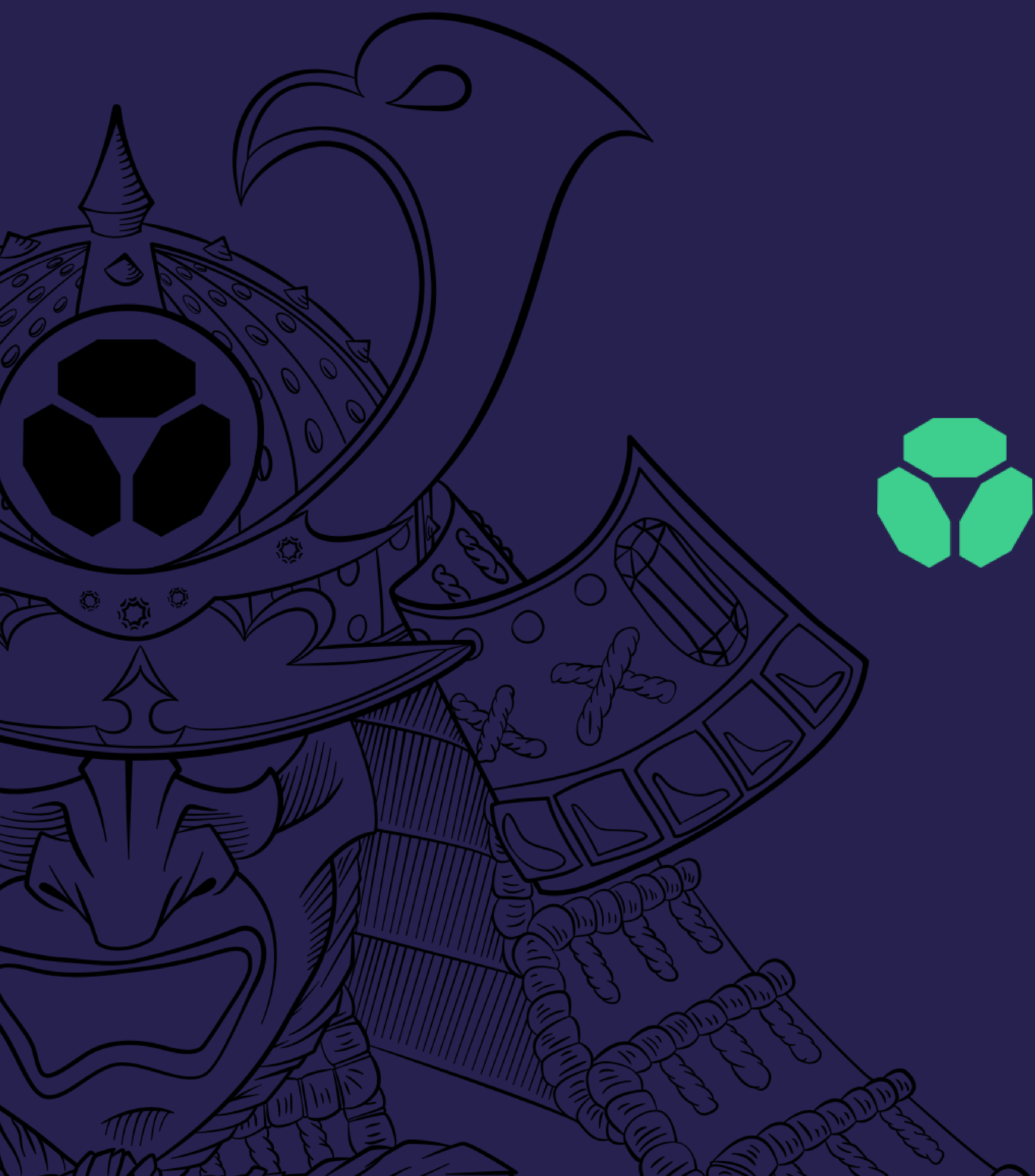


smart state

# > Smart Contract Audit #

# GAMES PAD

Dec 17
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

## GMPD.SOL

## CONTRACT METHODS ANALYSIS:

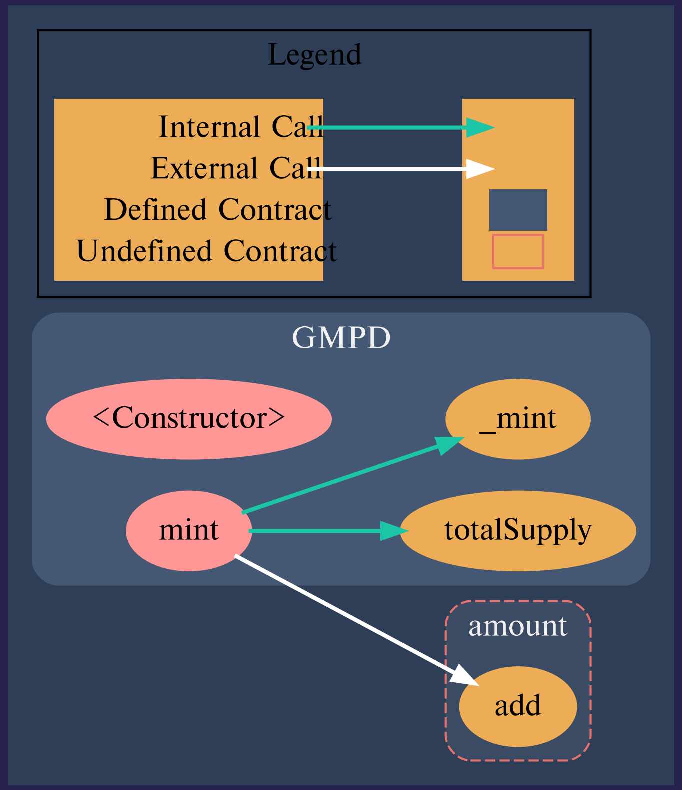
- mint(address to, uint256 amount)
  Vulnerabilities not detected

- burn(uint256 amount)
  Vulnerabilities not detected

- burnFrom(address account, uint256 amount)
