



Cyberscope

# Audit Report

## **Governance**

Aug 2023

Github      <https://github.com/L3A-Protocol/daodevt-contracts>  
Commit      8ed9a7f1fea443d57063b3b422d1a074dc51c7b1  
Audited by   © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Review</b>	<b>2</b>
Audit Updates	2
Source Files	3
<b>Overview</b>	<b>5</b>
<b>Contract</b>	<b>6</b>
TokenListGovernance	6
Initialization and Setup	6
Member Management	6
Voting and Proposal Creation	6
Voting Power Calculation	6
Validation and Authorization	6
TokenList	7
TokenListGovernanceSetup	8
TokenMajorityVotingBase	8
TaskDrafts	9
Contract Initialization and Dependencies:	9
Supports Interface:	9
Getter Functions:	9
Update Addresses:	9
Create Draft Task:	9
TaskDraftsSetup	10
<b>Testing Deploy</b>	<b>11</b>
<b>Functions Analysis</b>	<b>12</b>
<b>Inheritance Graph</b>	<b>21</b>
<b>Flow Graph</b>	<b>22</b>
<b>Summary</b>	<b>23</b>
<b>Disclaimer</b>	<b>24</b>
<b>About Cyberscope</b>	<b>25</b>

## Review

Repository	<a href="https://github.com/L3A-Protocol/daodevt-contracts">https://github.com/L3A-Protocol/daodevt-contracts</a>
Commit	8ed9a7f1fea443d57063b3b422d1a074dc51c7b1

## Audit Updates

Initial Audit	08 Aug 2023
---------------	-------------

## Source Files

Filename	SHA256
Deps/PreferredProxy.sol	adb809b290ac7e055ebf754b4479a1cd9b b7e66b24697a3f0a481ea5d0dedd68
Deps/DepsEns.sol	a84ff7677462c821a1ce09e6dc857dedb3e 8117a5a9ad5a3d9308f224428c51f
Deps/DepsAragon.sol	ad94b5150daa5af1d42d7148fc842e13c66 142b8069cf08134433074be91190e
DAO/TokenMembership/ITokenMembership.sol	f725a8b7fe10e883d7b899ccfee1d55c6fcd b13c7cdddb3cde7014a71f39fd75
DAO/TokenMajorityVoting/TokenMajorityVotingBase.sol	e905c3ccee1a8f14ba34304ba428546d70 cea4ad8523831f8e9873b26818ac92
DAO/TokenMajorityVoting/ITokenMajorityVoting.sol	ac633b6d97b5c0040d9744847aff8714c47 a78b445fed52386d24c9f32084dcb
DAO/TaskDrafts/TaskDraftsSetup.sol	a2c2a405016c1af093563e69a6da15d880 0f7911fd6684bfd9b111650ac2a59e
DAO/TaskDrafts/TaskDrafts.sol	403428cf93bfdc8fb8b50b3fc0a94b567a1 a0d5e36ec3910655d89f131abcfce
DAO/TaskDrafts/ITaskDrafts.sol	3b3af0b2160e95f0381f56459378bd3eb9f e5769396f9c9dac3d9e04d284f0d6
DAO/Governance/TokenListGovernanceSetup.sol	0760cc702664e4497d4c639343a071477f 4457e16e493d6cb05b6cf82ef77098
DAO/Governance/TokenListGovernance.sol	fa70b9652defac0879b56f719cd01333040 14efba989d6def6c807126eaf7da6
DAO/Governance/TokenList.sol	4413fb887a1a5b416b22de7a0c5135ca03 89eb83e4f703362a8f8ecab1b8d777

<b>DAO/Governance/ITokenListGovernance.sol</b>	aa479003b04ad091c20f5925223167c02d da0ca037d34b01e7a53638990a7b84
<b>DAO/Governance/IPluginProposals.sol</b>	9b469ed92c6a8fc3824eff56134f36eb7693 8eb001381092724a0362d1916a75

## Overview

The project implements a governance model where the users have the authority to vote if they are holders of an NFT of a specific collection. The main functionality is forked from the Aragon protocol based on the token voting plugin. According to the project's requirements, the plugin has been modified in order to support NFT instead of ERC20 token. Cyberscope audit assessment focuses on the changes that have been introduced from the forked version.

