STATE MIND

Easy Track

19-09-2022 - 30-09-2022

Table of contents

1. Project Brief

Title	Description
Client	Lido
Project name	Easy Track
Timeline	19-09-2022 - 30-09-2022
Number of auditors	4
Initial commit	22c955540e6b9fb5cb46b2ea40bebf367d38eb24
Final commit	cf5e7887b60a3043f92f6cc0c25b5b4034431556

Short Overview

Easy Track motion is a lightweight voting considered to have passed if the minimum objections threshold hasn't been reached. EasyTrack contract uses standalone EVMScript factory contracts to create EVMScripts which are executed if the motion passes.

Context

As opposed to regular Aragon votings, Easy Track motions are cheaper (no need to vote 'pro', token holders only have to vote 'contra' if they have objections) and easier to manage (no need to ask broad DAO community vote on proposals that spark no debate).

Usage and purpose

There are three types of votings run periodically by the Lido DAO wrapped into the Easy Track motions:

- Node Operators increasing staking limits
- Funds being allocated to LEGO program
- Funds being allocated to allowed recipients

Project Scope

The audit covered the following files:

- AddAllowedRecipient.sol
- AddRewardProgram.sol
- IncreaseNodeOperatorStakingLimit.sol
- RemoveAllowedRecipient.sol
- RemoveRewardProgram.sol
- TopUpAllowedRecipients.sol
- TopUpLegoProgram.sol
- TopUpRewardPrograms.sol
- IBokkyPooBahsDateTimeContract.sol
- IEVMScriptExecutor.sol

- IEVMScriptFactory.sol
- BytesUtils.sol
- EVMScriptPermissions.sol
- EVMScriptExecutor.sol
- EasyTrack.sol
- MotionSettings.sol
- TrustedCaller.sol
- IFinance.sol
- EVMScriptCreator.sol
- AllowedRecipientsRegistry.sol
- EVMScriptFactoriesRegistry.sol
- LimitsChecker.sol
- RewardProgramsRegistry.sol

2. Finding Severity breakdown

All vulnerabilities discovered during the audit are classified based on its potential severity and has the following classification:

Severity	Description
Critical	Bugs leading to assets theft, fund access locking, or any other loss funds to be transferred to any party.
High	Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.
Medium	Bugs that can break the intended contract logic or expose it to DoS attacks, but do not cause direct loss funds.
Informational	Bugs that do not have a significant immediate impact and could be easily fixed.

Based on the feedback received from the Customer regarding the list of findings discovered by the Contractor, they are assigned the following statuses:

Status	Description
Fixed	Recommended fixes have been made to the project code and no longer affect its security.
Acknowledged	The Customer is aware of the finding. Recommendations for the finding are planned to be resolved in the future.

3. Summary of findings

Severity	# of Findings
Critical	0
High	1
Medium	0
Informational	8

4. Conclusion

Commit with all fixes: `cf5e7887b60a3043f92f6cc0c25b5b4034431556`
1 high and 8 informational severity issue was found, 9 out of 9 issues were acknowledged.

Deployment

File name	Contract deployed on mainnet
AllowedRecipientsRegistry.sol	0xAa47c268e6b2D4ac7d7f7Ffb28A39484f5212c2A
AddAllowedRecipient.sol	0x1dCFc37719A99d73a0ce25CeEcbeFbF39938cF2C
RemoveAllowedRecipient.sol	0x00BB68a12180a8f7E20D8422ba9F81c07A19A79E
TopUpAllowedRecipients.sol	0x85d703B2A4BaD713b596c647badac9A1e95bB03d
AllowedRecipientsRegistry.sol (LEGO LDO)	0x97615f72c3428A393d65A84A3ea6BBD9ad6C0D74
TopUpAllowedRecipients.sol (LEGO LDO)	0x00caAeF11EC545B192f16313F53912E453c91458
TopUpAllowedRecipients.sol (LEGO DAI)	0x0535a67ea2D6d46f85fE568B7EaA91Ca16824FEC
AllowedRecipientsRegistry.sol (LEGO DAI)	0xb0FE4D300334461523D9d61AaD90D0494e1Abb43

