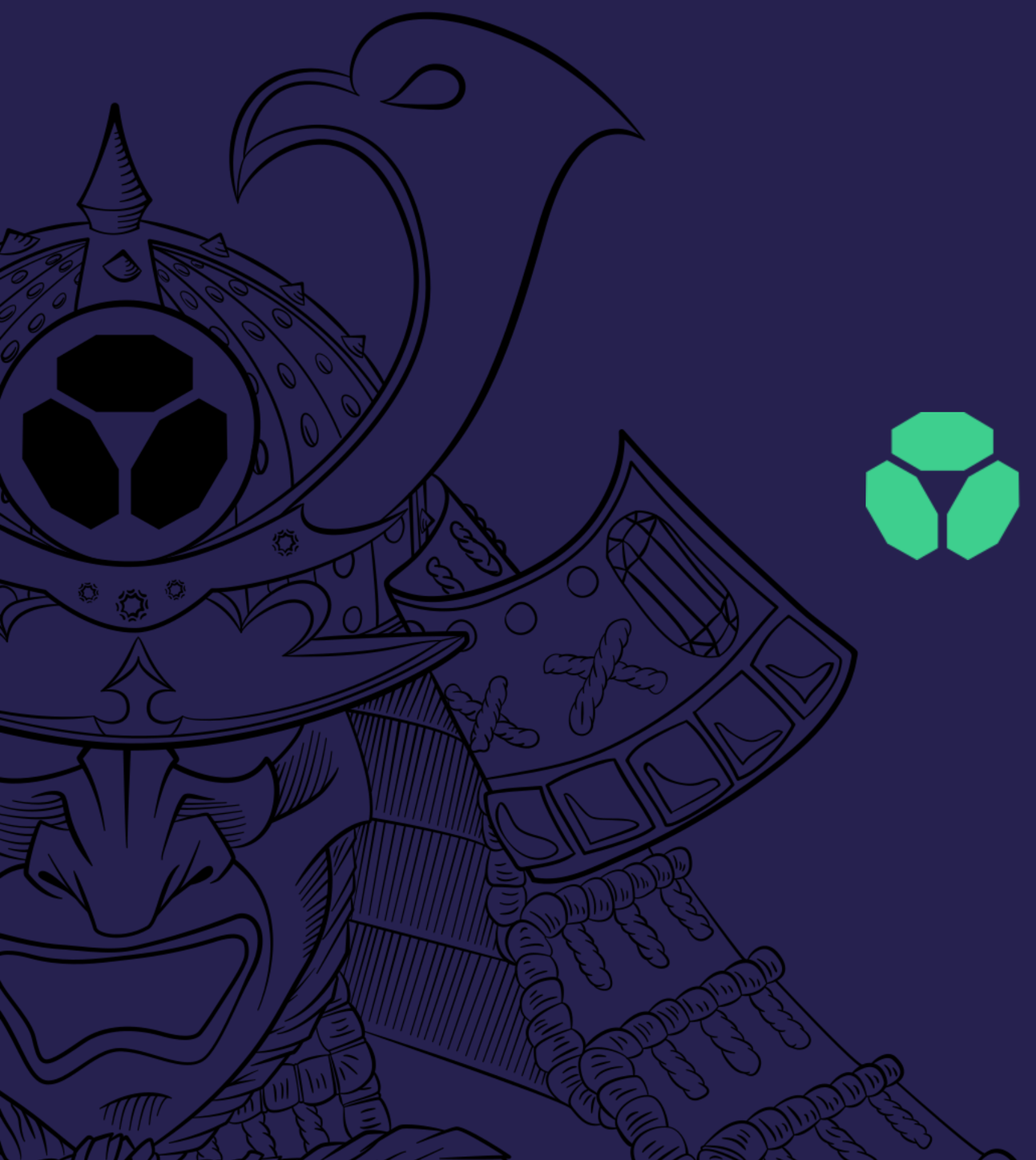


smart state

> Smart
Contract
Audit #

XENUM

Feb 11
2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

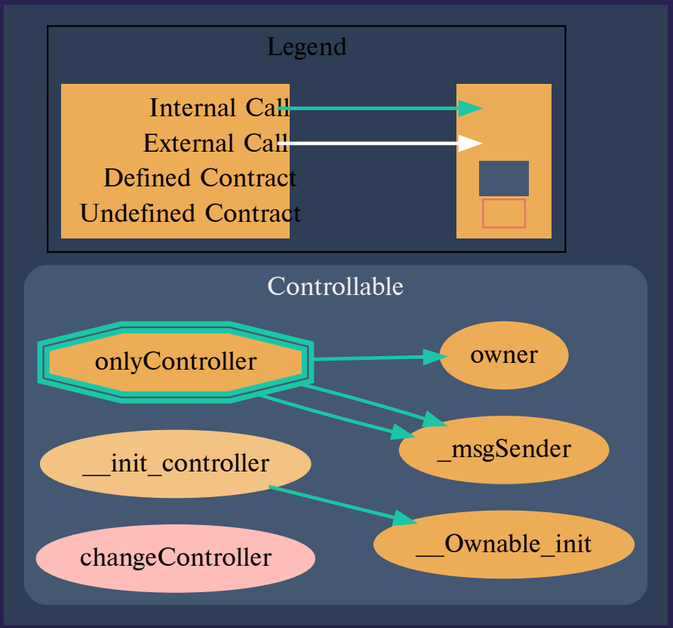
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Pool Asset Security (backdoors in the underlying ERC-20)
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

STRUCTURE OF CONTRACT

CONTROLLABLE.SOL

CONTRACT METHODS ANALYSIS:

- __init_controller(address _controller)
