

smart state

new generation of
smart contract audit





Xana

Jul 15

2022

TABLE OF CONTENTS

Table of contents.....	3
Methodology.....	4
Structure of contract Xeta.sol.....	5
Verification check sums.....	6

METHODOLOGY

MAIN TESTS LIST:

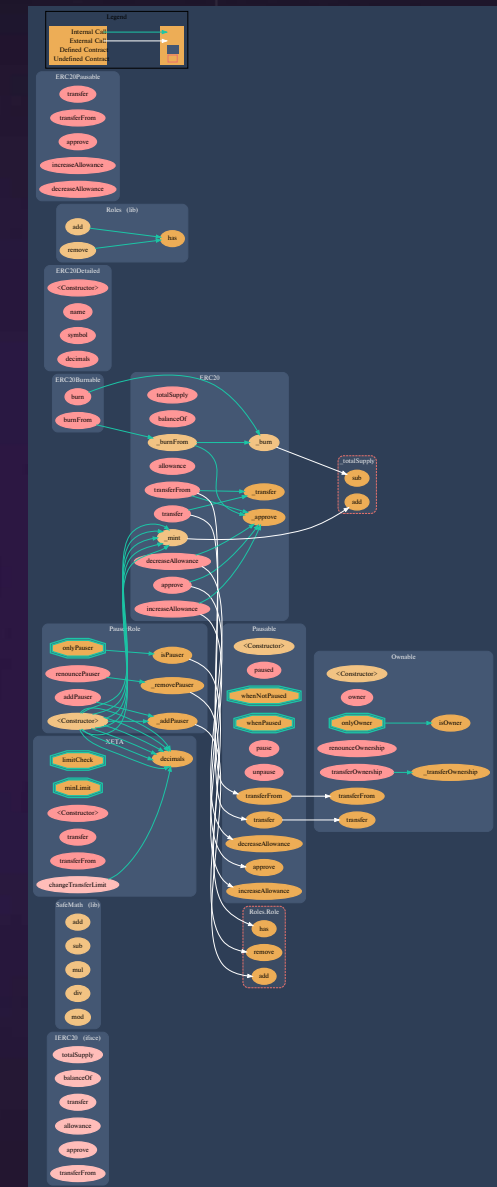
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool 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

XETA.SOL

CONTRACT METHODS ANALYSIS:

- `transfer(address to, uint256 value)`
Vulnerabilities not detected
- `transferFrom(address from, address to, uint256 value)`
Vulnerabilities not detected
- `changeTransferLimit(uint256 _limit)`
Vulnerabilities not detected

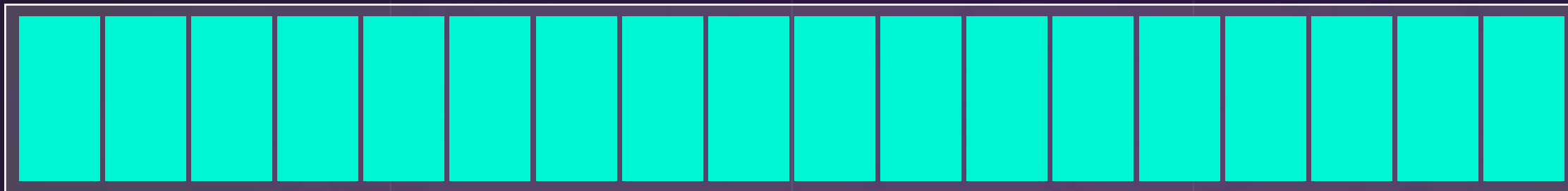


Xeta.sol

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimization	Bytecode hash (SHA 256)
Xeta.sol	0.5.0+commit.1d4f565a	200	f5b3a686dc9a75010fe130f 9330afc0f9f6ddea2519b97 598ba94c59ad582c36

PROJECT EVALUATION



10/10



GET IN TOUCH

info@smartstate.tech
smartstate.tech



in

View this report on smartstate.tech