File name	Contract deployed on mainnet
AllowedRecipientsRegistry.sol (RCC DAI)	0xDc1A0C7849150f466F07d48b38eAA6cE99079f80
TopUpAllowedRecipients.sol (RCC DAI)	0x84f74733ede9bFD53c1B3Ea96338867C94EC313e
AllowedRecipientsRegistry.sol (PML DAI)	0xDFfCD3BF14796a62a804c1B16F877Cf7120379dB
TopUpAllowedRecipients.sol (PML DAI)	0x4E6D3A5023A38cE2C4c5456d3760357fD93A22cD
AllowedRecipientsRegistry.sol (ATC DAI)	0xe07305F43B11F230EaA951002F6a55a16419B707
TopUpAllowedRecipients.sol (ATC DAI)	0x67Fb97ABB9035E2e93A7e3761a0d0571c5d7CD07
AllowedRecipientsRegistry.sol (Gas Funder ETH)	0xCf46c4c7f936dF6aE12091ADB9897E3F2363f16F
TopUpAllowedRecipients.sol (Gas Funder ETH)	0x41F9daC5F89092dD6061E59578A2611849317dc8

5. Findings report

High

Possible griefing attack to cancel motions

Acknowledged

Description

At the line EasyTrack.sol#L146, the motion snapshot block is set as the current `block.number`. An attacker can backrun the create motion transaction, take a flashloan of the governance token and object the motion multiple times from different addresses until the objections threshold is reached.

Recommendation

It is recommended to set the snapshot block to `block.number - 1`.

Client's comments

> We accept this risk, because the costs of redeployment of EasyTrack is higher than the possible benefits. Now we mitigate the risk as follows:
>
> - Have monitoring for unusual on-chain activities (single-block objections occurred within the block of the motion creation)
> - Once someone decides to exploit the behavior, the possibility of front-running could be circumvented by using the private communication channels with block proposers (e.g., Flashbots) to prevent tx interception and front-running inside the mempool.
> - Full-fledged Aragon voting can still perform the necessary actions
> - We created an issue and PR for this improvement: https://github.com/lidofinance/easy-track/issues/26 https://github.com/lidofinance/easy-track/pull/25

Informational

Inconsistent naming of function parameters

Acknowledged

Description

At the lines:

- AllowedRecipientsRegistry.sol#L143
- AllowedRecipientsRegistry.sol#L130
- RewardProgramsRegistry.sol#L115

It is recommended to rename the function parameters `_evmScriptFactory` and `_address` to improve readability.

Recommendation

Consider renaming these function parameters to be more in line with the context of each contract.

Client's comments

> Fixed for AllowedRecipientsRegistry.sol We plan to replace the deployed reward program factories with new corresponding factories for allowed recipients. Reward factories will never deploy again

Variables can be immutable

Acknowledged

Description

At the lines:

- TopUpAllowedRecipients.sol#L35
- TopUpAllowedRecipients.sol#L38
- AddAllowedRecipient.sol#L25
- RemoveAllowedRecipient.sol#L24

The variables `token` and `allowedRecipientsRegistry` can be declared as `immutable` since they are set in the constructor and do not change.

Recommendation

It is recommended to declare these variables as `immutable`.

Client's comments

> We deliberately do not use immutable variables for the `token` and `AllowedRecipientsRegistry` for the following reason: we plan to deploy a set of factories for allowed recipients many times for different committees. To save time on deployment and verification, and for security purposes, we want the contract bytecode be the same for different `token` and `allowedRecipientsRegistry` values.

No checks for address zero

Acknowledged

Description

At the line AddAllowedRecipient.sol#L51, the `recipientAddress` is not checked for `address(0)`.
At the line AddRewardProgram.sol#L50, the `rewardProgramAddress` is not checked for `address(0)`.
At the line EVMScriptFactoriesRegistry.sol#L57, the `_evmScriptFactory` is not checked for `address(0)`.
At the line EasyTrack.sol#L258, the `_evmScriptExecutor` is not checked for `address(0)`.

Recommendation

It is recommended to ensure these variables are not `address(0)`.

Client's comments

> Added check for AddAllowedRecipient.sol. Other contracts will not be redeployed anytime soon

Incorrect NatSpec comments

Acknowledged

Description

At the line AddAllowedRecipient.sol#L43, the encoded tuple should be `(address recipientAddress, string title)`.
At the line AddRewardProgram.sol#L42, the encoded tuple should be `(address _rewardProgram, string _title)`.

Recommendation

It is recommended to fix these comments.

Client's comments

> Fixed for AddAllowedRecipient.sol

Possible to create a motion with transfer amount bigger than single transfer limit

Acknowledged

Description

At the lines:

- TopUpAllowedRecipients.sol#L134
- TopUpLegoProgram.sol#L107
- TopUpRewardPrograms.sol#L114

The variables `_amounts[i]` are not checked for max limit, so it is possible to create a motion with transfer amount bigger than single transfer limit implemented in LIP-13. If such a motion is created it has to be cancelled since it cannot be enacted.

Recommendation

Consider not allowing to create such motions.

