# TUBICOIN 安全性分析


- (#) Author: xxxeyJ
- (#) Blog: tricksongs.com
- (#) Github: github.com/xxxeyJ
- (#) 区块链安全学习资料: xxxeyJ/Awesome-Blockchain-Security


## TL;DR

最近 TOOls.Net 在 BSC MainNet 上面发行了一个名为 **TuBiCoin** 的 ERC20 Token，我作为 TOOls 论坛区块链安全版主自然要对其进行一波安全审计(旺柴)，其实 TOOls 本身发币用的就是第三方服务，只是实现了一个基础 ERC20 Token 的智能合约，尽管编译器版本过低，但并没有什么复杂的逻辑，代码健壮性还是不错的。

## INFORMATION

| Key | Value |
| --- | --- |
| Website | https://tubicoin.com |
| Smart Contract | 0x713ac71a6ad1021416f12c4a9e17bdf489de6d7e |
| Name | TuBi Coin |
| Symbol | TUBI |
| Holders | 1,197 Addresses (Not constant) |
| Transfers | 1,813 (Not constant) |
| Decimals | 0 |
| Contract Name | TokenMintERC20Token |
| Compiler Version | v0.4.24+commit.e67f0147 |
| Optimization Enabled | No with 200 runs |
| Other Settings | Default evmVersion, MIT license |
| Smart Contract Creator | 0x729968a431ac46d8455971ddb86c356a480b9ae6 |
| Creation Tx Hash | 0x67d457949219b24ea7bb0418794078a4f60c5b2a7bc7637982d03006d72adc96 |

# SMART CONTRACT CREATION

部署智能合约花销: **msg.value** => 0.07590108 BNB，按照当时 BNB 的市场价差不多花了 $39.99

# FIXED SUPPLY ERC20 TOKEN

$39.99

Total supply set at token creation

Get 100% ownership of generated ERC20 tokens

Custom token name, symbol, and initial supply

No programming skills required

Verified and published contract source code

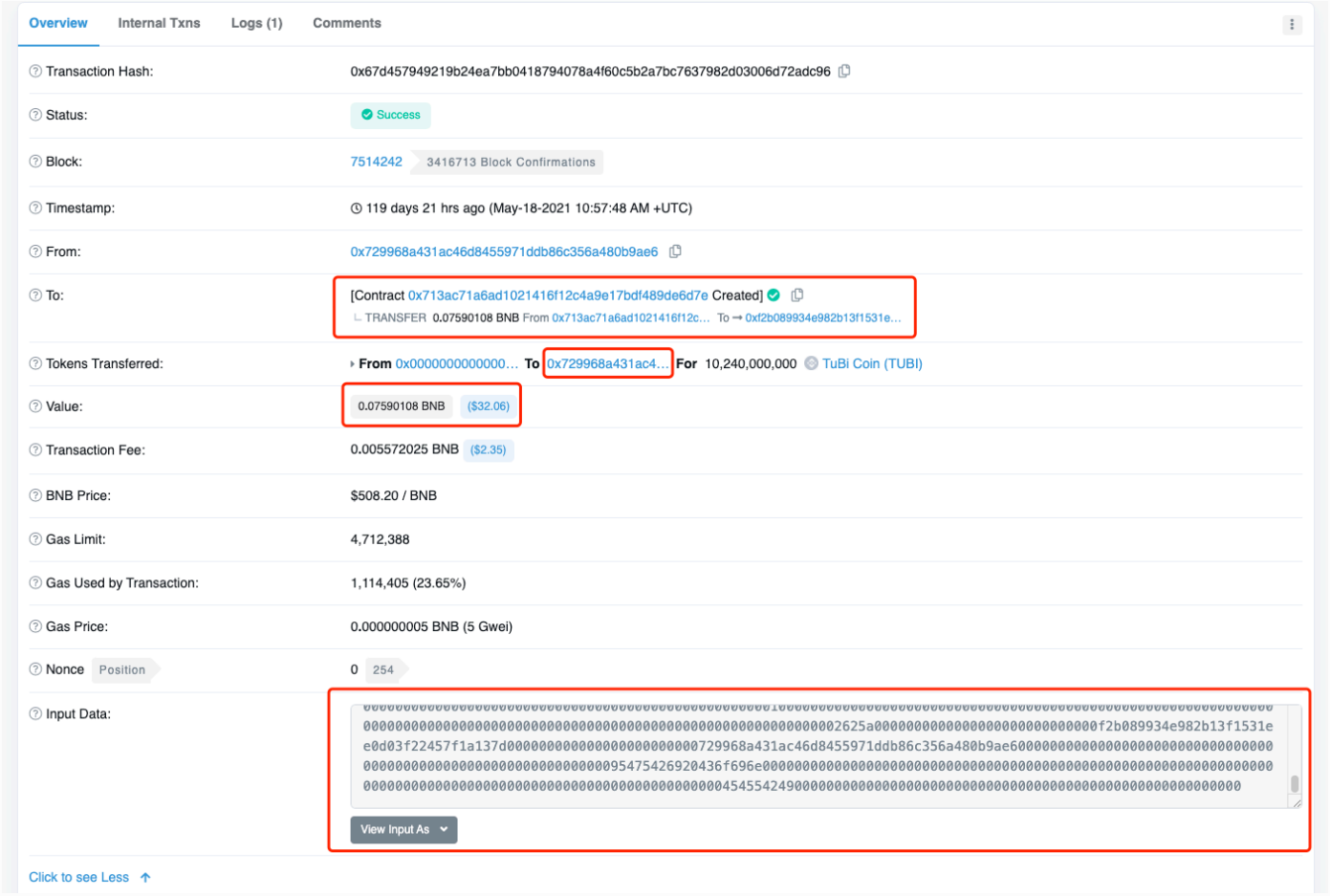
Industry-standard token accepted by most exchanges

