# Immutable Internal Contract Audit

# Contract Deployer

| | |
|---|---|
| **Internal Auditors** | Peter Robinson |
| **Assessment Date** | May 20, 2024 |
| **Final Report** | May 21, 2024 |

Previous audits:

- Feb 2023: Audit of Axelar’s deployer code: https://github.com/axelarnetwork/audits/blob/main/audits/2023-02%20Ackee%20Blockchain-3.pdf
- March 2024: Immutable internal audits: unpublished

# Contents

# Description

Immutable contracts currently use one of two deployer contracts, OwnableCreate2Deployer or OwnableCreate3Deployer contracts to deploy official contracts to testnet or mainnet. Currently, these contracts only allow a single deployer address, the owner, to deploy contracts through them. This is restrictive and there is a need to enhance this so as to allow a set of authorised addresses to deploy contracts.

AccessControlledDeployer contract has been introduced as a wrapper, forwarding deployment requests to the existing Create2 and Create3 deployers while layering role-based access controls to these capabilities. This contract could thus enable more flexible deployment access controls for existing single-owner Create2 and Create3 deployers.

# Scope

Commit: `24dc02426b0a9d2526d9750fa5452a650099a7d2`

Fix review commit: `eab4acb8e6469bbc98bbf94d1ed968f74085ffb3`

| Asset | Description |
|---|---|
| Smart Contracts | OwnableCreateDeploy.sol |
| | OwnableCreate2Deployer.sol<br>Which includes from Open Zeppelin (v4.9.3):<br>● Ownable.sol which imports:<br>○ Context.sol<br>While includes from Axelar (v5.8.0):<br>● Create2.sol which includes:<br>○ IDeploy.sol<br>○ ContractAddress.sol<br>● Deployer.sol which includes:<br>○ IDeploy.sol<br>○ SafeNativeTransfer.sol |
| | OwnableCreate3Deployer.sol which includes:<br>● OwnableCreate3.sol<br>○ OwnableCreate3Address.sol<br>○ OwnableCreateDeploy.sol<br>Which includes from Open Zeppelin (v4.9.3):<br>● Ownable.sol which imports:<br>○ Context.sol<br>While includes from Axelar (latest, assumed to be v5.8.0):<br>● IDeploy.sol<br>● ContractAddress.sol<br>● Deployer.sol which includes: |

| | |
|---|---|
| | ○ IDeploy.sol<br>○ SafeNativeTransfer.sol |
| | AccessControlledDeployer.sol<br><br>Which includes from Open Zeppelin (v4.9.3):<br>● AccessControlEnumerable.sol which imports:<br>○ AccessControl.sol<br>○ IAccessControl.sol<br>○ IAccessControlEnumerable.sol<br>○ EnumerableSet.sol<br>○ Context.sol<br>○ Strings.sol<br>○ Math.sol<br>○ SignedMath.sol<br>○ ERC165.sol<br>○ ERC2981.sol<br>○ IERC2981.sol<br>● Pausable.sol which imports:<br>○ Context.sol |

# Team’s Greatest Concerns

- The team would like a general review. They have no specific concerns.

# Basic Contract Analysis

The table below analyzes[1] the contracts.

| Type | File | Lines | nSLOC | Complexity |
|---|---|---|---|---|
| Contract | OwnableCreateDeploy | 35 | 15 | 28 |
| Contract | OwnableCreate2Deployer | 49 | 15 | 12 |
| Contract | OwnableCreate3Deployer | 53 | 15 | 12 |
| Contract | AccessControlledDeployer | 165 | 70 | 93 |

[1] Analysis produced using the Solidity Metrics VSCode extension.

# Smart Contracts

## OwnableCreateDeploy

Roles:

- Owner

External or Public Functions[2] that modify state:

| Function Name | Function Selector | Authorisation Check | Parameter Validation |
|---|---|---|---|
| deploy | 00774360 | Msg.sender must be the "owner". | bytecode: parameter length not checked. If bytecode is zero length, the create call will revert. |

External or Public Functions that do not modify state: None.

Upgradeable checks: This contract is not upgradeable.

## OwnableCreate2Deployer

Roles:

- Owner

External or Public Functions that modify state:

| Function Name | Function Selector | Authorisation Check | Parameter Validation |
|---|---|---|---|
| deploy | 4af63f02 | Msg.sender must be the "owner" | bytecode: parameter length zero checked here.<br>salt: No check needed. |
| deployAndInit | cf4d6432 | Msg.sender must be the "owner" | bytecode: parameter length zero checked here.<br>salt: No check needed.<br>init: Not checked. Will revert if init code is not valid bytecode. |
| renounceOwnership | 715018a6 | Msg.sender must be the "owner" | No checks. |
| transferOwnership | f2fde38b | Msg.sender must be the "owner" | newOwner: Address can't be zero. |

External or Public Functions that do not modify state:

[2] The list of functions was determined using `forge inspect OwnableCreateDeploy methods`

| Function Name | Function Selector | Notes |
|---|---|---|
| deployedAddress | c2b1041c | Returns the address where a contract will be stored if deployed via {deploy} or {deployAndInit} by `sender`. |
| owner | 8da5cb5b | Returns the address of the current owner. |

Upgradeable checks: This contract is not upgradeable.