Client's comments

> We accept this risk, there is no possibility of losing funds. The check implemented in LIP-13 is a safety check and should not be part of the logic for EasyTrack factories

Event parameter can be indexed

Acknowledged

Description

At the line EasyTrack.sol#L39, the event parameter `_creator` can be set as `indexed`.

Recommendation

Consider setting the parameter `_creator` as `indexed`.

Client's comments

> while the cost of EasyTrack redeploy is high, we will postpone these improvements

Gas optimization by replacing memory with calldata

Acknowledged

Description

Files:

- contracts/EVMScriptFactories/AddAllowedRecipient.sol
- contracts/EVMScriptFactories/AddRewardProgram.sol
- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol
- contracts/EVMScriptFactories/RemoveAllowedRecipient.sol
- contracts/EVMScriptFactories/RemoveRewardProgram.sol
- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol
- contracts/EVMScriptFactories/TopUpLegoProgram.sol
- contracts/EVMScriptFactories/TopUpRewardPrograms.sol
- contracts/EVMScriptExecutor.sol
- contracts/EVMScriptFactoriesRegistry.sol
- contracts/EasyTrack.sol

External calls to functions with `memory` parameters can be made more gas efficient by replacing `memory` with `calldata`, as long as the memory parameters are not modified.

Recommendation

Consider replacing `memory` with `calldata`.

Client's comments

> To implement these changes, a redeploy of EasyTrack is required. Overrun gas cost is insignificant in terms of DAO payments, and it does not add any risks.

Node operator can spam

Acknowledged

Description

The node operator can spam motions until he is disabled EasyTrack.sol#L133
IncreaseNodeOperatorStakingLimit.sol#L118-L119

Recommendation

We recommend limiting the motion amount for a single operator.

Client's comments

> Indeed, there is such a risk. But EasyTrack's redeploy is high cost. If a Node Operator starts spamming motions, there are two options for responding to the situation:
>
> 1. we can either deactivate NO through Aragon voting
> 2. or remove all the IncreaseNodeOperatorStakingLimit Factory from EVMScriptFactoriesRegistry and then increase NO's staking limits through Aragon votings

6. Appendix A. Linter

Error/compiler-version

- contracts/AllowedRecipientsRegistry.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EasyTrack.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptExecutor.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/AddAllowedRecipient.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/AddRewardProgram.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/RemoveAllowedRecipient.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/RemoveRewardProgram.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/TopUpLegoProgram.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/EVMScriptFactoriesRegistry.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/interfaces/IBokkyPooBahsDateTimeContract.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/interfaces/IEVMScriptExecutor.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/interfaces/IEVMScriptFactory.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/interfaces/IFinance.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement
- contracts/libraries/BytesUtils.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/libraries/EVMScriptCreator.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/libraries/EVMScriptPermissions.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/LimitsChecker.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/MotionSettings.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/RewardProgramsRegistry.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

- contracts/TrustedCaller.sol:4 - Compiler version ^0.8.4 does not satisfy the 0.8.13 semver requirement

Error/ordering

- contracts/AllowedRecipientsRegistry.sol:21 - Function order is incorrect, state variable declaration can not go after event definition (line 16)

- contracts/EasyTrack.sol:16 - Function order is incorrect, external view function can not go after external pure function (line 14)

- contracts/EasyTrack.sol:59 - Function order is incorrect, state variable declaration can not go after event definition (line 54)

- contracts/EVMScriptExecutor.sol:31 - Function order is incorrect, state variable declaration can not go after event definition (line 26)

- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:23 - Function order is incorrect, external function can not go after external view function (line 10)

- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:111 - Function order is incorrect, private view function can not go after private pure function (line 103)

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:153 - Function order is incorrect, private view function can not go after private pure function (line 145)

- contracts/EVMScriptFactoriesRegistry.sol:29 - Function order is incorrect, state variable declaration can not go after event definition (line 22)

- contracts/LimitsChecker.sol:47 - Function order is incorrect, state variable declaration can not go after event definition (line 43)

- contracts/MotionSettings.sol:22 - Function order is incorrect, state variable declaration can not go after event definition (line 16)

- contracts/RewardProgramsRegistry.sol:21 - Function order is incorrect, state variable declaration can not go after event definition (line 16)

- contracts/TrustedCaller.sol:20 - Function order is incorrect, modifier definition can not go after constructor (line 15)