Learn more about Fixed Supply ERC20 Token

CREATE FIXED SUPPLY TOKEN

* payment is made in ETH

| | | | | | | |
|---|---|---|---|---|---|---|
| 7514242 | 119 days 21 hrs ago | 0x67d457949219b24ea7… | call | 0x713ac71a6ad1021416… | 0xf2b089934e982b13f15… | 0.07590108 BNB |




这里消息调用的 Input Data 字段用于初始化智能合约，完整 msg.data 如下

```
0x60806040526040516200148f3803806200148f83398101806040528101908
0805182019291906020018051820192919060200180519060200190929190805
1906020019092919080519060200190929190805190602001909291905050508
5600390805190602001906200007592919062000029a565b50846004908051
9060200190620000 8e9291906200029a565b5083600560006101000a8154816
0ff021916908360ff16021790555062000c581846200011964010000000002
64010000000090045 65b8173ffffffffffffffffffffffffffffffffffffffff
f166108fc34908115029060405160006040518083038185888f19350505050
1580156200010c573d6000803e3d6000fd5b50505050505050620003495 65b6
0008273ffffffffffffffffffffffffffffffffffffffff1614151515620001
4057600080fd5b62000165816002546200027864010000000002620010e9179
0919064010000000090045 65b60028190555062000 1cc816000808573ffffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff
ffffffffffffff16815260200190815260200160002054620002786401000 0
000002620010e9179091906401000000009004565b6000808473ffffffffff
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff
fffffffff16815260200190815260200160002081905550817 3ffffffffff
ffffffffffffffffffffffffffff16600073ffffffffffffffffffffffffffff
ffffffffffff167fddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a
```

