ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (25ms)

---> Project withdraw: 59207 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (**

Stage: 0, Price: 25000000000000000

√ Jump to the next block: 15 (145ms)
---> Contribution : 120777 GAS
      \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (250ms)}
---> Project withdraw: 59207 GAS
     ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
Stage: 0, Price: 250000000000000000

√ Jump to the next block: 16 (97ms)
---> Project withdraw: 59207 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
9

Stage: 1, Price: 283333333333333333

√ Jump to the next block: 17 (97ms)

---> Project withdraw: 59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
Stage: 1, Price: 283333333333333333

√ Jump to the next block: 18 (103ms)
---> Contribution : 65455 GAS

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (219ms)

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (17ms)

√ Jump to the next block: 19 (148ms)

√ Jump to the next block: 20 (221ms)

---> Project withdraw: 59207 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
Stage: 1, Price: 283333333333333333

√ Jump to the next block: 21 (100ms)

√ Freeze contract at block 22 (63ms)
Stage: 1, Price: 283333333333333333
```

```
√ Jump to the next block: 22 (99ms)

Stage: 2, Price: 31666666666666666

√ Jump to the next block: 23 (119ms)
√ Jump to the next block: 24 (98ms)

√ Jump to the next block: 25 (85ms)
Stage: 2, Price: 3166666666666666

√ Jump to the next block: 26 (86ms)

√ Jump to the next block: 27 (107ms)

√ Jump to the next block: 28 (130ms)

√ Jump to the next block: 29 (122ms)

√ Jump to the next block: 30 (113ms)

√ Jump to the next block: 31 (104ms)

√ 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)
     \sqrt{0}x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (32ms)
Stage: 0, Price: 250000000000000000

√ Jump to the next block: 38 (123ms)

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (26ms)

✓ Jump to the next block: 39 (131ms)

√ Jump to the next block: 40 (131ms)

Stage: 1, Price: 283333333333333333

√ Jump to the next block: 41 (130ms)

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (26ms)

Stage: 1, Price: 283333333333333333

√ Jump to the next block: 42 (162ms)
---> Project withdraw: 59207 GAS
     ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (2
 age: 1, Price: 283333333333333333

√ Jump to the next block: 43 (166ms)

--> Contribution : 65455 GAS
```

```
\sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5:}} Buy tokens (515ms)

√ Jump to the next block: 44 (180ms)
     \sqrt{0}x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (37ms)
---> Project withdraw: 59207 GAS
    √ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (2

√ Jump to the next block: 45 (198ms)

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (21ms)

√ Jump to the next block: 46 (92ms)

√ Jump to the next block: 47 (89ms)

---> Whitelisting: 276818 GAS
---> Contribution with auto accepting : 185174 GAS

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (1166ms)

√ Jump to the next block: 48 (114ms)

---> Project withdraw: 98129 GAS
     ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (*
---> Whitelisting: 210967 GAS
---> Contribution with auto accepting : 185174 GAS
     \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (994ms)

√ Jump to the next block: 49 (89ms)
---> Contribution with auto accepting : 200351 GAS
    √ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (490ms)

√ Jump to the next block: 50 (87ms)

√ Jump to the next block: 51 (86ms)

√ Jump to the next block: 52 (91ms)
---> Project withdraw: 68129 GAS
    ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
---> Contribution with auto accepting : 200709 GAS
    \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5:}} Buy tokens (492ms)

√ Jump to the next block: 53 (88ms)
---> Project withdraw: 68129 GAS
    ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (

√ Jump to the next block: 54 (78ms)
---> Withdraw: 171420 GAS
     ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (166ms)
✓ Jump to the next block: 55 (87ms)
 age: 3, Price: 34999999999999999

√ Jump to the next block: 56 (86ms)

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (16ms)
```

```
Stage: 4. Price: 38333333333333333

√ Jump to the next block: 57 (78ms)

√ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (13ms)

Stage: 4, Price: 38333333333333333

√ 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 (
9

---> Contribution with auto accepting : 186126 GAS

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (455ms)

---> Contribution with auto accepting : 186126 GAS

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (474ms)

Stage: 4, Price: 38333333333333333

√ 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: 416666666666665

√ Jump to the next block: 63 (81ms)
      \checkmark 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (13ms)
---> Project withdraw: 68129 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (**

---> Project withdraw: 60858 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (*

Stage: 5, Price: 416666666666665

√ Jump to the next block: 64 (87ms)

---> Project withdraw: 68129 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (

Stage: 5, Price: 416666666666665

√ Jump to the next block: 65 (103ms)
---> Project withdraw: 68129 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (

Stage: 5, Price: 416666666666665

√ Jump to the next block: 66 (92ms)

---> Contribution with auto accepting : 186602 GAS
      \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Buy tokens (503ms)}
Stage: 5, Price: 416666666666665

√ Jump to the next block: 67 (88ms)

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Return tokens (14ms)

 --> Contribution with auto accepting : 186602 GAS

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (512ms)

 tage: 5, Price: 41666666666666665
```

/ .lumn to the next block: 68 (89ms)

```
V Jump to the Heat Dion. Of (Johns)
---> Withdraw: 156420 GAS

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Return tokens (228ms)

Stage: 6, Price: 449999999999998

√ Jump to the next block: 69 (85ms)

---> Project withdraw: 68129 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
---> Project withdraw: 60858 GAS
     ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH ({
Stage: 6, Price: 4499999999999998

