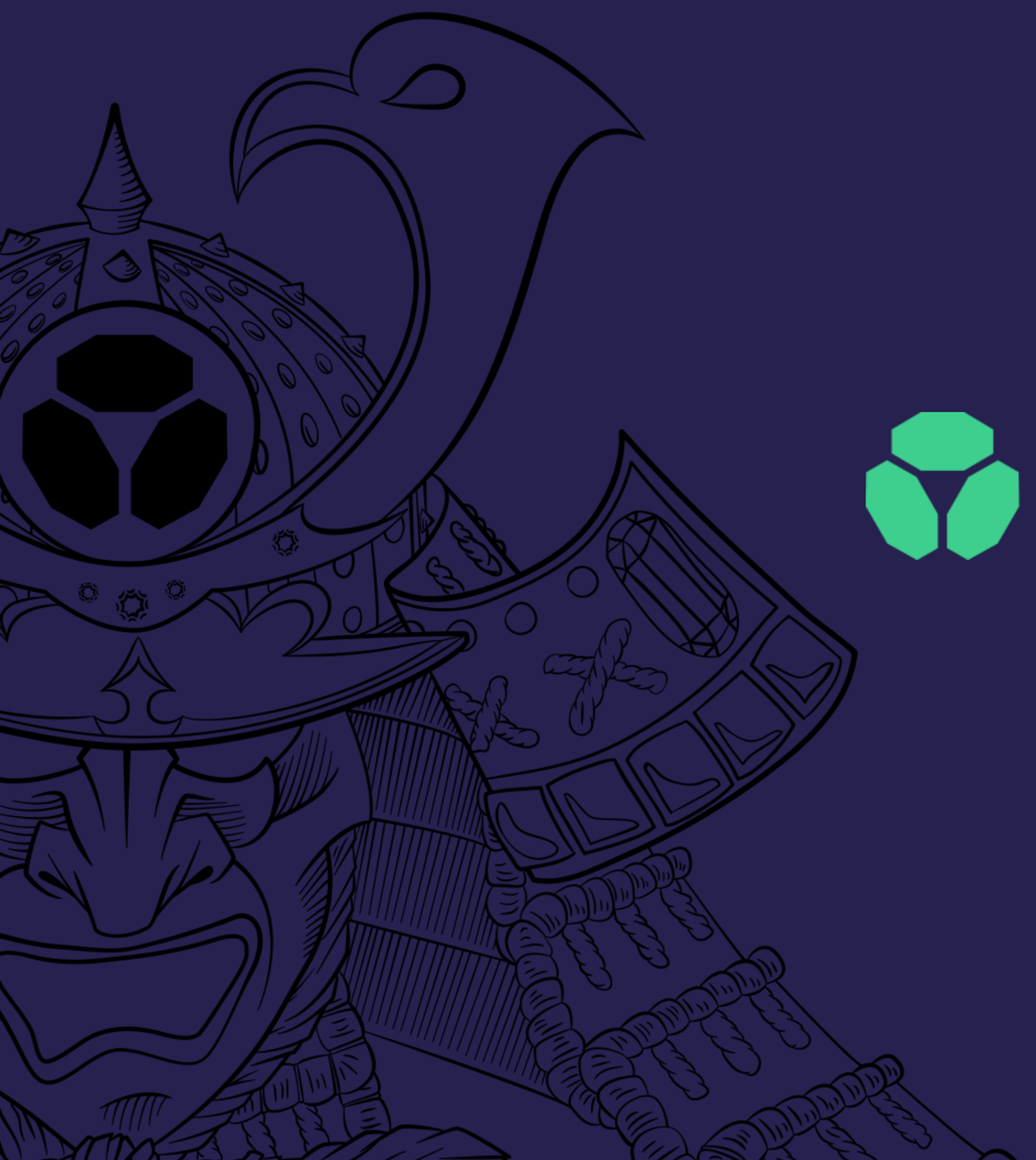


smart state

> Smart
Contract
Audit #

AXEs

METAVERSE

Dec 16
2021

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

- Best code practices
- ERC20/BEP20 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