11628f55a4df523b3ef836040518082815260200191505060405180910390a3
5050565b60008082840190508381101515156200029057600080fd5b8091505
092915050565b828054600181600116156101000203166002900490600052602
0600020906001f016020900481019282601f10620002dd57805160ff1916838
0011785556200030e565b828001600101855582156200030e579182015b8281
11156200030d578251825591602001919060010190620002f0565b5b5090506
200031d919062000321565b5090565b6200034691905b808211156200034257
600081600090555060010162000328565b5090565b90565b611136806200035
96000396000f300608060405260043610610af576000357c01000000000000
0000000000000000000000000000000000000000900463ffffffff16806
306fdde03146100b4578063095ea7b3146101445780631816 0ddd146101a957
806323b872dd146101d4578063313ce567146102595780633950935114610 28
a57806370a08231146102ef57806395d89b4114610346578063a457c2d71461
03d6578063a9059cbb1461043b578063dd62ed3e146104a0575b600080fd5b3
480156100c057600080fd5b506100c9610517565b6040518080602001828103
8252838181518152602001915080519060200190808383 60005b83811015610
1095780820151818401526020810190506100ee565b5050505090509081019 0
601f1680156101365780820380516001836020036101000a031916815260200
191505b509250505060405180910390f35b34801561015057600080fd5b5061
018f60048036038101908080357 3ffffffffffffffffffffffffffffffffffffff
ffff1690602001909291908035906020019092919050505061 05b9565b6040
5180821515151581526020019150506040518091 0390f35b3480156101b5576
00080fd5b506101be6106e6565b60405180828152602001915050604051809 1
0390f35b3480156101e057600080fd5b5061023f60048036038101908080357
3ffffffffffffffffffffffffffffffffffffff1690602001909291908035
73ffffffffffffffffffffffffffffffffffffff1690602001909291908035
90602001909291905050506106f0565b604051808215151515815260200191
505060405180910390f35b34801561026557600080fd5b5061026e6108a2565
b604051808260ff1660ff16815260200191505060405180910390f35b348015
6102965760 0080fd5b506102d560048036038101908080357 3ffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffff1690602001909291908035 90602001909291
905050506108b9565b604051808215151515815260200191505060405180910
390f35b3480156102fb57600080fd5b506103306004803603810190808035 73
ffffffffffffffffffffffffffffffffffffff1690602001909291905050 5
0610af0565b604051808281526020019150506040518091 0390f35b34801561
035257600080fd5b5061035b610b38565b604051808060200182810382528 38
181518152602001915080519060200190808383 60005b8381101561039b5780
820151818401526020810190506103805b505050509050908101906 01f168
0156103c857808203805160018360200361010 00a031916815260200191505b
509250505060405180910390f35b3480156103e257600080fd5b50610421600
480360381019080803573ffffffffffffffffffffffffffffffffffffff16
906020019092919080359060200190929190505050610bda565b60405180821
515151581526020019150506040518091 0390f35b34801561044757600080fd