  Vulnerabilties not detected
- changeController(address _controller)
  Function should emit an event



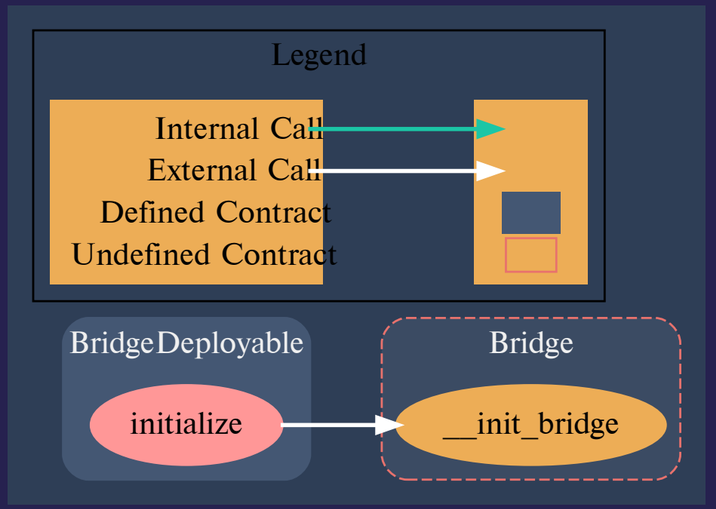
Pic. 1.1
Controllable.sol

STRUCTURE OF CONTRACT

BRIDGEDEPLOYABLE.SOL

CONTRACT METHODS ANALYSIS:

- initialize(address _controller)
  Vulnerabilties not detected



Pic. 1.2
BridgeDeployable.sol

STRUCTURE OF CONTRACT

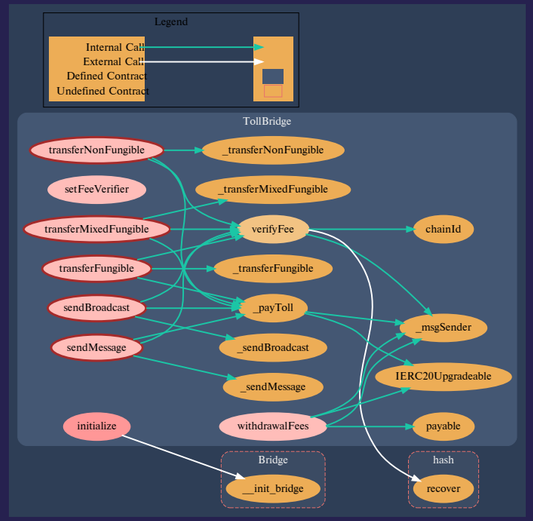
TOLLBRIDGE.SOL

CONTRACT METHODS ANALYSIS:

- initialize(address _controller, address _verifier)
  Vulnerabilties not detected

- setFeeVerifier(address _newVerifier) external onlyOwner
  Function should emit an event

- verifyFee(
  uint256 _destination,
  bytes memory _messageWithReceiptRequestAndTo, // This will be abi.encode(message, receipt, recipient) where `message` is the bytes of the message, and `receipt` is a bool that says weather or not a delivery receipt is requested
  bytes calldata _feeData
)
  Vulnerabilities not detected



Pic. 1.3
TollBridge.sol

PAYABLE

- transferFungible(
  address _token,
  uint256 _amount,
  uint256 _networkId,
  bytes calldata _feeData
)

Vulnerabilties not detected

Tokens in

PAYABLE

- transferMixedFungible(
  address _token,
  uint256 _tokenId,
  uint256 _amount,
  uint256 _networkId,
  bytes calldata _feeData
)

Vulnerabilities not detected

Tokens in

PAYABLE

- transferNonFungible(
  address _token,
  uint256 _tokenId,
  uint256 _networkId,
  bytes calldata _feeData
)

Vulnerabilties not detected

Tokens in

PAYABLE

- sendMessage(
  uint256 _messageId,
  uint256 _destination,
  string calldata _recipient,
  bool _receipt,
  bytes calldata _message,
  bytes calldata _feeData
)

Vulnerabilities not detected

Tokens in

PAYABLE

- sendBroadcast(
  uint256 _messageId,
  bool _receipt,
  bytes calldata _message,
  bytes calldata _feeData
)

  Vulnerabilties not detected

ETH in

PAYABLE

- withdrawalFees(address _token,
  uint256 _amount)

  Vulnerabilties not detected

ETH out

- _payToll(bytes calldata _feeData)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

BRIDGE.SOL

CONTRACT METHODS ANALYSIS:

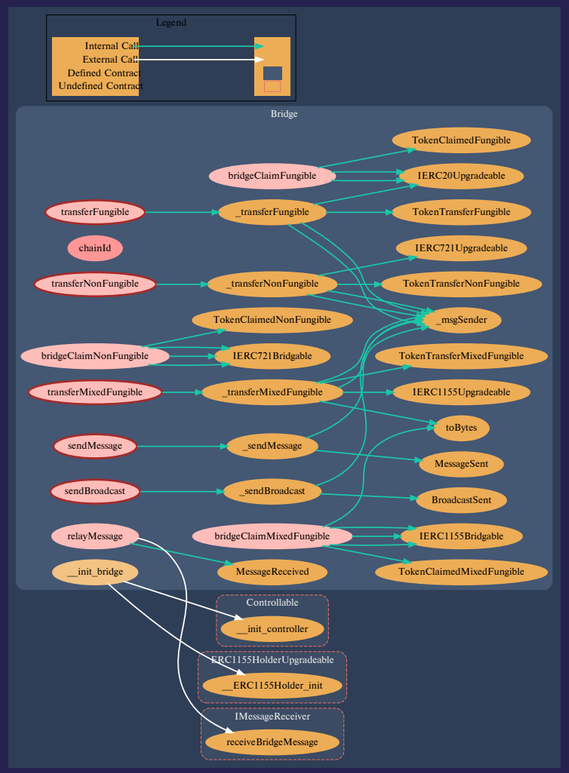
- __init_bridge(address _controller)
  Vulnerabilties not detected

