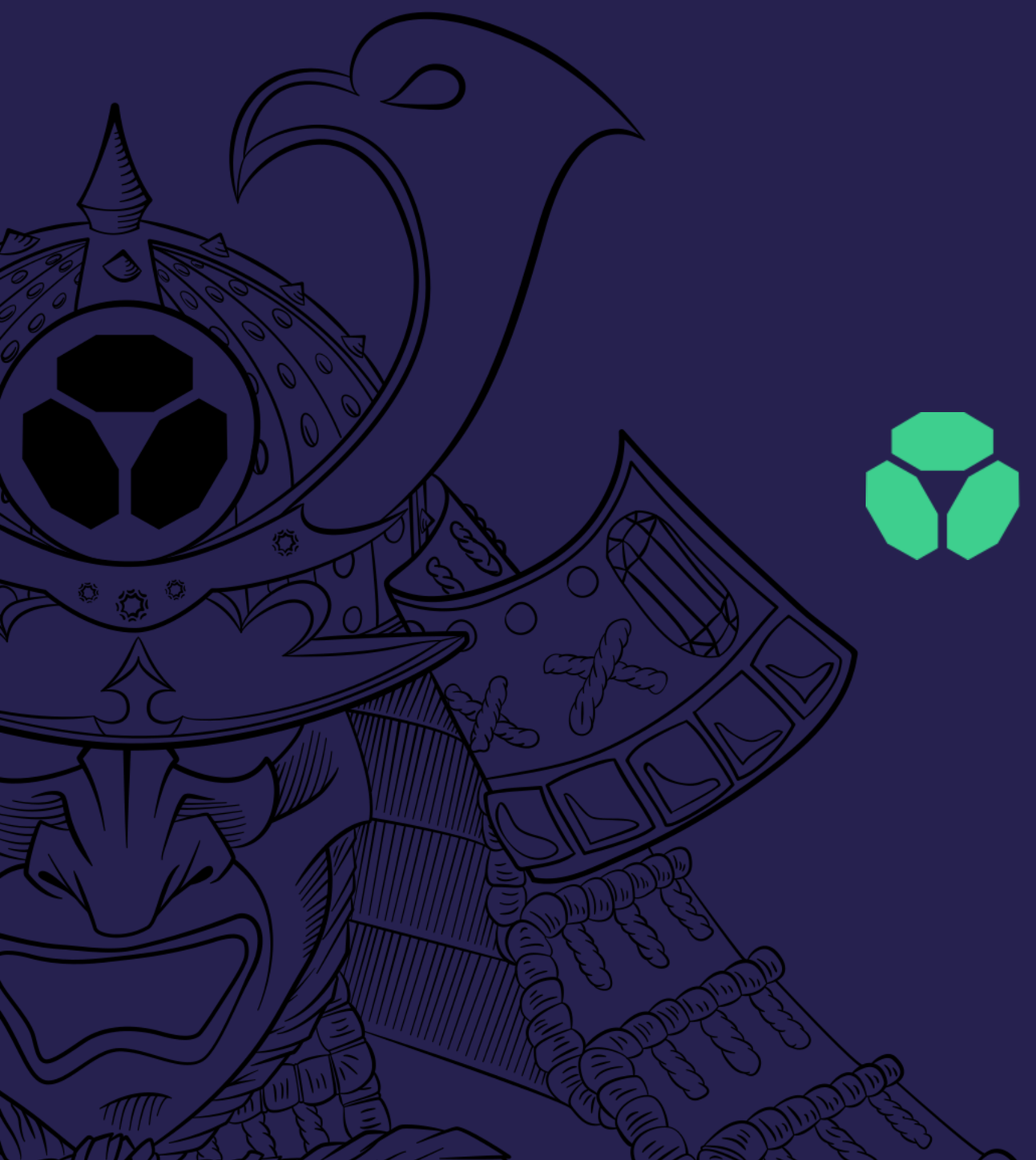

smart state

> Smart
Contract
Audit #

# XP.NETWORK

Jan 04
2022

# TABLE OF CONTENTS

Table of contents ..... 3

Methodology ..... 4

Stucture of contact Contracts.py ..... 5

Verification check sums ..... 8

# 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

## BRIDGE.PY

### CONTRACT METHODS ANALYSIS:

- call(c, x)
  Vulnerabilities not detected
- __init__(self, administrator)
  Vulnerabilities not detected
- is_administrator(self, sender)
  Vulnerabilities not detected
- is_paused(self)
  Vulnerabilities not detected
- contains(self, list, given)
  Vulnerabilities not detected
- setup(self, params)
  Vulnerabilities not detected
- validate_action(self, action_id, action)
  Vulnerabilities not detected

**PAYABLE**

- validate_transfer_nft(self, params)
  Vulnerabilities not detected

**Nft out**

- withdraw_nft(self, params)
  Vulnerabilities not detected

PAYABLE

- freeze_fa2(self, params)

  Vulnerabilities not detected

Nft in

- validate_pause_bridge(self, params)

  Vulnerabilities not detected

- validate_unpause_bridge(self, params)

  Vulnerabilities not detected

PAYABLE

- validate_unfreeze_nft(self, params)

  Vulnerabilities not detected

Nft out

- validate_whitelist_nft(self, params)

  Vulnerabilities not detected

- validate_add_validator(self, params)

  Vulnerabilities not detected

- validate_remove_validator(self, params)

  Vulnerabilities not detected

- validate_set_threshold(self, params)

  Vulnerabilities not detected

- validate_withdraw_fees(self, action_id)
  Vulnerabilities not detected

- get_frozen_nfts(self, addr)
  Vulnerabilities not detected

- get_quorum_failure(self)
  Vulnerabilities not detected

# VERIFICATION CHECK SUMS

| Contract Name | Bytecode hash (SHA 256) |
| --- | --- |
| Bridge.py | d77700a039929df84f74a4991362c5501208608c3ffe3095dd58807b3ae4e56d |

# Get In Touch

info@smartstate.tech

smartstate.tech