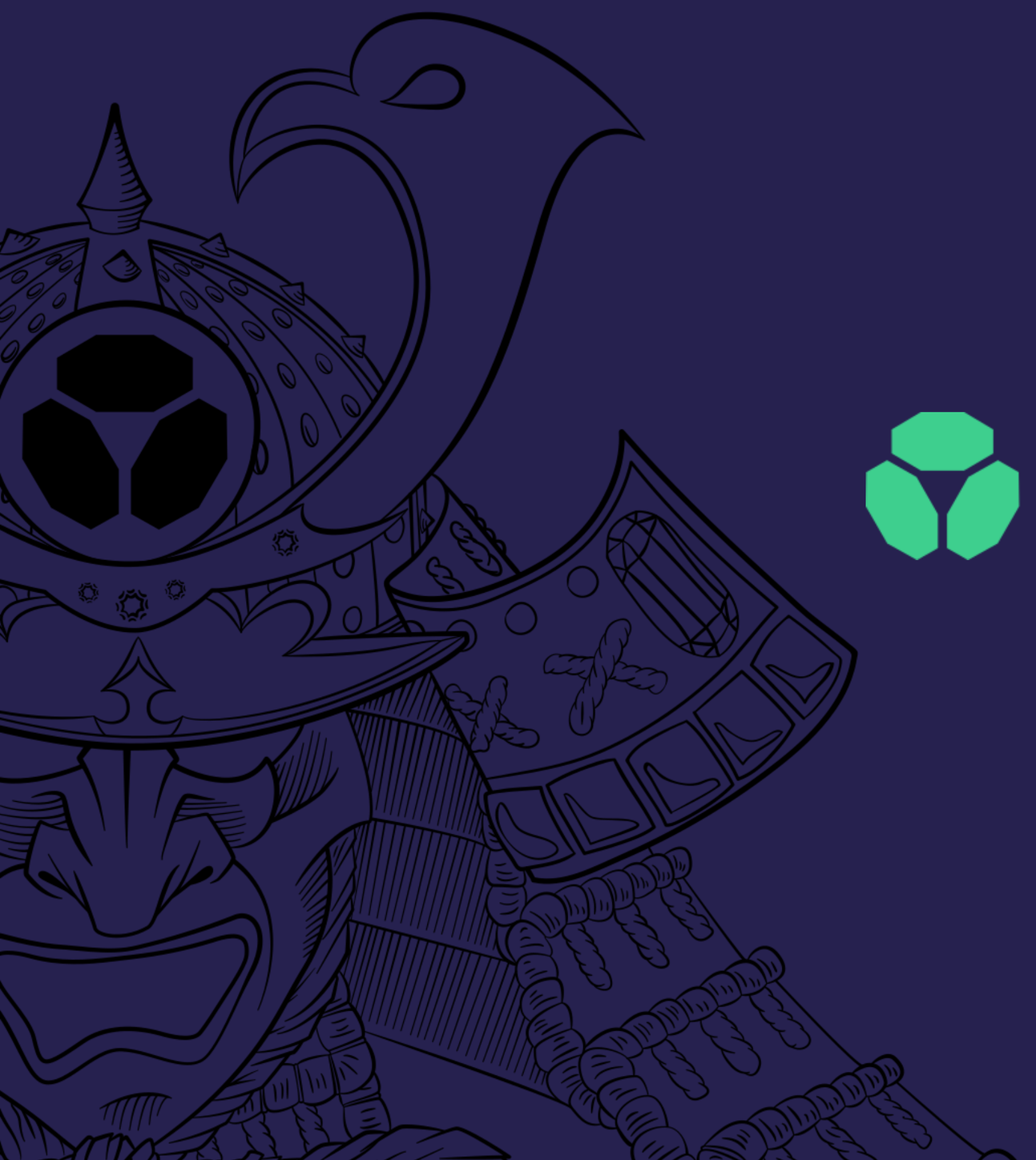


smart state

> Smart
Contract
Audit #

Mar 18
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

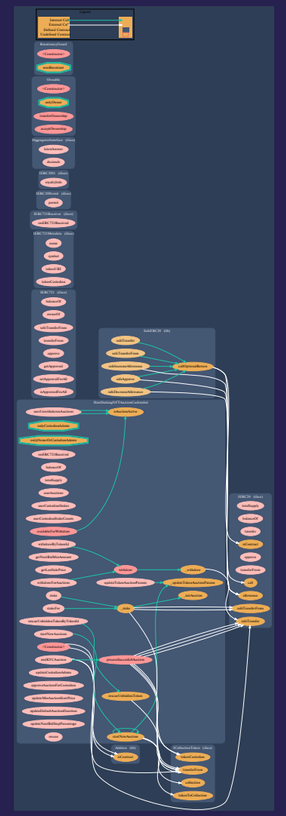
HARDSTAKINNFTAUCTION-CUSTODIALTOKEN.SOL

CONTRACT METHODS ANALYSIS:

- onERC721Received(address operator, address from, uint256 tokenId, bytes calldata data) external pure override returns (bytes4)
  Vulnerabilties not detected

- balanceOf(address account) external view returns (uint)
  Vulnerabilities not detected

- totalSupply() external view returns (uint)
  Vulnerabilities not detected



Pic. 1.1

HardStakinNFTAuctionCustodialToken.sol

- userAuctions(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected
- userCustodianStakes(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected
- userCustodianStakeCounts(address user) external view returns (uint)
  Vulnerabilities not detected
- userUnwithdrawnAuctions(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected
- availableForWithdraw(address user, uint auctionId) public view returns (uint stake)
  Vulnerabilities not detected
- getNextBidMinAmount(uint auctionId) external view returns (uint nextBid)
  Vulnerabilities not detected
- isAuctionActive(uint auctionId) public view returns (bool)
  Vulnerabilities not detected
- getLastSalePrice(uint tokenId) external view returns (uint)
  Vulnerabilities not detected

PAYABLE

- stake(uint auctionId, uint amount)
  Vulnerabilties not detected

Tokens in, public

- stakeFor(uint auctionId, uint amount, address user)
  Vulnerabilties not detected

PAYABLE

- withdraw(uint auctionId)
  Vulnerabilties not detected

Tokens out, public

- withdrawByTokenId(uint tokenId)
  Vulnerabilties not detected

- withdrawForAuctions(uint[] memory auctionIds)
  Vulnerabilties not detected

PAYABLE

- processSuccesfullAuction(uint auctionId)
  Vulnerabilties not detected

NFT out, tokens out, public

PAYABLE

- endKYCAuction(uint auctionId, bool kycResult)
  Vulnerabilties not detected

NFT out, tokens out, onlyCustodianAdmin

- startNewAuctions(uint[] memory tokenIds, uint[] memory startBidAmounts, AuctionType[] memory auctionTypes, string[] memory descriptions)
  Vulnerabilties not detected

- startNewAuction(uint tokenId, uint startBidAmount, uint roundDuration, uint successAuctionFeePercentage, string memory description, AuctionType auctionType)
  Vulnerabilties not detected

PAYABLE

- startNewAuction(uint tokenId, uint startBidAmount, string memory description, AuctionType auctionType)
  Vulnerabilties not detected

NFT in, public

- rescueUnbiddenTokenByTokenId(uint tokenId)
  Vulnerabilties not detected

PAYABLE

- rescueUnbiddenToken(uint auctionId)
  Vulnerabilties not detected

NFT out, public

- _stake(uint auctionId, uint amount, address user)
  Vulnerabilties not detected

- _withdraw(uint auctionId)
  Vulnerabilties not detected

- _initAuction(uint auctionId)
  Vulnerabilties not detected

- updateCustodianAdmin(address newAdmin)
  Vulnerabilties not detected

- approveAuctionForCustodian(uint auctionId, bool isApproved)
  Vulnerabilties not detected

- updateMinAuctionStartPrice(uint newMinAuctionStartPrice)
  Vulnerabilties not detected

- updateDefaultAuctionDuration(uint newDefaultAuctionDuration)
  Vulnerabilties not detected

- updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage, AuctionType auctionType)
  Vulnerabilties not detected

- _updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage, AuctionType auctionType)
  Vulnerabilties not detected

- updateNextBidStepPercentage(uint newNextBidStepPercentage)
  Vulnerabilties not detected

- rescue(address to, address tokenAddress, uint amount)
  Vulnerabilties not detected

STRUCTURE OF CONTRACT

UNCIRON.SOL

CONTRACT METHODS ANALYSIS:

- onERC721Received(address operator, address from, uint256 tokenId, bytes calldata data) external pure override returns (bytes4)
  Vulnerabilties not detected

- balanceOf(address account) external view returns (uint)
  Vulnerabilities not detected

- totalSupply() external view returns (uint)
  Vulnerabilities not detected

- userAuctions(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected

- userCustodianStakes(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected

- userCustodianStakeCounts(address user) external view returns (uint)
  Vulnerabilities not detected

- userUnwithdrawnAuctions(address user) external view returns (uint[] memory auctionIds)
  Vulnerabilities not detected

- availableForWithdraw(address user, uint auctionId) public view returns (uint actualStake)
  Vulnerabilities not detected

- getNextBidMinAmount(uint auctionId) external view returns (uint actualBid, uint convertedBid)
  Vulnerabilities not detected

- isAuctionActive(uint auctionId) public view returns (bool)
  Vulnerabilities not detected

- getRate() public view returns (uint)
  Vulnerabilities not detected

- getAmountEthToUsd(uint amountEth) public view returns (uint)
  Vulnerabilties not detected

- getAmountEthToUsd(uint amountEth, uint rate) public pure returns (uint)
  Vulnerabilties not detected

- getAmountUsdToEth(uint amountUsd) public view returns (uint)
  Vulnerabilties not detected

- getAmountUsdToEth(uint amountUsd, uint rate) public pure returns (uint)
  Vulnerabilties not detected

- getLastSalePrice(uint tokenId) external view returns (uint)
  Vulnerabilties not detected

- stake(uint auctionId)
  Vulnerabilties not detected

- stakeFor(uint auctionId, address user)
  Vulnerabilties not detected

- withdraw(uint auctionId)
  Vulnerabilties not detected

- withdrawByTokenId(uint tokenId)
  Vulnerabilties not detected

- withdrawForAuctions(uint[] memory auctionIds)
  Vulnerabilties not detected

- processSuccesfullAuction(uint auctionId)
  Vulnerabilties not detected

- startNewAuctions(uint[] memory tokenIds, uint[] memory startBidAmounts, bool[] memory isAmountInEths, uint[] memory roundDurations, bool[] memory isCustodials, string[] memory descriptions)
  Vulnerabilties not detected

- startNewAuction(uint tokenId, uint startBidAmount, bool isAmountInEth, uint roundDuration, uint successAuctionFeePercentage, string memory description, bool isCustodial)
  Vulnerabilties not detected

- startNewAuction(uint tokenId, uint startBidAmount, bool isAmountInEth, string memory description, bool isCustodial)
  Vulnerabilties not detected

- rescueUnbiddenTokenByTokenId(uint tokenId)
  Vulnerabilties not detected

- rescueUnbiddenToken(uint auctionId)
  Vulnerabilties not detected

- _stake(uint auctionId, address user)
  Vulnerabilties not detected

- _withdraw(uint auctionId)
  Vulnerabilties not detected

- _initAuction(uint auctionId)
  Vulnerabilties not detected
- _safeTransferETH(address to, uint value)
  Vulnerabilties not detected
- updateCustodianAdmin(address newAdmin)
  Vulnerabilties not detected
- approveAuctionForCustodian(uint auctionId, bool isApproved)
  Vulnerabilties not detected
- updateMinAuctionStartPrice(uint newMinAuctionStartPrice)
  Vulnerabilties not detected
- updateDefaultAuctionDuration(uint newDefaultAuctionDuration)
  Vulnerabilties not detected
- updatePriceFeed(address newPriceFeed)
  Vulnerabilties not detected
- updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage)
  Vulnerabilties not detected
- _updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage)
  Vulnerabilties not detected

- updateNextBidStepPercentage(uint newNextBidStepPercentage)
  Vulnerabilties not detected

- rescue(address to, address tokenAddress, uint amount)
  Vulnerabilties not detected

- updateCustodian(address newCustodian)
  Vulnerabilties not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
HardStakinNFTAuction CustodialToken	0.8.7	200	6d06ef4fff904808260fb83d37ee96acec2e3f9066479f0e63a15378da6327c9
Unciron	0.8.7	200	fabad96f367a5e5a3d8954c0e0fc1df5d7864c001cf68267fc5bf0adfa6dfd66

Get In Touch

info@smartstate.tech

smartstate.tech