Error/private-vars-leading-underscore

- contracts/AllowedRecipientsRegistry.sol:29 - 'ERROR_RECIPIENT_ALREADY_ADDED_TO_ALLOWED_LIST' should start with _
- contracts/AllowedRecipientsRegistry.sol:31 - 'ERROR_RECIPIENT_NOT_FOUND_IN_ALLOWED_LIST' should start with _
- contracts/AllowedRecipientsRegistry.sol:43 - 'allowedRecipientIndices' should start with _
- contracts/EasyTrack.sol:59 - 'ERROR_ALREADY_OBJECTED' should start with _
- contracts/EasyTrack.sol:60 - 'ERROR_NOT_ENOUGH_BALANCE' should start with _
- contracts/EasyTrack.sol:61 - 'ERROR_NOT_CREATOR' should start with _
- contracts/EasyTrack.sol:62 - 'ERROR_MOTION_NOT_PASSED' should start with _
- contracts/EasyTrack.sol:63 - 'ERROR_UNEXPECTED_EVM_SCRIPT' should start with _
- contracts/EasyTrack.sol:64 - 'ERROR_MOTION_NOT_FOUND' should start with _
- contracts/EasyTrack.sol:65 - 'ERROR_MOTIONS_LIMIT_REACHED' should start with _
- contracts/EasyTrack.sol:79 - 'HUNDRED_PERCENT' should start with _
- contracts/EasyTrack.sol:89 - 'lastMotionId' should start with _
- contracts/EasyTrack.sol:99 - 'motionIndicesByMotionId' should start with _
- contracts/EVMScriptExecutor.sol:31 - 'ERROR_CALLER_IS_FORBIDDEN' should start with _
- contracts/EVMScriptExecutor.sol:32 - 'ERROR_EASY_TRACK_IS_NOT_CONTRACT' should start with _
- contracts/EVMScriptExecutor.sol:33 - 'ERROR_CALLS_SCRIPT_IS_NOT_CONTRACT' should start with _
- contracts/EVMScriptExecutor.sol:42 - 'INITIALIZATION_BLOCK_POSITION' should start with _
- contracts/EVMScriptFactories/AddAllowedRecipient.sol:17 - 'ERROR_ALLOWED_RECIPIENT_ALREADY_ADDED' should start with _
- contracts/EVMScriptFactories/AddRewardProgram.sol:17 - 'ERROR_REWARD_PROGRAM_ALREADY_ADDED' should start with _
- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:41 - 'ERROR_NODE_OPERATOR_DISABLED' should start with _

- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:42 - 'ERROR_CALLER_IS_NOT_NODE_OPERATOR' should start with _

- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:43 - 'ERROR_STAKING_LIMIT_TOO_LOW' should start with _

- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:44 - 'ERROR_NOT_ENOUGH_SIGNING_KEYS' should start with _

- contracts/EVMScriptFactories/RemoveAllowedRecipient.sol:17 - 'ERROR_ALLOWED_RECIPIENT_NOT_FOUND' should start with _

- contracts/EVMScriptFactories/RemoveRewardProgram.sol:17 - 'ERROR_REWARD_PROGRAM_NOT_FOUND' should start with _

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:18 - 'ERROR_LENGTH_MISMATCH' should start with _

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:19 - 'ERROR_EMPTY_DATA' should start with _

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:20 - 'ERROR_ZERO_AMOUNT' should start with _

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:21 - 'ERROR_RECIPIENT_NOT_ALLOWED' should start with _

- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:22 - 'ERROR_SUM_EXCEEDS_SPENDABLE_BALANCE' should start with _

- contracts/EVMScriptFactories/TopUpLegoProgram.sol:17 - 'ERROR_LENGTH_MISMATCH' should start with _

- contracts/EVMScriptFactories/TopUpLegoProgram.sol:18 - 'ERROR_EMPTY_DATA' should start with _

- contracts/EVMScriptFactories/TopUpLegoProgram.sol:19 - 'ERROR_ZERO_AMOUNT' should start with _

- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:18 - 'ERROR_LENGTH_MISMATCH' should start with _

- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:19 - 'ERROR_EMPTY_DATA' should start with _

- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:20 - 'ERROR_ZERO_AMOUNT' should start with _

- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:21 - 'ERROR_REWARD_PROGRAM_NOT_ALLOWED' should start with _

- contracts/EVMScriptFactoriesRegistry.sol:33 - 'evmScriptFactoryIndices' should start with _

- contracts/libraries/EVMScriptCreator.sol:11 - 'SPEC_ID' should start with _

- contracts/libraries/EVMScriptPermissions.sol:20 - 'SPEC_ID_SIZE' should start with _