5b5061048660048036038101908080357 3fffffffffffffffffffffffffffff
ffffffffff1690602001909291908035906020019092919050505061 0e1156
5b604051808215151515815260200191505060405180910390f35b348015610
4ac57600080fd5b506105016004803603810190808035 73ffffffffffffffff
ffffffffffffffffffffffff1690602001909291908035 73ffffffffffffff
ffffffffffffffffffffffff1690602001909291905050506 10e28565b6040
518082815260200191505060405180910390f35b606060038054600181600 11
615610100020316600290048060 1f01602080910402602001604051908101600
40528092919081815260200018280546001816001161561010002031660029 00
480156105af5780601f10610584576101008083540402835291602001916105
af565b820191906000526020600020905b81548152906001019060200180831
161059257829003601f168201915b5050505050905090565b60008073ffffff
ffffffffffffffffffffffffffffffff168373ffffffffffffffffffffffff
ffffffffffffffff161415151561 05f657600080fd5b81600160003373ffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff
ffffffffffffffff168152602001908152602001600020600 08573ffffffff
ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
ffffffffffff168152602001908152602001600020819055508273ffffffff
ffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffff
ffffffffffffff167f8c5be1e5ebec7d5bd14f71427d1e84f3dd0314c0f7b2
291e5b200ac8c7c3b92584604051808281526020019150506040518091039 0a
360019050929150505 65b60006002549050905 65b60006001600 8573ffffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff
ffffffffffffff168152602001908152602001600020600 03373ffffffffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
fffffffffff168152602001908152602001600020548211151515610 77d5760
0080fd5b61080c82600160008773ffffffffffffffffffffffffffffffffffff
fffff1673ffffffffffffffffffffffffffffffffffffffffffff16815260200190
815260200160002060003373ffffffffffffffffffffffffffffffffffffffff
f1673ffffffffffffffffffffffffffffffffffffffffff168152602001908152
602001600020546 10eaf90919063fffffff16565b600160008673ffffffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
ffffffffffff168152602001908152602001600020600 03373ffffffffffff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffff
fffffff16815260200190815260200160002081905550610897848484610ed
0565b60019050939250505 0565b60006005600090549061010 00a900460ff16
905090565b60008073ffffffffffffffffffffffffffffffffffffffffffff16837
3ffffffffffffffffffffffffffffffffffffffffff161415151561 08f6576000
80fd5b610985826001600 03373ffffffffffffffffffffffffffffffffffffff
fff1673ffffffffffffffffffffffffffffffffffffffffff168152602001908 1
526020016000206000 8673ffffffffffffffffffffffffffffffffffffffff1
673ffffffffffffffffffffffffffffffffffffffffff168152602001908152 60
200160002054611 0e990919063fffffff16565b600160003373fffffffffff

```
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
fffffffff16815260200190815260200160002060008573fffffffffffff
ffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffff
ffffff16815260200190815260200160002081905550827 3fffffffffffff
ffffffffffffffffffffffff163373ffffffffffffffffffffffffffffff
fffffff167f8c5be1e5ebec7d5bd14f71427d1e84f3dd0314c0f7b2291e5b2
00ac8c7c3b9256001600033 73ffffffffffffffffffffffffffffffffff
ff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815
260200160002060008773ffffffffffffffffffffffffffffffffffff16
73ffffffffffffffffffffffffffffffffffff16815260200190815260 2
00160002054604051808281526020019150506040518091039 0a36001905092
915050565b60008060008373ffffffffffffffffffffffffffffffffff
f1673ffffffffffffffffffffffffffffffffffff16815260200190815 2
602001600020549050919050565b606060048054600181600116156101000 20
3166002900480601f0160208091040260200160405190810160405280929190
818152602001828054600181600116156101000203166002900 48015610bd05
780601f10610ba55761010080835404028352916020019161 0bd0565b820191
906000526020600020905b81548152906001019060200180831 1610bb357829
003601f168201915b5050505050905090565b60008073ffffffffffffffff
ffffffffffffffffffff168373ffffffffffffffffffffffffffffffffff
fffff1614151515610c1757600080fd5b610ca68260016000 3373ffffffffff
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
fffffffffff16815260200190815260200160002060008673ffffffffffff
ffffffffffffffffffffffff1673ffffffffffffffffffffffffffffff
fffffff16815260200190815260200160002054610eaf90919063ffffffff16
565b600160003373ffffffffffffffffffffffffffffffffffffffff1673fff
ffffffffffffffffffffffffffffffffffff16815260200190815260200160
002060008573ffffffffffffffffffffffffffffffffffffffff1673ffffff
ffffffffffffffffffffffffffffffffff16815260200190815260200160002 0
819055508273ffffffffffffffffffffffffffffffffffffffff163373fffff
ffffffffffffffffffffffffffffffff167f8c5be1e5ebec7d5bd14f7142
7d1e84f3dd0314c0f7b2291e5b200ac8c7c3b9256001600033 73ffffffffff
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffff
fffffffffff16815260200190815260200160002060008773ffffffffffffff
ffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffff
ffffff16815260200190815260200160002054604051808281526020019150 5
060405180910390a3600190509291505056 5b6000610e1e338484610ed0565b
600190509291505056 5b6000600160008473ffffffffffffffffffffffff
ffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152
602001908152602001600020600083 73ffffffffffffffffffffffffffffff
fffffffff1673ffffffffffffffffffffffffffffffffffffffff1681526020
019081526020016000205490509291505056 5b60008083831115151561 0ec15
7600080fd5b828403905080915050929150505 65b6000808473ffffffffffff
```

```
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff
ffffffff16815260200190815260200160002054811115151561 0f1d576000
80fd5b600073ffffffffffffffffffffffffffffffffffffffff168273fffff
fffffffffffffffffffffffffffffffff16141515156 10f5957600080fd5b
610faa816000808673ffffffffffffffffffffffffffffffffffffffff1673f
ffffffffffffffffffffffffffffffffffffffff168152602001908152602001
60002054610eaf90919063fffffff16565b6000808573ffffffffffffffff
ffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffff
ffff16815260200190815260200160002081905550611 03d816000808573fff
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffff
ffffffffffffffff16815260200190815260200160002054611 0e99091906
3fffffff16565b6000808473ffffffffffffffffffffffffffffffffffffffff
ff1673ffffffffffffffffffffffffffffffffffff168152602001908 15
260200160002081905550817 3ffffffffffffffffffffffffffffffffffffffff
ff168373ffffffffffffffffffffffffffffffffffff167fddf252ad1be
2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef8360405180
828152602001915050604051809103 90a3505050565b6000808284019050838
110151515611100576000 80fd5b8091505092915050560 0a165627a7a723058
2068bac03c03fccee8a37eb7c8d485f3e7293f5b94960acc491e245a5df51ce
1ef0029000000000000000000000000000000000000000000000000000000
000000c0000000000000000000000000000000000000000000000000000000
0000001000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
002625a000000000000000000000000f2b089934e982b13f1531ee0d03f
22457f1a137d00000000000000000000729968a431ac46d8455971ddb86
c356a480b9ae6000000000000000000000000000000000000000000000000
0000000000095475426920436f696e000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000454554249000000000000000000000000000000000000000
00000000000000000
```