  Vulnerabilities not detected

- _blacklist(address account, bool enabled)
  Vulnerabilities not detected

- blacklist(address account, bool enabled)
  Vulnerabilities not detected



Pic. 1.1
GMPD.sol

- blacklistBatch(address[] memory accounts, bool enabled)
  Vulnerabilities not detected

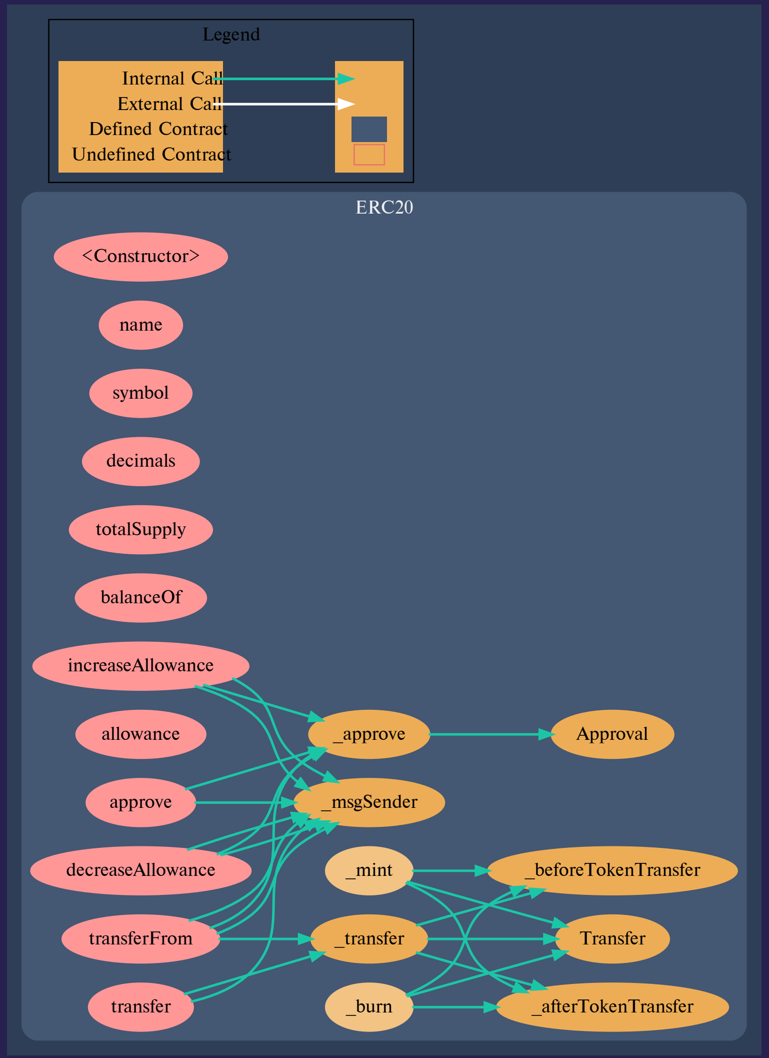
- _beforeTokenTransfer(address from,address to,uint256 amount)
  Vulnerabilities not detected