- contracts/libraries/EVMScriptPermissions.sol:23 - 'ADDRESS_SIZE' should start with _
- contracts/libraries/EVMScriptPermissions.sol:26 - 'CALLDATA_LENGTH_SIZE' should start with _
- contracts/libraries/EVMScriptPermissions.sol:29 - 'METHOD_SELECTOR_SIZE' should start with _
- contracts/libraries/EVMScriptPermissions.sol:32 - 'PERMISSION_SIZE' should start with _
- contracts/LimitsChecker.sol:47 - 'ERROR_INVALID_PERIOD_DURATION' should start with _
- contracts/LimitsChecker.sol:48 - 'ERROR_SUM_EXCEEDS_SPENDABLE_BALANCE' should start with _
- contracts/LimitsChecker.sol:49 - 'ERROR_TOO_LARGE_LIMIT' should start with _
- contracts/LimitsChecker.sol:68 - 'periodDurationMonths' should start with _
- contracts/LimitsChecker.sol:71 - 'currentPeriodEndTimestamp' should start with _
- contracts/LimitsChecker.sol:74 - 'limit' should start with _
- contracts/LimitsChecker.sol:77 - 'spentAmount' should start with _
- contracts/MotionSettings.sol:22 - 'ERROR_VALUE_TOO_SMALL' should start with _
- contracts/MotionSettings.sol:23 - 'ERROR_VALUE_TOO_LARGE' should start with _
- contracts/RewardProgramsRegistry.sol:27 - 'ERROR_REWARD_PROGRAM_ALREADY_ADDED' should start with _
- contracts/RewardProgramsRegistry.sol:28 - 'ERROR_REWARD_PROGRAM_NOT_FOUND' should start with _
- contracts/RewardProgramsRegistry.sol:39 - 'rewardProgramIndices' should start with _
- contracts/TrustedCaller.sol:10 - 'ERROR_TRUSTED_CALLER_IS_ZERO_ADDRESS' should start with _
- contracts/TrustedCaller.sol:11 - 'ERROR_CALLER_IS_FORBIDDEN' should start with _

Error/max-states-count

- contracts/EasyTrack.sol:21 - Contract has 6 states declarations but allowed no more than 3
- contracts/LimitsChecker.sol:32 - Contract has 4 states declarations but allowed no more than 3

Error/not-rely-on-time

- contracts/EasyTrack.sol:145 - Avoid to make time-based decisions in your business logic
- contracts/EasyTrack.sol:174 - Avoid to make time-based decisions in your business logic

- contracts/LimitsChecker.sol:116 - Avoid to make time-based decisions in your business logic
- contracts/LimitsChecker.sol:132 - Avoid to make time-based decisions in your business logic
- contracts/LimitsChecker.sol:133 - Avoid to make time-based decisions in your business logic
- contracts/LimitsChecker.sol:183 - Avoid to make time-based decisions in your business logic

Error/max-line-length

- contracts/EasyTrack.sol:167 - Line length must be no more than 100 but current length is 104.
- contracts/EasyTrack.sol:168 - Line length must be no more than 100 but current length is 102.
- contracts/EasyTrack.sol:273 - Line length must be no more than 100 but current length is 108.
- contracts/EasyTrack.sol:298 - Line length must be no more than 100 but current length is 108.
- contracts/EVMScriptExecutor.sol:20 - Line length must be no more than 100 but current length is 144.
- contracts/EVMScriptExecutor.sol:40 - Line length must be no more than 100 but current length is 122.
- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:67 - Line length must be no more than 100 but current length is 103.
- contracts/EVMScriptFactories/IncreaseNodeOperatorStakingLimit.sol:86 - Line length must be no more than 100 but current length is 103.
- contracts/EVMScriptFactories/TopUpAllowedRecipients.sol:13 - Line length must be no more than 100 but current length is 105.
- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:57 - Line length must be no more than 100 but current length is 102.
- contracts/EVMScriptFactories/TopUpRewardPrograms.sol:90 - Line length must be no more than 100 but current length is 102.
- contracts/EVMScriptFactoriesRegistry.sol:49 - Line length must be no more than 100 but current length is 109.
- contracts/EVMScriptFactoriesRegistry.sol:50 - Line length must be no more than 100 but current length is 104.
- contracts/LimitsChecker.sol:16 - Line length must be no more than 100 but current length is 102.
- contracts/LimitsChecker.sol:27 - Line length must be no more than 100 but current length is 106.
- contracts/LimitsChecker.sol:107 - Line length must be no more than 100 but current length is 104.
- contracts/LimitsChecker.sol:172 - Line length must be no more than 100 but current length is 104.

- contracts/LimitsChecker.sol:274 - Line length must be no more than 100 but current length is 101.
- contracts/LimitsChecker.sol:278 - Line length must be no more than 100 but current length is 102.
- contracts/LimitsChecker.sol:300 - Line length must be no more than 100 but current length is 115.
- contracts/MotionSettings.sol:9 - Line length must be no more than 100 but current length is 119.
- contracts/RewardProgramsRegistry.sol:81 - Line length must be no more than 100 but current length is 129.
- contracts/TrustedCaller.sol:7 - Line length must be no more than 100 but current length is 114.