AXES721.SOL

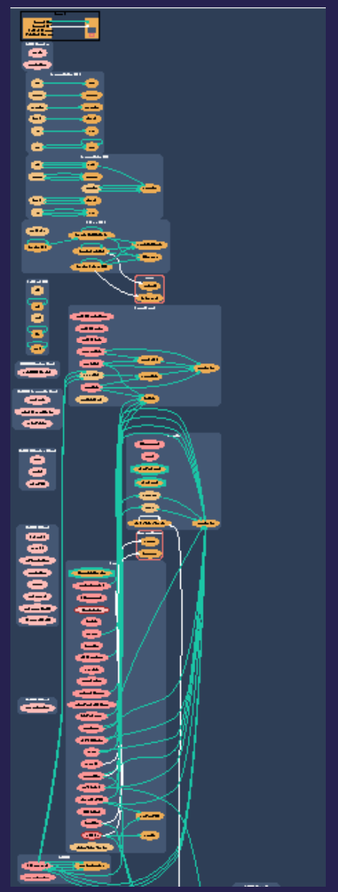
CONTRACT METHODS ANALYSIS:

- startStopItemsSale () public virtual returns (bool success)
  Function can be declared external. Function should emit an event.

- itemInfo(string memory _item) public view returns (uint _price, bool _active)
  Vulnerabilities not detected

- addChangeItem(string memory _item, uint _price, bool _item_bool)
  Vulnerabilities not detected

- itemsList() public view returns (string[] memory)
  Vulnerabilities not detected



Pic. 1.1
Axes721.sol

- setItemsAddresses(address _contract, address _withdraw)
  Vulnerabilities not detected

- seasonInfo(uint256 seasonId)
  Vulnerabilities not detected

- seasonOptions(uint256 seasonId)
  Vulnerabilities not detected

- currentId() public view returns (uint _ currentId)
  Vulnerabilities not detected

- tokensBoughtByAddress(uint256 _season, address _buyer)
  Function can be declared external

- saleMint(address _to, uint _season)
  Vulnerabilities not detected

- itemMint(address to, string memory _item)
  Vulnerabilities not detected

- systemMint(address to, string memory _item)
  Vulnerabilities not detected

- initNewSeason(uint _seasonStart, uint _seasonStop, uint _seasonPrice, uint _ seasonAmount, bool _whitelist, address _withdraw, address _tokenContract, string memory _ seasonItem, string memory _seasonName, uint _tokensPerBuyer)
  Vulnerabilities not detected

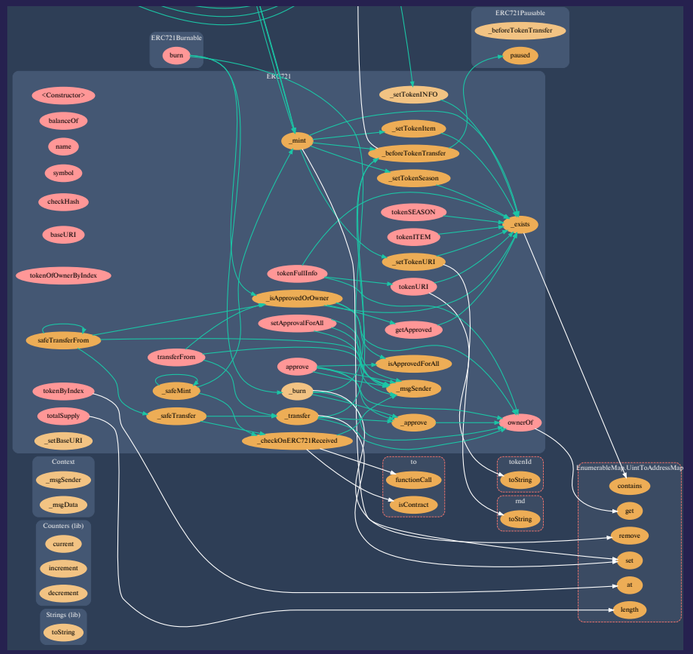
- resetSeason(uint _season)
  Vulnerabilities not detected
- changeBaseURI(string memory baseURI)
  Vulnerabilities not detected
- setTokenInfo(uint256 tokenId, string memory tokenData)
  Vulnerabilities not detected
- addToWhitelist(address[] memory _address, uint _season)
  Vulnerabilities not detected
- isWhitelisted(address _address, uint256 _season)
  Vulnerabilities not detected
- pause()
  Vulnerabilities not detected
- unpause()
  Vulnerabilities not detected
- _beforeTokenTransfer(address from, address to, uint256 tokenId)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