√ Jump to the next block: 70 (84ms)
---> Whitelisting: 52939 GAS
---> Contribution with auto accepting : 283023 GAS
      \sqrt{0}x10a0717595A97A777F51f3ae542d4312edfD20FA: Buy tokens (543ms)
Stage: 6, Price: 449999999999998

√ Jump to the next block: 71 (82ms)
Stage: 6, Price: 449999999999998

√ Jump to the next block: 72 (83ms)
---> Contribution with auto accepting : 187019 GAS
      \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (515ms)
Stage: 6, Price: 449999999999998

√ Jump to the next block: 73 (92ms)

---> Withdraw: 171420 GAS

√ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (175ms)

---> Project withdraw: 68070 GAS
     ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
Stage: 6, Price: 449999999999998

√ Jump to the next block: 74 (80ms)

---> Contribution with auto accepting : 187019 GAS

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (590ms)

Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 75 (97ms)
Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 76 (99ms)
Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 77 (95ms)

---> Project withdraw: 68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
---> Contribution with auto accepting : 187377 GAS
      \sqrt{0}x10a0717595A97A777F51f3ae542d4312edfD20FA: Buy tokens (463ms)
---> Withdraw: 156297 GAS

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (159ms)

Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 78 (85ms)
---> Whitelisting: 235613 GAS
---> Contribution with auto accepting : 187259 GAS
      \sqrt{0x668d51}FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: Buy tokens (1859ms)
 --> Withdraw: 156361 GAS

√ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (257ms)

  -> Contribution with auto accepting : 187377 GAS
```

```
√ UXEFOULBB3283203Q351859993B008843E/A05890T5: BUY TOKENS (/30MS)

---> Contribution with auto accepting : 187377 GAS
      √ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (799ms)
Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 79 (107ms)
---> Project withdraw: 68129 GAS

√ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (**

---> Contribution with auto accepting : 187377 GAS
      \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (894ms)
Stage: 7, Price: 4833333333333333333

√ Jump to the next block: 80 (101ms)

Stage: 8, Price: 516666666666664
      ✓ Jump to the next block: 81 (98ms)
---> Withdraw: 156356 GAS

√ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: Return tokens (288ms)

Stage: 8, Price: 516666666666664

√ Jump to the next block: 82 (97ms)

Stage: 8, Price: 516666666666664

√ Jump to the next block: 83 (156ms)
---> Contribution with auto accepting : 187853 GAS
      \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (594ms)
Stage: 8, Price: 5166666666666664

√ Jump to the next block: 84 (89ms)
---> Project withdraw: 68129 GAS
      ✓ 0xFE6B56FdCF920382Af1493828E79C017EE090F2a Project: Withdraws ETH (
Stage: 8, Price: 516666666666664

√ Jump to the next block: 85 (76ms)
---> Withdraw: 156356 GAS

√ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: Return tokens (173ms)

Stage: 8, Price: 5166666666666664

√ Jump to the next block: 86 (144ms)

---> Contribution with auto accepting : 187853 GAS
      \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: Buy tokens (706ms)
Stage: 9, Price: 549999999999997

√ Jump to the next block: 87 (101ms)

√ rICO should be finished (37ms)

√ rICO balance - getAvailableProjectETH should be 0 (25ms)

      \checkmark rICO rest balance should be no more or less than 0% off to what was

√ rICO balance should have all getAvailableProjectETH still (25ms)

√ Project balance + getAvailableProjectETH should be committedETH (46r)

      ✓ Project should have all projectWithdrawnETH (14ms)
      \sqrt{0x668d51}FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: compare full token balar
      \checkmark 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: reserved token balance :

√ 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: unlocked token balance 
§
Participant Stats: 0x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F Result {
  '0': true,
  '1': '3',
  '2': '0',
   3': '6200000000000000000000'.
  '4': '20633333333333333282',
```

```
'5': '0',
  '6': '6200000000000000000000000',
  '7': '0',
  '8': '67',
  whitelisted: true,
  contributions: '3',
 withdraws: '0',
  reservedTokens: '62000000000000000000',
  committedEth: '2063333333333333282'.
  pendingEth: '0',
  _currentReservedTokens: '62000000000000000000',
  _unlockedTokens: '0',
  _lastBlock: '67' }
\sqrt{0}x668d51FD53ee7d1dA66d8Cc9eB0274E0D9634C2F: compare price average, $
      \sqrt{9}x10a0717595A97A777F51f3ae542d4312edfD20FA: compare full token balar
      √ 0x10a0717595A97A777F51f3ae542d4312edfD20FA: reserved token balance :
      \sqrt{9x10a0717595A97A777F51f3ae542d4312edfD20FA}: unlocked token balance
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 466666666666664
Compare prices withdraw 46237780567259190
      \sqrt{0}x10a0717595A97A777F51f3ae542d4312edfD20FA: compare price average, $\( \)
      \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5}}; compare full token balar
      \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5}}: reserved token balance s
      ✓ 0xeF6DCBB32a3263d35185993B608843E7A65e90f5: unlocked token balance :
Participant Stats: 0xeF6DCBB32a3263d35185993B608843E7A65e90f5 Result {
  '0': true,
  '1': '7',
  '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
      \sqrt{\text{0xeF6DCBB32a3263d35185993B608843E7A65e90f5}}: compare price average, $\frac{1}{2}$
      √ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: compare full token balar

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: reserved token balance 
§

√ 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: unlocked token balance s
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 416666666666665
Compare prices withdraw 33769882384568211
      \sqrt{0} 0x920aF392141B3aaEc72f93D829F00aB47cFdbd2c: compare price average,
  200 passing (33s)
```



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.