7. Appendix B. Slither

High/Medium/controlled-delegatecall

EVMScriptExecutor.executeEVMScript(bytes) uses delegatecall to a input-controlled function id

- (success,output) = callsScript.delegatecall(execScriptCallData)

Informational/High/assembly

EVMScriptExecutor.executeEVMScript(bytes) uses assembly

- INLINE ASM

BytesUtils.bytes24At(bytes,uint256) uses assembly

- INLINE ASM

BytesUtils.addressAt(bytes,uint256) uses assembly

- INLINE ASM

BytesUtils.uint32At(bytes,uint256) uses assembly

- INLINE ASM

BytesUtils.uint256At(bytes,uint256) uses assembly

- INLINE ASM

Informational/High/low-level-calls

Low level call in EVMScriptExecutor.executeEVMScript(bytes):

- (success,output) = callsScript.delegatecall(execScriptCallData)

Informational/High/missing-inheritance

EVMScriptExecutor should inherit from IEVMScriptExecutor

Informational/High/naming-convention

Parameter LimitsChecker.isUnderSpendableBalance(uint256,uint256)._payoutAmount is not in mixedCase

Parameter LimitsChecker.isUnderSpendableBalance(uint256,uint256)._motionDuration is not in mixedCase

Parameter LimitsChecker.updateSpentAmount(uint256)._payoutAmount is not in mixedCase

Parameter LimitsChecker.setLimitParameters(uint256,uint256)._limit is not in mixedCase

Parameter LimitsChecker.setLimitParameters(uint256,uint256)._periodDurationMonths is not in mixedCase

Parameter AddAllowedRecipient.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter AddAllowedRecipient.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter AddAllowedRecipient.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter EVMScriptExecutor.executeEVMScript(bytes)._evmScript is not in mixedCase

Parameter EVMScriptExecutor.setEasyTrack(address)._easyTrack is not in mixedCase

Parameter AddRewardProgram.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter AddRewardProgram.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter AddRewardProgram.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter MotionSettings.setMotionDuration(uint256)._motionDuration is not in mixedCase

Parameter MotionSettings.setObjectionsThreshold(uint256)._objectionsThreshold is not in mixedCase

Parameter MotionSettings.setMotionsCountLimit(uint256)._motionsCountLimit is not in mixedCase

Parameter RemoveAllowedRecipient.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter RemoveAllowedRecipient.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter RemoveAllowedRecipient.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter EVMScriptFactoriesRegistry.addEVMScriptFactory(address,bytes)._evmScriptFactory is not in mixedCase

Parameter EVMScriptFactoriesRegistry.addEVMScriptFactory(address,bytes)._permissions is not in mixedCase

Parameter EVMScriptFactoriesRegistry.removeEVMScriptFactory(address)._evmScriptFactory is not in mixedCase

Parameter EVMScriptFactoriesRegistry.isEVMScriptFactory(address)._maybeEVMScriptFactory is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes)._to is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes)._methodId is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes)._evmScriptCallData is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes[])._to is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes[])._methodId is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4,bytes[])._evmScriptCallData is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4[],bytes[])._to is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4[],bytes[])._methodIds is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address,bytes4[],bytes[])._evmScriptCallData is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address[],bytes4[],bytes[])._to is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address[],bytes4[],bytes[])._methodIds is not in mixedCase

Parameter EVMScriptCreator.createEVMScript(address[],bytes4[],bytes[])._evmScriptCallData is not in mixedCase

Parameter IncreaseNodeOperatorStakingLimit.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter IncreaseNodeOperatorStakingLimit.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter IncreaseNodeOperatorStakingLimit.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter AllowedRecipientsRegistry.addRecipient(address,string)._recipient is not in mixedCase

Parameter AllowedRecipientsRegistry.addRecipient(address,string)._title is not in mixedCase

Parameter AllowedRecipientsRegistry.removeRecipient(address)._recipient is not in mixedCase

Parameter AllowedRecipientsRegistry.isRecipientAllowed(address)._address is not in mixedCase

Parameter RemoveRewardProgram.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter RemoveRewardProgram.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter RemoveRewardProgram.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter RewardProgramsRegistry.addRewardProgram(address,string)._rewardProgram is not in mixedCase

Parameter RewardProgramsRegistry.addRewardProgram(address,string)._title is not in mixedCase