- chainId() public view returns (uint256)
  Vulnerabilties not detected

PAYABLE

- transferFungible(
  address token,
  uint256 amount,
  uint256 networkId,
  bytes calldata
)
  Vulnerabilties not detected

Tokens in



Pic. 1.4
Bridge.sol

PAYABLE

- bridgeClaimFungible(
  address _token,
  address _to,
  uint256 _amount
)

Vulnerabilties not detected

Tokens out

PAYABLE

- bridgeClaimNonFungible(
  address _token,
  address _to,
  uint256 _tokenId
)

Vulnerabilities not detected

Tokens out

PAYABLE

- transferNonFungible(
  address _token,
  uint256 _tokenId,
  uint256 _networkId,
  bytes calldata
)

Vulnerabilties not detected

Tokens in

PAYABLE

- transferMixedFungible(
  address _token,
  uint256 _tokenId,
  uint256 _amount,
  uint256 _networkId,
  bytes calldata
)

Vulnerabilities not detected

Tokens in

PAYABLE

- bridgeClaimMixedFungible(
  address token,
  address to,
  uint256 tokenId,
  uint256 amount
)

  Vulnerabilities not detected

Tokens out

- sendMessage(
  uint256 _messageId,
  uint256 _destination,
  string calldata _recipient,
  bool _receipt,
  bytes calldata _message,
  bytes calldata
)

  Vulnerabilties not detected

- sendBroadcast(
  uint256 _messageId,
  bool _receipt,
  bytes calldata _message,
  bytes calldata
)

  Vulnerabilties not detected

- relayMessage(
  IMessageReceiver _recipient,
  uint256 _messageId,
  string calldata _sender,
  uint256 _fromNetworkId,
  bool _receipt,
  bytes calldata _message
)

  Vulnerabilties not detected

- toBytes(uint256 x) internal pure returns (bytes memory b)
  Vulnerabilties not detected

- _transferFungible(address token, uint256 amount, uint256 networkId)
  Vulnerabilties not detected

- _transferNonFungible(address _token, uint256 _tokenId, uint256 _networkId)
  Vulnerabilties not detected

- _transferMixedFungible(
    address _token,
    uint256 _tokenId,
    uint256 _amount,
    uint256 _networkId
)
  Vulnerabilties not detected

- _sendMessage(
    uint256 _messageId,
    uint256 _destination,
    string calldata _recipient,
    bool _receipt,
    bytes calldata _message
)
  Vulnerabilties not detected

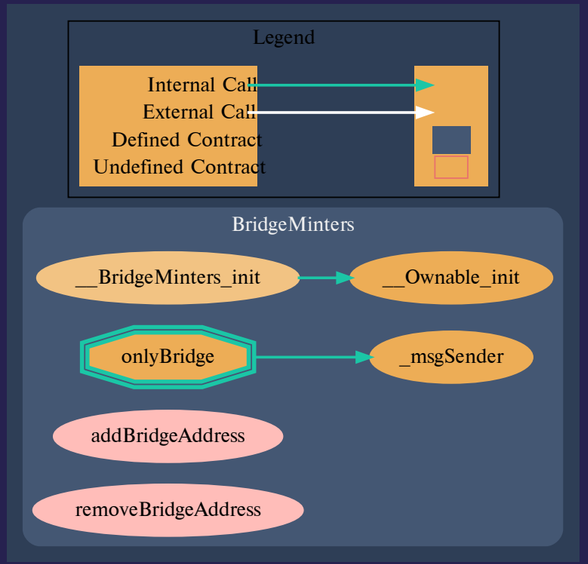
- _sendBroadcast(
    uint256 _messageId,
    bool _receipt,
    bytes calldata _message
)
  Vulnerabilties not detected

STRUCTURE OF CONTRACT

UTILS/BRIDGEMINTERS.SOL

CONTRACT METHODS ANALYSIS:

- __BridgeMinters_init()
  Vulnerabilties not detected
- addBridgeAddress(address _bridge)
  Vulnerabilities not detected
- removeBridgeAddress(address _bridge)
  Vulnerabilities not detected



