



Web3 security easier than ever



Crypto Story Bank
Smart contract audit report

Mar 12 2023

Disclaimer

The audited smart contract is an implementation of the ERC-20 token and has the following characteristics:

- The token admin can add and remove any user to a blacklist
- The contract has the transferFrom function

Table of contents

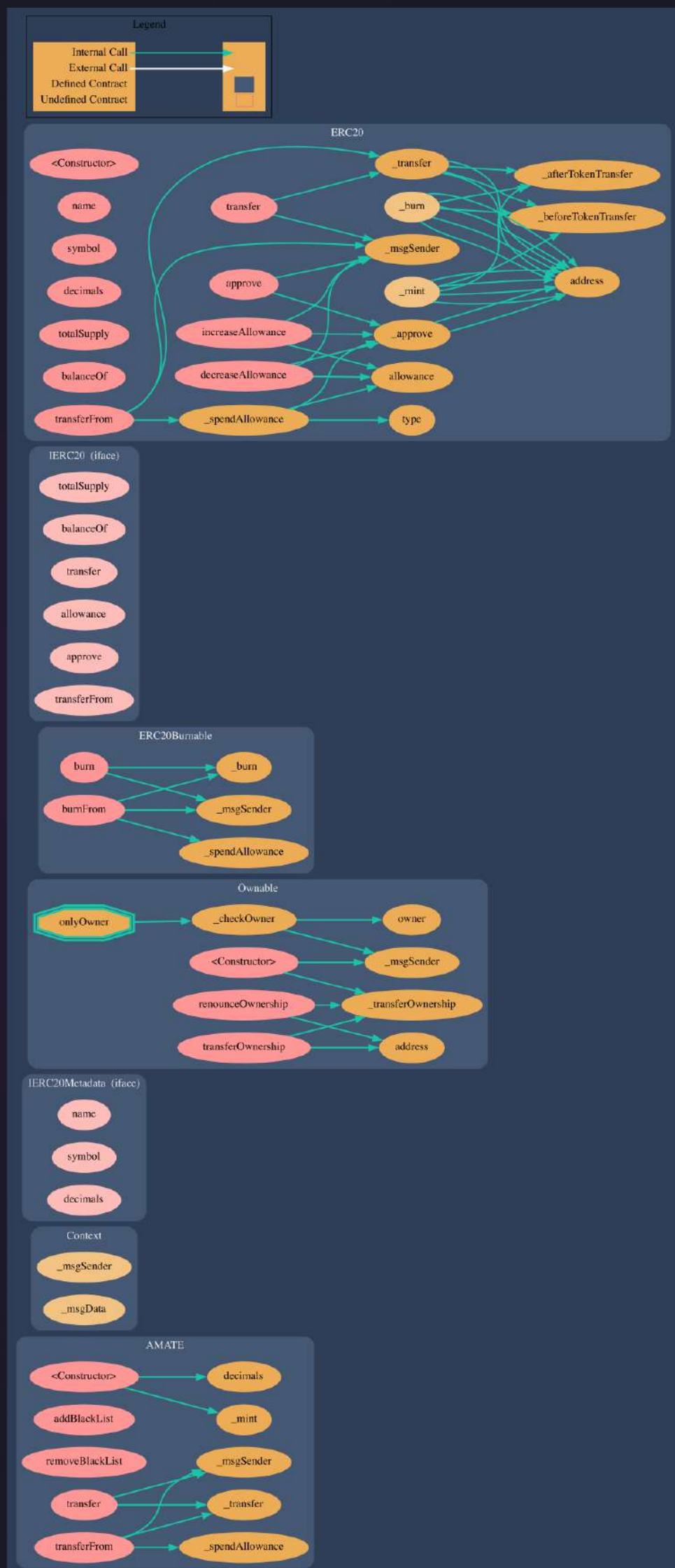
Table of contents	3
Methodology	4
Structure of contract AMATE.sol	5
Verification check sums	7
Project evaluation	8

Methodology

- 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

AMATE.sol



pic.1.1. AMATE.sol

Contract methods analysis:

WARNING

```
addBlackList (address
_evilUser)
```

Function should be declared external

WARNING

```
removeBlackList (address
_clearedUser)
```

Function should be declared external

WARNING

```
transfer(address to,
uint256 amount)
```

We would recommend to override `_beforeTokenTransfer` hook to check for black list, instead of overriding both functions

WARNING

```
decimals()
```

No need to override this function, it returns 18 by default

WARNING

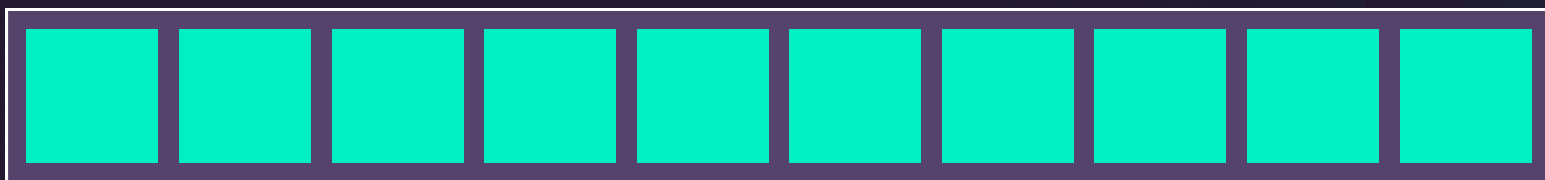
```
transferFrom(
  address from,
  address to,
  uint256 amount
)
```

We would recommend to override `_beforeTokenTransfer` hook to check for black list, instead of overriding both functions

Verification check sums

Contract name	Solc version	Optimization	Bytecode hash(SHA 256)
AMATE.sol	0.8.9	200	cabd44f696203032882d7b 29cd369469060431120acc 547dcf985b5a4c132b6e
Link to source code:	https://etherscan.io/ address/0xf8eB229a0386295E71326b84Ca595AfBF67fe404#code		

Project evaluation



10/10

Get in touch 🙌



[@smartstatetech](#)



[@smartstate](#)



[@SmartStateAudit](#)



[@smartstatetech](#)



[@smartstate.tech](#)

info@smartstate.tech

smartstate.tech