Parameter RewardProgramsRegistry.removeRewardProgram(address)._rewardProgram is not in mixedCase

Parameter RewardProgramsRegistry.isRewardProgram(address)._maybeRewardProgram is not in mixedCase

Parameter BytesUtils.uint32At(bytes,uint256)._data is not in mixedCase

Parameter BytesUtils.uint32At(bytes,uint256)._location is not in mixedCase

Parameter EVMScriptPermissions.canExecuteEVMScript(bytes,bytes)._permissions is not in mixedCase

Parameter EVMScriptPermissions.canExecuteEVMScript(bytes,bytes)._evmScript is not in mixedCase

Parameter EVMScriptPermissions.isValidPermissions(bytes)._permissions is not in mixedCase

Parameter TopUpLegoProgram.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter TopUpLegoProgram.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter TopUpLegoProgram.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter EasyTrack.createMotion(address,bytes)._evmScriptFactory is not in mixedCase

Parameter EasyTrack.createMotion(address,bytes)._evmScriptCallData is not in mixedCase

Parameter EasyTrack.enactMotion(uint256,bytes)._motionId is not in mixedCase

Parameter EasyTrack.enactMotion(uint256,bytes)._evmScriptCallData is not in mixedCase

Parameter EasyTrack.objectToMotion(uint256)._motionId is not in mixedCase

Parameter EasyTrack.cancelMotion(uint256)._motionId is not in mixedCase

Parameter EasyTrack.cancelMotions(uint256[])._motionIds is not in mixedCase

Parameter EasyTrack.setEVMScriptExecutor(address)._evmScriptExecutor is not in mixedCase

Parameter EasyTrack.canObjectToMotion(uint256,address)._motionId is not in mixedCase

Parameter EasyTrack.canObjectToMotion(uint256,address)._objector is not in mixedCase

Parameter EasyTrack.getMotion(uint256)._motionId is not in mixedCase

Parameter TopUpAllowedRecipients.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter TopUpAllowedRecipients.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter TopUpAllowedRecipients.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Parameter TopUpRewardPrograms.createEVMScript(address,bytes)._creator is not in mixedCase

Parameter TopUpRewardPrograms.createEVMScript(address,bytes)._evmScriptCallData is not in mixedCase

Parameter TopUpRewardPrograms.decodeEVMScriptCallData(bytes)._evmScriptCallData is not in mixedCase

Informational/High/pragma

Different versions of Solidity is used:

- Version used: ['^0.8.0', '^0.8.4']
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4

- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4
- ^0.8.4

Informational/High/solc-version

solc-mit.11564f7 is not recommended for deployment

Informational/Medium/costly-loop

EasyTrack._deleteMotion(uint256) has costly operations inside a loop:

- motions.pop()

EasyTrack._deleteMotion(uint256) has costly operations inside a loop:

- delete motionIndicesByMotionId[_motionId]

Informational/Medium/similar-names

Variable RewardProgramsRegistry.removeRewardProgram(address)._rewardProgram is too similar to RewardProgramsRegistry.rewardPrograms

Variable RewardProgramsRegistry.addRewardProgram(address,string)._rewardProgram is too similar to RewardProgramsRegistry.rewardPrograms

Variable TopUpAllowedRecipients._decodeEVMScriptCallData(bytes)._evmScriptCallData is too similar to TopUpAllowedRecipients.createEVMScript(address,bytes).evmScriptsCalldata

Variable IEVMScriptFactory.createEVMScript(address,bytes)._evmScriptCallData is too similar to TopUpAllowedRecipients.createEVMScript(address,bytes).evmScriptsCalldata

Variable TopUpAllowedRecipients.createEVMScript(address,bytes)._evmScriptCallData is too similar to TopUpAllowedRecipients.createEVMScript(address,bytes).evmScriptsCalldata

Variable TopUpAllowedRecipients.decodeEVMScriptCallData(bytes)._evmScriptCallData is too similar to TopUpAllowedRecipients.createEVMScript(address,bytes).evmScriptsCalldata

Variable TopUpRewardPrograms.decodeEVMScriptCallData(bytes)._evmScriptCallData is too similar to TopUpRewardPrograms.createEVMScript(address,bytes).evmScriptsCalldata

Variable IEVMScriptFactory.createEVMScript(address,bytes)._evmScriptCallData is too similar to TopUpRewardPrograms.createEVMScript(address,bytes).evmScriptsCalldata

Variable TopUpRewardPrograms.createEVMScript(address,bytes)._evmScriptCallData is too similar to TopUpRewardPrograms.createEVMScript(address,bytes).evmScriptsCalldata