Pic. 1.5
utils/BridgeMinters.sol

STRUCTURE OF CONTRACT

TOKENS/ERC721BRIDGABLE.SOL

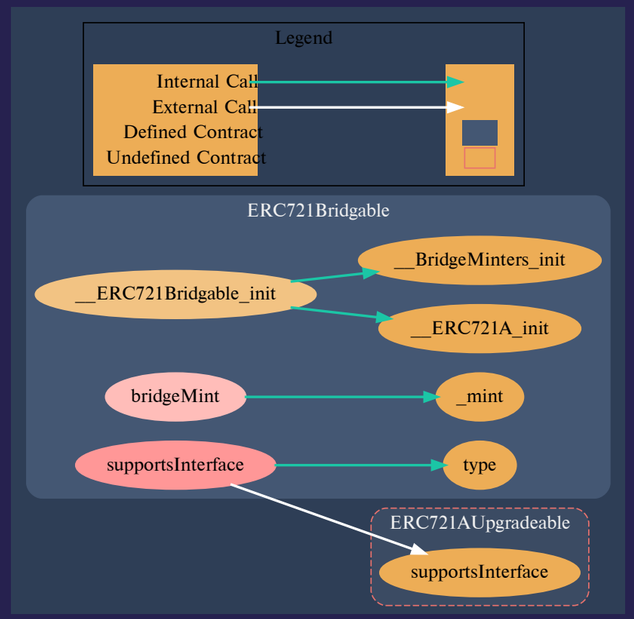
CONTRACT METHODS ANALYSIS:

- __ERC721Bridgable_init(
  string memory _name,
  string memory _symbol,
  uint256 _maxBatch
)

  Vulnerabilties not detected

- supportsInterface(
  bytes4 interfaceId
)

  Vulnerabilties not detected



Pic. 1.6
tokens/ERC721Bridgable.sol

- bridgeMint(
  address _recipient,
  uint256 _id,
  bytes calldata _verification
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

TOKENS/ERC721BRIDGABLE-USERMINTING.SOL

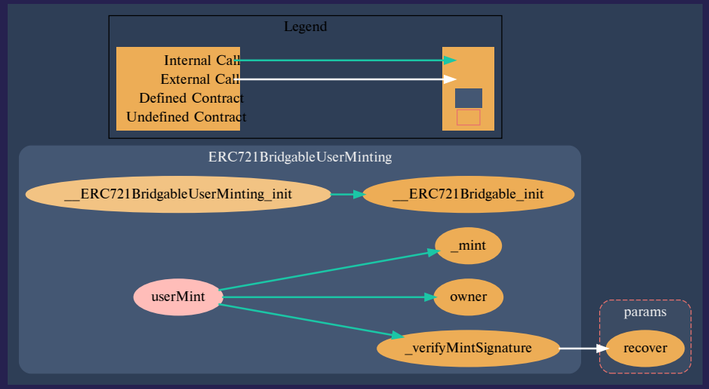
CONTRACT METHODS ANALYSIS:

- __ERC721BridgableUserMinting_init(
  string memory _name,
  string memory _symbol,
  uint256 _maxBatch
)

  Vulnerabilties not detected

- userMint(
  address _recipient,
  uint256 _id,
  uint256 _nonce,
  bytes calldata _verification
)

  Vulnerabilties not detected



Pic. 1.7
tokens/ERC721BridgableUserMinting.sol

- _verifyMintSignature(
  address _recipient,
  uint256 _id,
  uint256 _nonce,
  bytes calldata _verification,
  address _expectedSigner
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