ERC721.SOL

CONTRACT METHODS ANALYSIS:

- balanceOf(address owner)
  Vulnerabilities not detected
- ownerOf(uint256 tokenId)
  Vulnerabilities not detected
- name()
  Vulnerabilities not detected
- symbol()
  Vulnerabilities not detected
- tokenURI(uint256 tokenId)
  Vulnerabilities not detected



Pic. 1.2
ERC721.sol

- tokenFullInfo(uint256 tokenId)
  Vulnerabilities not detected
- tokenITEM(uint256 tokenId)
  Vulnerabilities not detected
- tokenSEASON(uint256 tokenId)
  Vulnerabilities not detected
- checkHash(string memory _key)
  Vulnerabilities not detected
- tokenOfOwnerByIndex(address owner, uint256 index)
  Vulnerabilities not detected
- totalSupply()
  Vulnerabilities not detected
- tokenByIndex(uint256 index)
  Vulnerabilities not detected
- approve(address to, uint256 tokenId)
  Vulnerabilities not detected
- getApproved(uint256 tokenId)
  Vulnerabilities not detected
- setApprovalForAll(address operator, bool approved)
  Vulnerabilities not detected

- isApprovedForAll(address owner, address operator)
  Vulnerabilities not detected

- transferFrom(address from, address to, uint256 tokenId)
  Vulnerabilities not detected

- safeTransferFrom(address from, address to, uint256 tokenId)
  Vulnerabilities not detected

- safeTransferFrom(address from, address to, uint256 tokenId, bytes memory _data)
  Vulnerabilities not detected

- _safeTransfer(address from, address to, uint256 tokenId, bytes memory _data)
  Vulnerabilities not detected

- _exists(uint256 tokenId)
  Vulnerabilities not detected

- _isApprovedOrOwner(address spender, uint256 tokenId)
  Vulnerabilities not detected

- _safeMint(address to, uint256 tokenId)
  Vulnerabilities not detected

- _safeMint(address to, uint256 tokenId, bytes memory _data)
  Vulnerabilities not detected

- _mint(address to, uint256 tokenId, string memory mintItem, uint _season)
  Vulnerabilities not detected

- _burn(uint256 tokenId)
  Vulnerabilities not detected

- _transfer(address from, address to, uint256 tokenId)
  Vulnerabilities not detected

- _setTokenURI(uint256 tokenId)
  Vulnerabilities not detected

- _setTokenSeason(uint tokenId, uint _season)
  Vulnerabilities not detected

- _setTokenINFO(uint256 tokenId, string memory tokenInfo)
  Vulnerabilities not detected

- _setTokenItem(uint256 tokenId, string memory tokenItem)
  Vulnerabilities not detected

- setBaseURI(string memory baseURI_)
  Vulnerabilities not detected

- _checkOnERC721Received(address from, address to, uint256 tokenId, bytes memory _data)
  Vulnerabilities not detected

- _beforeTokenTransfer(address from, address to, uint256 tokenId)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
Axes721	0.7.6	200	ceed0b8ac075867301ecc64460c40cf223ae4823145795ee903fe70ec1a589f8

Get In Touch

info@smartstate.tech

smartstate.tech