# Contract

## TokenListGovernance

The TokenListGovernance contract implements a governance mechanism for managing a list of token holders within a decentralized autonomous organization (DAO). This contract is based on several existing libraries and interfaces, including OpenZeppelin's upgradeable contracts, Aragon's OS (Open Source) project, and various token-related interfaces. The contract features include:

### Initialization and Setup

Initializes the contract with the associated DAO, voting settings, ERC721 token collection (used for representing token ownership), and initial members of the DAO.

### Member Management

The contract provides functions to add and remove members to/from the token list. These actions are protected by an authorization mechanism through the `UPDATE_MEMBERS_PERMISSION_ID` permission.

### Voting and Proposal Creation

The contract allows token holders to create proposals. The creator of a proposal must own an NFT from the collection to create the proposal. Voting is possible with the options of "Yes" "No" or "Abstain". Proposals have a start, end date, and they can be executed before the end date if certain conditions are met.

### Voting Power Calculation

The contract calculates the total voting power based on the length of the token list at a specific block.

### Validation and Authorization

The contract enforces various validations and authorizations to ensure that actions are carried out only by authorized parties and that certain conditions are met before executing certain functions.

## TokenList

The contract TokenList is an abstract contract that provides functionality for managing a list of token IDs. It's designed to keep track of the tokens that are considered "listed" in the system. Tokens can be added or removed from this list, and historical changes are checkpointed to ensure transparency and accountability.

The contract maintains two types of checkpointed histories:

- `_tokenlistCheckpoints` : A mapping that stores the checkpointed history of the token list. Each token ID maps to a CheckpointsUpgradeable. History object that records changes to the token's status (whether listed or not) at different block numbers.
- `_tokenlistLengthCheckpoints` : A CheckpointsUpgradeable. History object that stores the checkpointed history of the length of the token list. The functions `isListedAtBlock` and `isListed` are used to check whether a specific token is listed at a given block number or at the latest block respectively.

The contract defines a storage gap at the end of the contract's storage layout to accommodate potential storage additions in future versions without disrupting the existing storage layout.



## TokenListGovernanceSetup

The TokenListGovernanceSetup contract is responsible for setting up the deployment and initialization of the TaskDrafts plugin within a DAO environment. The code leverages some Aragon-related libraries and interfaces.

The TokenListGovernanceSetup contract serves as a setup contract that handles the deployment, initialization, and permissions of the TaskDrafts plugin within an Aragon DAO environment.

## TokenMajorityVotingBase

This contract appears to be related to a token-based majority voting mechanism for a decentralized autonomous organization (DAO). Overall, the contract defines a flexible and extensible framework for managing token-based majority voting for proposals within a DAO. It leverages concepts from the Aragon framework and integrates with the OpenZeppelin library for various functionalities. The code structure suggests that the contract is designed to be upgradable, allowing for modifications and improvements over time while maintaining compatibility with existing data and implementations.

## TaskDrafts

The TaskDrafts contract is creating draft tasks within a decentralized autonomous organization (DAO) using Aragon's framework.

### Contract Initialization and Dependencies:

This contract uses the OpenZeppelin's Initializable and Aragon's PluginUUPSUpgradeable contracts for initialization and upgrades.

### Supports Interface:

The supportsInterface function checks if the contract supports the given interface. It supports both the ITaskDrafts interface and the interfaces inherited from PluginUUPSUpgradeable.

### Getter Functions:

`getTasksContract` : This function returns the address of the ITasks contract.

`getGovernanceContract` : This function returns the address of the IPluginProposals contract.

### Update Addresses:

The updateAddresses function is used to update the addresses of the ITasks and IPluginProposals contracts. It requires the UPDATE\_ADDRESSES\_PERMISSION\_ID permission to be called.

### Create Draft Task:

The createDraftTask function creates a draft task within the DAO using the provided information.

It takes parameters such as metadata, start date, end date, and a CreateTaskInfo struct which includes task-related information like metadata, deadline, budget, manager, and preapproval status.

Inside the function, an IDAO. Action array is created with the encoded call data to create a task using the `tasks.createTask` function.

The `governancePlugin.createPluginProposal` function is then called to create a governance proposal for creating the task with the provided actions and other information.

This contract acts as a bridge between the `ITasks` contract (for creating tasks) and the `IPluginProposals` contract (for creating governance proposals). It allows tasks to be drafted and proposed within the DAO's governance framework.

## **TaskDraftsSetup**

The `TaskDraftsSetup` contract is responsible for setting up the deployment and initialization of the `TaskDrafts` plugin within a DAO environment. The code leverages some Aragon-related libraries and interfaces.

The `TaskDraftsSetup` contract serves as a setup contract that handles the deployment, initialization, and permissions of the `TaskDrafts` plugin within an Aragon DAO environment.