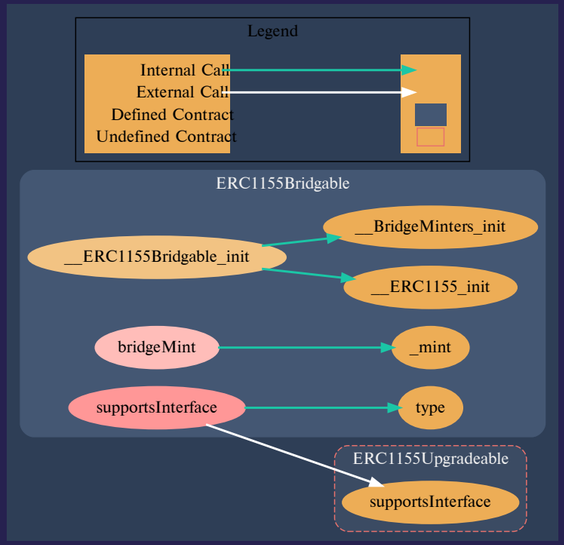
TOKENS/ERC1155BRIDGABLE.SOL

CONTRACT METHODS ANALYSIS:

- __ERC1155Bridgable_init(string memory _uri)
  Vulnerabilties not detected

- supportsInterface(
    bytes4 interfaceId
)
  Vulnerabilities not detected

- bridgeMint(
    address _recipient,
    uint256 _id,
    uint256 _amount,
    bytes calldata _data,
    bytes calldata _verification
)
  Vulnerabilities not detected



Pic. 1.8
tokens/ERC1155Bridgable.sol

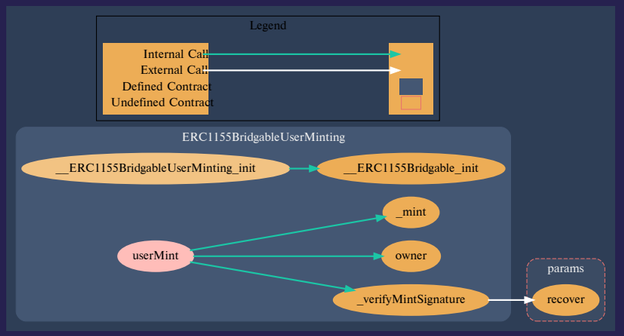
STRUCTURE OF CONTRACT

TOKENS/ERC1155BRIDGABLEUSERMINTING.SOL

CONTRACT METHODS ANALYSIS:

- __ERC1155BridgableUserMinting_init(string memory _uri)
  Vulnerabilties not detected

- userMint(
  address _recipient,
  uint256 _id,
  uint256 _amount,
  bytes calldata _data,
  uint256 _nonce,
  bytes calldata _verification
)
  Vulnerabilities not detected



Pic. 1.8

tokens/
ERC1155BridgableUserMinting.sol

- _verifyMintSignature(
  address _recipient,
  uint256 _id,
  uint256 _amount,
  bytes calldata _data,
  uint256 _nonce,
  bytes calldata _verification,
  address _expectedSigner
)

  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
Controllable.sol	9da51a7becae07e038189a6f9a4b0554922b062228e7d41aa3c336f39668c6b3
BridgeDeployable.sol	d96ddf5d77f0ef09133e5d3a3e7983a298f50d13b14e93b61d3d0621e50708d0
TollBridge.sol	97191850cb8bde3a7be2403fa45c1ad77fca71ddc69ff407b11d60135dcdde33
Bridge.sol	5df2a083897ddd29589c2ac815079eb7c414391810c80f93de106fa32b76d585

Contract Name	Bytecode hash (SHA 256)
tokens/ERC721Bridgable.sol	70d95666e38b4464594f70c0edec534142d88541271b6500e45d8e57fc79a9db
tokens/ERC721BridgableUserMinting.sol	9d861d0f0528cfba00841d04dc26e7a2d860b9c53be92e1dcb0c773ad448dccf
tokens/ERC1155Bridgable.sol	bc2bc70b6133bec34fc1e2fcb28c661b75b20c803bb60ca0c049454bf31947dc
tokens/ERC1155BridgableUserMinting.sol	06b5a5d0be8825de9a7bc9547b5c89483b6d7117efedd89f054da15e26b8c37f

Get In Touch

info@smartstate.tech

smartstate.tech