# STRUCTURE OF CONTRACT

## ERC20.SOL

## CONTRACT METHODS ANALYSIS:

- name()
  Vulnerabilities not detected
- symbol()
  Vulnerabilities not detected
- decimals()
  Vulnerabilities not detected
- totalSupply()
  Vulnerabilities not detected
- balanceOf(address account)
  Vulnerabilities not detected



Pic. 1.2
ERC20.sol

- transfer(address recipient, uint256 amount)
  Vulnerabilities not detected

- allowance(address owner, address spender)
  Vulnerabilities not detected

- approve(address spender, uint256 amount)
  Vulnerabilities not detected

- transferFrom(
  ```
      address sender,
      address recipient,
      uint256 amount
  )
  ```
  Vulnerabilities not detected

- increaseAllowance(address spender, uint256 addedValue)
  Vulnerabilities not detected

- decreaseAllowance(address spender, uint256 subtractedValue)
  Vulnerabilities not detected

- _transfer(
  ```
      address sender,
      address recipient,
      uint256 amount
  )
  ```
  Vulnerabilities not detected

- _mint(address account, uint256 amount)

  Vulnerabilities not detected

- _burn(address account, uint256 amount)

  Vulnerabilities not detected

-
  ```
  _approve(
        address owner,
        address spender,
        uint256 amount
    )
  ```

  Vulnerabilities not detected

-
  ```
  _beforeTokenTransfer(
        address from,
        address to,
        uint256 amount
    )
  ```

  Vulnerabilities not detected

-
  ```
  _afterTokenTransfer(
        address from,
        address to,
        uint256 amount
    )
  ```

  Vulnerabilities not detected

# CONTRACT SUMMARY

- Token type: ERC20
- Symbol: GMPD
- Decimals: 18

**Token Management:** The Token's Contract does contain Blacklist logic to prevent transferring from and/or to blacklisted addresses. Blacklists management requires Owner role.
Owner can enable or disable blacklist functionality for the exact address or for the batch of addresses via blacklist and blacklistBatch methods.
It does not have token locks functionality.

The Contact has public method Mint accessible only by the Owner.
Minted tokens will be sent to the receiver address that goes as a second parameter in the Mint method.
The Contract has public methods Burn and burnFrom that based on ERC20's allowance value for the caller.

**Ownership:** The Token's Contact implements Ownable interface.
The Owner in the contact has the next permissions: to mint the token until the TotalSupply reaches the MaxSupply value and for Blacklists management.

The Token's Contract does not have any additional functionality for Bridges and specific Vesting contracts.

✓ **The Contract can be assumed as safe**

# VERIFICATION CHECK SUMS

| Contract Name | Solc version | Optimisation | Bytecode hash (SHA 256) |
|---|---|---|---|
| GMPD | 0.8.0 | 200 | c098618719ecbdf09c5ea5ee451e40d76e6ce7b8d89a64121f6fae4abc0674b6 |

# Get In Touch

info@smartstate.tech

smartstate.tech