## Testing Deploy

Contact Name	Explorer
TokenListGovernance	<a href="https://mumbai.polygonscan.com/address/0x172F66c8A99d53ffc0C521161156D9a30f9B3269">https://mumbai.polygonscan.com/address/0x172F66c8A99d53ffc0C521161156D9a30f9B3269</a>
TaskDrafts	<a href="https://mumbai.polygonscan.com/address/0x62787bacC9AabF203C85EC0Ac6a67AD7F7f7ada9">https://mumbai.polygonscan.com/address/0x62787bacC9AabF203C85EC0Ac6a67AD7F7f7ada9</a>
TaskDraftsSetup	<a href="https://mumbai.polygonscan.com/address/0x6e985568F7865b45adC737C9580adaa9F083775D">https://mumbai.polygonscan.com/address/0x6e985568F7865b45adC737C9580adaa9F083775D</a>
TokenListGovernanceSetup	<a href="https://mumbai.polygonscan.com/address/0x98ce51BBbc878c00405aAeFc45C58ADF115e29B7">https://mumbai.polygonscan.com/address/0x98ce51BBbc878c00405aAeFc45C58ADF115e29B7</a>

## Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>MockERC721</b>	Implementation	ERC721		
		Public	✓	ERC721
	grantToken	External	✓	-
	burnToken	External	✓	-
<b>MockERC721</b>	Implementation	ERC721		
		Public	✓	ERC721
	grantToken	External	✓	-
	burnToken	External	✓	-
<b>MockERC20</b>	Implementation	ERC20		
		Public	✓	ERC20
	increaseBalance	Public	✓	-
	decreaseBalance	Public	✓	-
	setBalance	External	✓	-
<b>TasksUtils</b>	Implementation	ITasks, Context		
	_toOffchainTask	Internal		
	_increaseBudgetToReward	Internal	✓	

	_setRewardBellowBudget	Internal	✓	
	_payoutTask	Internal	✓	
	_refundCreator	Internal	✓	
<b>TasksEnsure</b>	Implementation	ITasks, Context		
	_ensureTaskIsOpen	Internal		
	_ensureTaskIsTaken	Internal		
	_ensureTaskNotClosed	Internal		
	_ensureSenderIsManager	Internal		
	_ensureSenderIsExecutor	Internal		
	_ensureRewardEndsWithNextToken	Internal		
	_ensureApplicationExists	Internal		
	_ensureSenderIsApplicant	Internal		
	_ensureApplicationIsAccepted	Internal		
	_ensureSubmissionExists	Internal		
	_ensureSubmissionNotJudged	Internal		
	_ensureJudgementNotNone	Internal		
	_ensureCancelTaskRequestExists	Internal		
	_ensureRequestNotAccepted	Internal		
	_ensureRequestAccepted	Internal		
	_ensureRequestNotExecuted	Internal		
<b>Tasks</b>	Implementation	Context, TasksEnsure, TasksUtils		

		Public	✓	-
	taskCount	External		-
	taskStatistics	External		-
	getTask	Public		-
	getTasks	Public		-
	getManagingTasks	External		-
	getExecutingTasks	External		-
	createTask	External	✓	-
	applyForTask	External	✓	-
	acceptApplications	External	✓	-
	takeTask	External	✓	-
	createSubmission	External	✓	-
	reviewSubmission	External	✓	-
	cancelTask	External	✓	-
	acceptRequest	External	✓	-
	executeRequest	External	✓	-
	extendDeadline	External	✓	-
	increaseBudget	External	✓	-
	editMetadata	External	✓	-
	disable	External	✓	-
	refund	External	✓	-
	_getTask	Internal		
	_ensureNotDisabled	Internal		

	_ensureDisabled	Internal		
	_ensureDisabler	Internal		
<b>ITasks</b>	Interface			
	taskCount	External		-
	taskStatistics	External		-
	getTask	External		-
	getTasks	External		-
	getManagingTasks	External		-
	getExecutingTasks	External		-
	createTask	External	✓	-
	applyForTask	External	✓	-
	acceptApplications	External	✓	-
	takeTask	External	✓	-
	createSubmission	External	✓	-
	reviewSubmission	External	✓	-
	cancelTask	External	✓	-
	acceptRequest	External	✓	-
	executeRequest	External	✓	-
	extendDeadline	External	✓	-
	increaseBudget	External	✓	-
	editMetadata	External	✓	-