Variable TopUpRewardPrograms._decodeEVMScriptCallData(bytes)._evmScriptCallData is too similar to TopUpRewardPrograms.createEVMScript(address,bytes).evmScriptsCalldata

Informational/Medium/too-many-digits

BytesUtils.addressAt(bytes,uint256) uses literals with too many digits:

- result = word & 0xffffffffffffffffffffffffffffffffffffffff000000000000000000000000 >> 96

BytesUtils.uint32At(bytes,uint256) uses literals with too many digits:

- result = word & 0xffffffff00000000000000000000000000000000000000000000000000000000 >> 224

Low/Medium/missing-zero-check

TopUpLegoProgram.constructor(address,IFinance,address)._legoProgram lacks a zero-check on :

- legoProgram = _legoProgram

TopUpAllowedRecipients.constructor(address,address,address,address,address)._token lacks a zero-check on :

- token = _token

TopUpRewardPrograms.constructor(address,address,address,address)._rewardToken lacks a zero-check on :

- rewardToken = _rewardToken

Low/Medium/reentrancy-events

Reentrancy in EasyTrack.createMotion(address,bytes): External calls:

- evmScript = _createEVMScript(_evmScriptFactory,msg.sender,_evmScriptCallData)
- _evmScript = IEVMScriptFactory(_evmScriptFactory).createEVMScript(_creator,_evmScriptCallData) Event emitted after the call(s):
- MotionCreated(_newMotionId,msg.sender,_evmScriptFactory,_evmScriptCallData,evmScript)

Reentrancy in EVMScriptExecutor.executeEVMScript(bytes): External calls:

- (success,output) = callsScript.delegatecall(execScriptCallData) Event emitted after the call(s):
- ScriptExecuted(msg.sender,_evmScript)

Low/Medium/timestamp

LimitsChecker.isUnderSpendableBalance(uint256,uint256) uses timestamp for comparisons Dangerous comparisons:

- block.timestamp + _motionDuration >= currentPeriodEndTimestamp

LimitsChecker.updateSpentAmount(uint256) uses timestamp for comparisons Dangerous comparisons:

- block.timestamp >= currentPeriodEndTimestampLocal

EasyTrack.enactMotion(uint256,bytes) uses timestamp for comparisons Dangerous comparisons:

- require(bool,string)(motion.startDate + motion.duration <= block.timestamp,ERROR_MOTION_NOT_PASSED)

Medium/Medium/divide-before-multiply

LimitsChecker._getFirstMonthInPeriodFromMonth(uint256,uint256) performs a multiplication on the result of a division:

- periodNumber = (_month - 1) / _periodDurationMonths
- _firstMonthInPeriod = periodNumber * _periodDurationMonths + 1

Medium/Medium/unused-return

EasyTrack.enactMotion(uint256,bytes) ignores return value by evmScriptExecutor.executeEVMScript(evmScript)

8. Appendix C. Tests

Tests result

```
171 passed, 1 skipped, 24 warnings in 285.42s
```

- tests/test_vote_for_reward_programs.py::test_vote_for_reward_programs SKIPPED
- BrownieEnvironmentWarning: 'Agent' defines a 'balance' function, 'Agent.balance' is available as Agent.wei_balance

Tests coverage

Function	Coverage
EVMScriptFactoriesRegistry._getEVMScriptFactoryIndex	100.0%
EVMScriptFactoriesRegistry.addEVMScriptFactory	100.0%
EVMScriptFactoriesRegistry.removeEVMScriptFactory	100.0%
EVMScriptFactoriesRegistry._createEVMScript	100.0%
EasyTrack._deleteMotion	100.0%
EasyTrack._getMotion	100.0%
EasyTrack.cancelMotion	100.0%
EasyTrack.cancelMotions	100.0%
EasyTrack.enactMotion	100.0%
EasyTrack.objectToMotion	100.0%
EVMScriptFactoriesRegistry.addEVMScriptFactory	75.0%
MotionSettings._setMotionsCountLimit	75.0%
EVMScriptFactoriesRegistry._getEVMScriptFactoryIndex	0.0%
EVMScriptFactoriesRegistry.removeEVMScriptFactory	0.0%
MotionSettings._setMotionDuration	0.0%
MotionSettings._setObjectionsThreshold	0.0%

Function	Coverage
MotionSettings._setMotionDuration	100.0%
MotionSettings._setMotionsCountLimit	100.0%
MotionSettings._setObjectionsThreshold	100.0%
RewardProgramsRegistry._getRewardProgramIndex	100.0%
RewardProgramsRegistry.addRewardProgram	100.0%
RewardProgramsRegistry.removeRewardProgram	100.0%

STATE
MIND