# OwnableCreate3Deployer

Roles:

- Owner

External or Public Functions that modify state:

| Function Name | Function Selector | Authorisation Check | Parameter Validation |
|---|---|---|---|
| deploy | 4af63f02 | Msg.sender must be the “owner” | bytecode: parameter length zero checked here.<br>salt: No check needed. |
| deployAndInit | cf4d6432 | Msg.sender must be the “owner” | bytecode: parameter length zero checked here.<br>salt: No check needed.<br>init: Not checked. Will revert if init code is not valid bytecode. |
| renounceOwnership | 715018a6 | Msg.sender must be the “owner” | No checks. |
| transferOwnership | f2fde38b | Msg.sender must be the “owner” | newOwner: Address can’t be zero. |

External or Public Functions that do not modify state:

| Function Name | Function Selector | Notes |
|---|---|---|
| deployedAddress | c2b1041c | Returns the address where a contract will be stored if deployed via {deploy} or {deployAndInit} by `sender`. |
| owner | 8da5cb5b | Returns the address of the current owner. |

Upgradeable checks: This contract is not upgradeable.

# AccessControlledDeployer

Roles:

- DEFAULT_ADMIN_ROLE: Role administrator for PAUSER_ROLE, UNPAUSER_ROLE, and DEPLOYER_ROLE; plus right to upgrade ownership of a Deployer contract using transferOwnershipOfDeployer.
- DEPLOYER_ROLE: Deploy contracts.
- PAUSER_ROLE: Halt deployments.
- UNPAUSER_ROLE: Re-commence deployments.

External or Public Functions[3] that modify state:

| Function Name | Function Selector | Authorisation Check | Parameter Validation |
|---|---|---|---|
| deploy | 37e9ccea | Not paused & only DEPLOYER_ROLE | deployer: Checks not address 0.<br>bytecode: Delegated to OwnableCreate2Deployer or OwnableCreate3Deployer.<br>salt: Delegated to OwnableCreate2Deployer or OwnableCreate3Deployer. |
| deployAndInit | 3051b2df | Not paused & only DEPLOYER_ROLE | deployer: Checks not address 0.<br>bytecode: Delegated to OwnableCreate2Deployer or OwnableCreate3Deployer.<br>salt: Delegated to OwnableCreate2Deployer or OwnableCreate3Deployer.<br>init: Delegated to OwnableCreate2Deployer or OwnableCreate3Deployer. |
| grantDeployerRole | e2345dfe | Delegated to grantRole function. | deployers: Checks not length 0 and each deployer is not address 0. |
| grantRole | 2f2ff15d | Msg.sender must be the role admin for the role | role: No check needed.<br>account: No check needed. |
| pause | 8456cb59 | Only PAUSER role. | No parameters |
| renounceRole | 36568abe | Msg.sender can only remove their own access. | role: No check needed.<br>callerConfirmation: Checks is same as msg.sender |
| revokeDeployerRole | f028fc30 | Delegated to revokeRole function. | deployers: Checks not length 0 and each deployer is not address 0. |
| revokeRole | d547741f | Msg.sender must be role admin for the role being revoked. For DEFAULT_ADMIN_ROLE, they must be another account with DEFAULT_ADMIN_ROLE. | role: No check needed.<br>account: No check needed. |
| transferOwnershipOf Deployer | ebd6843b | Only DEFAULT_ADMIN_ROLE | ownableDeployer: Checked not address 0. Owner is called, which will revert if not a deployer contract.<br>newOwner: Check not address 0. |
| unpause | 3f4ba83a | Only UNPAUSER role. | No parameters |

External or Public Functions that do not modify state:

[3] The list of functions was determined using `forge inspect ImmutableSignedZoneV2 methods`

| Function Name | Function Selector | Notes |
|---|---|---|
| DEFAULT_ADMIN_ROLE | a217fddf | Role identifier for those who can administer the contract and other roles |
| DEPLOYER_ROLE | ecd00261 | Role identifier for those who can deploy contracts |
| PAUSER_ROLE | e63ab1e9 | Role identifier for those who can pause the deployer |
| UNPAUSER_ROLE | fb1bb9de | Role identifier for those who can unpause the deployer |
| getRoleAdmin | 248a9ca3 | Returns the admin role that controls role. |
| getRoleMember | 9010d07c | Returns one of the accounts that have `role`. |
| getRoleMemberCount | ca15c873 | Returns the number of accounts that have `role`. |
| hasRole | 91d14854 | Returns true if account has been granted role. |
| paused | 5c975abb | Returns true if the contract is paused, and false otherwise. |
| supportsInterface | 01ffc9a7 | Returns true if this contract implements the interface defined by `interfaceId`. |

Upgradeable checks: This contract is not upgradeable.

# Abuser Test Cases and Findings

## transferOwnershipOfDeployer controlled by DEFAULT_ADMIN_ROLE

Classification: Minor

Description: The DEFAULT_ADMIN_ROLE is role administrator, and a configuration admin. It should just be a role administrator. Configuration roles should be separate.

Action: Create a new admin role for calling transferOwnershipOfDeployer.

Status: Team actioned as proposed.

Fix review: New separate admin created OWNERSHIP_MANAGER_ROLE.

# Code Review Comments

AccessControlledDeployer.sol:

- Please add a contract level comment explaining what the contract does, and the approach to upgrade (deploy a new contract and call transferOwnershipOfDeployer).
- Comment addressed.

OwnableCreate3Address.sol:

- OwnableCreate3Address.sol should be abstract. Users of the contract repo could inadvertently deploy this contract. Their intended usage is to be extended and used as a part of OwnableCreate3Deployer.
- Comment addressed.