我们切入至相关代码进行解读，`TokenMintERC20Token` 是该 Token 的主合约，其中定义了三个 private 状态变量用以标识 Token 信息，name()/symbol()/decimals() 三个视图函数可见性都为 public 用于读取Token 信息，构造函数参数共有6个，name, symbol, decimals, totalSupply 通过部署合约时确认 Token 信息，后期不可更改，feeReceiver(0xf2b0...137d) 外部账户用于接收原生币 BNB 报酬，在这个 Token 当中并没有特权账户的概念，只是在部署时将 `10,240,000,000` 数量的 TuBi Coin 转给了 tokenOwnerAddress(0x7299...9ae6) TOOls管理团队的账户，后期依靠手动或批量转账工具发放 Token

```
323  contract TokenMintERC20Token is ERC20 {
324
325      string private _name;
326      string private _symbol;
327      uint8 private _decimals;
328
329      constructor(string name, string symbol, uint8 decimals, uint256 totalSupply, address feeReceiver, address tokenOwnerAddress) public payable {
330        _name = name;
331        _symbol = symbol;
332        _decimals = decimals;
333
334        _mint(tokenOwnerAddress, totalSupply);
335
336        feeReceiver.transfer(msg.value);
337      }
338
339      function name() public view returns (string) {
340        return _name;
341      }
342
343      function symbol() public view returns (string) {
344        return _symbol;
345      }
346
347      function decimals() public view returns (uint8) {
348        return _decimals;
349      }
350  }
```

#L334 调用 `_mint()` 用于铸币，实现如下，可见性没有问题，require 检查接收账户不为 `0x00`，涉及到数学运算的功能点使用了 `SafeMath Library` -> add() 进行运算从而杜绝掉了整型溢出的问题，该 Token 调用 `_mint()` 的功能点只有构造函数一处，后期不可增发/铸币

```
281  function _mint(address account, uint256 value) internal {
282    require(account != 0);
283    _totalSupply = _totalSupply.add(value);
284    _balances[account] = _balances[account].add(value);
285    emit Transfer(address(0), account, value);
286  }
```

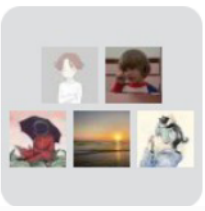
`_burn()` / `_burnFrom()` 可见性皆为 `internal`，且无功能点调用这两个 function，代码层面不存在烧币/销毁 Token 的风险，且转账方法已校验不可将 Token 打入黑洞地址

```
289   function _burn(address account, uint256 value) internal {
290     require(account != 0);
291     require(value <= _balances[account]);
292
293     _totalSupply = _totalSupply.sub(value);
294     _balances[account] = _balances[account].sub(value);
295     emit Transfer(account, address(0), value);
296   }
297
298   function _burnFrom(address account, uint256 value) internal {
299     require(value <= _allowed[account][msg.sender]);
300
301     _allowed[account][msg.sender] = _allowed[account][msg.sender].sub(
302       value);
303     _burn(account, value);
304   }
```

除此之外，比如说 IERC20 Interface, SafeMath Library 等实现都是很基础的概念，市面上没有诸如此类的安全风险，所以此次的安全性审核是通过的。

## 写在最后

我和几个小伙伴共同建立维护了一个纯交流区块链安全知识的微信群，感兴趣的师傅可以扫描下方二维码入群，入群须知：“本群严禁水群等违规行为，具体规则看群公告！“



Blockchain Security

该二维码7天内(9月23日前)有效，重新进入将更新