<b>Escrow</b>	Implementation			
	__Escrow_init	External	✓	-
	transfer	External	✓	-
<b>PreferredProxy</b>	Implementation	ERC1967Pro xy		
		Public	Payable	ERC1967Proxy
<b>ITokenMembers hip</b>	Interface			
	isMember	External		-
<b>TokenMajorityV otingBase</b>	Implementation	ITokenMajorit yVoting, Initializable, ERC165Upgr adeable, PluginUUPS Upgradeable , ProposalUpg radeable		
	__TokenMajorityVotingBase_init	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	vote	Public	✓	-
	execute	Public	✓	-
	getVoteOption	Public		-
	canVote	Public		-
	canExecute	Public		-
	isSupportThresholdReached	Public		-
	isSupportThresholdReachedEarly	Public		-

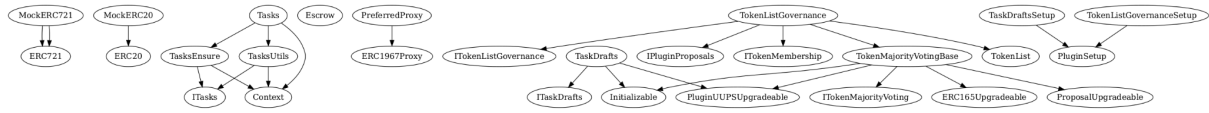
	isMinParticipationReached	Public		-
	supportThreshold	Public		-
	minParticipation	Public		-
	minDuration	Public		-
	minProposerVotingPower	Public		-
	votingMode	Public		-
	totalVotingPower	Public		-
	getProposal	Public		-
	updateVotingSettings	External	✓	auth
	createProposal	External	✓	-
	_vote	Internal	✓	
	_execute	Internal	✓	
	_canVote	Internal		
	_canExecute	Internal		
	_isProposalOpen	Internal		
	_updateVotingSettings	Internal	✓	
	_validateProposalDates	Internal		
<b>ITokenMajorityVoting</b>	Interface			
	supportThreshold	External		-
	minParticipation	External		-
	isSupportThresholdReached	External		-
	isSupportThresholdReachedEarly	External		-

	isMinParticipationReached	External		-
	canVote	External		-
	canExecute	External		-
	vote	External	✓	-
	execute	External	✓	-
	getVoteOption	External		-
<b>TaskDraftsSetup</b>	Implementation	PluginSetup		
		Public	✓	-
	prepareInstallation	External	✓	-
	prepareUninstallation	External		-
	implementation	External		-
<b>TaskDrafts</b>	Implementation	Initializable, PluginUUPS Upgradeable , ITaskDrafts		
	initialize	External	✓	initializer
	supportsInterface	Public		-
	getTasksContract	External		-
	getGovernanceContract	External		-
	updateAddresses	External	✓	auth
	createDraftTask	External	✓	-
<b>ITaskDrafts</b>	Interface			

	getTasksContract	External		-
	getGovernanceContract	External		-
	updateAddresses	External	✓	-
	createDraftTask	External	✓	-
<b>TokenListGovernanceSetup</b>	Implementation	PluginSetup		
		Public	✓	-
	prepareInstallation	External	✓	-
	prepareUninstallation	External		-
	implementation	External		-
<b>TokenListGovernance</b>	Implementation	TokenMajorityVotingBase, TokenList, ITokenMembership, ITokenListGovernance, IPluginProposals		
	initialize	External	✓	initializer
	supportsInterface	Public		-
	addMembers	External	✓	auth
	removeMembers	External	✓	auth
	totalVotingPower	Public		-
	createPluginProposal	External	✓	auth
	createProposal	External	✓	-
	isMember	External		-

	_createProposalBase	Internal	✓	
	_vote	Internal	✓	
	_canVote	Internal		
<b>TokenList</b>	Implementation			
	isListedAtBlock	Public		-
	isListed	Public		-
	tokenlistLengthAtBlock	Public		-
	tokenlistLength	Public		-
	_addTokens	Internal	✓	
	_removeTokens	Internal	✓	
<b>ITokenListGovernance</b>	Interface			
	addMembers	External	✓	-
	removeMembers	External	✓	-
<b>IPluginProposals</b>	Interface			
	createPluginProposal	External	✓	-

# Inheritance Graph



# Flow Graph



## Summary

Deeplink implements a governance model that is based on NFT holding voting power. This audit investigates security issues, business logic concerns, and potential improvements.



## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

## About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



**The Cyberscope team**

<https://www.cyberscope.io>