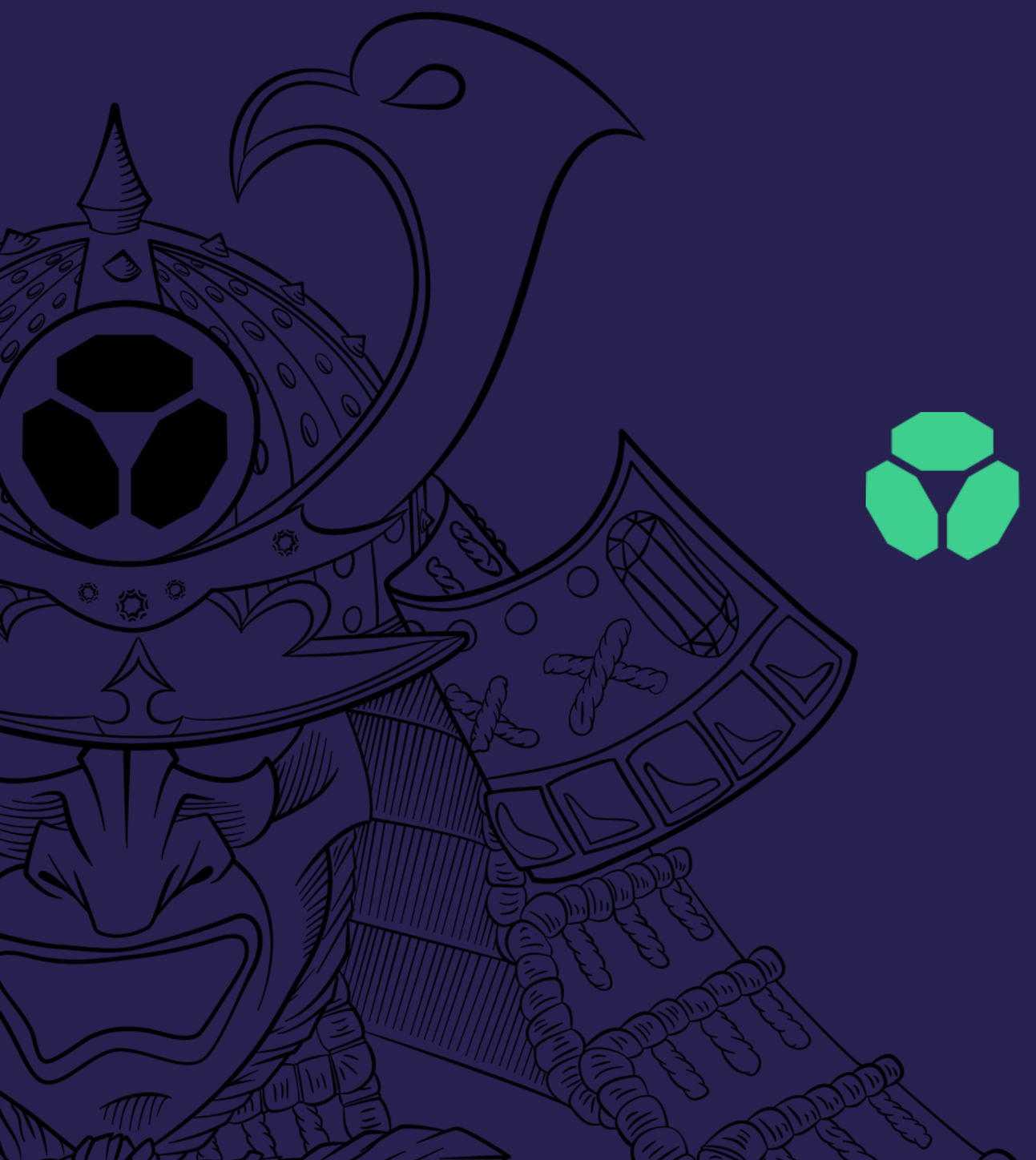

smart state

> Smart
Contract
Audit #

XP.NETWORK

Nov 29
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

CONTRACTS.PY

CONTRACT METHODS ANALYSIS:

- on_create
  Vulnerabilities not detected
- on_delete
  Vulnerabilities not detected
- on_create_nft
  Recommended to store whether NFT has already been created or not in order not to override created_nft_id_key by accidentally calling this method twice. This situation requires the validators to reach a consensus on this call. Due to this the severity of the reported issue is: Information level.
- on_transfer_algo
  Vulnerabilities not detected
- on_transfer_nft
  Vulnerabilities not detected
- on_opt_in_nft
  Vulnerabilities not detected
- on_receive_nft
  Vulnerabilities not detected

- on_update_validators
  Vulnerabilities not detected

- on_reset_receiver
  Vulnerabilities not detected

- on_call
  Vulnerabilities not detected

- application_start
  Vulnerabilities not detected

- approval_program
  Vulnerabilities not detected

- clear_program
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
BES	2fcaae5288a3cfd96fe2e5a6ba26e500d068d7e58bafc43c22b1dad2ad4f74ab

Get In Touch

info@smartstate.tech

smartstate.tech