



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



XEREZ CHAIN
\$XEREZ

18/04/2023



TOKEN OVERVIEW

Fees

- Buy fees: 5%
- Sell fees: 10%

Fees privileges

- Can change fees up to 100%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can change max tx amount without threshold and max wallet amount with threshold

Blacklist

- Blacklist function detected

Other privileges

- Can exclude / include from fees
-

TABLE OF CONTENTS

- 1 **DISCLAIMER**
- 2 **INTRODUCTION**
- 3-4 **AUDIT OVERVIEW**
- 5-7 **OWNER PRIVILEGES**
- 8 **CONCLUSION AND ANALYSIS**
- 9 **TOKEN DETAILS**
- 10 **XEREZ TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS**
- 11 **TECHNICAL DISCLAIMER**



DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website <https://freshcoins.io>

FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by **XEREZ CHAIN** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x93E185a9B20199a10fB49A2888c8Eb7669cbcAce

Network: Binance Smart Chain (BSC)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **18/04/2023**



AUDIT OVERVIEW



Security Score



Static Scan

Automatic scanning for common vulnerabilities



ERC Scan

Automatic checks for ERC's conformance



High



Medium



Low



Optimizations



Informational



No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Passed
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES

- Contract owner can't mint tokens after initial contract deploy

- Contract owner can exclude an address from transactions

```
function isBots(address _address, bool _value) public onlyOwner {  
    isBot[_address] = _value;  
}
```

- Contract owner can exclude/include wallet from tax

```
function setIsFeeExempt(address holder, bool exempt) external onlyOwner {  
    isFeeExempt[holder] = exempt;  
}
```

- Contract owner can change fees up to 100%

```
function setFees(uint256 _liquidityFee, uint256 _marketingFee, uint256 _devFee, uint256 _feeDenominator)  
external onlyOwner {  
    liquidityFee = _liquidityFee;  
    marketingFee = _marketingFee;  
    devFee = _devFee;  
    totalFee = _liquidityFee.add(_marketingFee).add(_devFee);  
    feeDenominator = _feeDenominator;  
}
```

- Contract owner can set sell multiplier (without threshold)

```
function setSellMultiplier(uint256 multiplier) external onlyOwner {  
    _sellMultiplier = multiplier;  
}
```

- Contract owner can change marketingFeeReceiver and devFeeReceiver addresses

Current values:

marketingFeeReceiver : 0x6e158850c33bd4881b204bc5e384613115c24763

devFeeReceiver : 0xfa2f02e89d7031107cc91478fb9498402b02a017

```
function setFeeReceiver(address _marketingFeeReceiver, address _devFeeReceiver) external onlyOwner {  
    marketingFeeReceiver = _marketingFeeReceiver;  
    devFeeReceiver = _devFeeReceiver;  
}
```


● Contract owner can change swap settings

```
function setSwapBackSettings(bool _enabled, uint256 _amount) external onlyOwner {
    swapEnabled = _enabled;
    swapThreshold = _amount;
}
```

● Contract owner can change max tx amount limitation to 0

Transfers can be disabled if `_maxTxAmount` value is set to 0

```
function setTxLimit(uint256 amountBuy) external onlyOwner {
    _maxTxAmount = amountBuy;
}
```

● Contract owner can change max wallet percent with threshold

```
function setMaxWallet(uint256 amount) external onlyOwner {
    require(amount >= _totalSupply / 1000);
    _maxWalletSize = amount;
}
```

● Contract owner can change cooldown between trades status and interval value

```
function cooldownEnabled(bool _status, uint8 _interval) public onlyOwner() {
    opCooldownEnabled = _status;
    cooldownTimerInterval = _interval;
}
```

● Contract owner can withdraw stuck tokens from smart contract

```
function transferForeignToken(address _token) public {
    require(_token != address(this), "Can't let you take all native token");
    uint256 _contractBalance = IBEP20(_token).balanceOf(address(this));
    payable(devFeeReceiver).transfer(_contractBalance);
}
```

● Contract owner can renounce ownership

```
function renounceOwnership() public onlyOwner {
    _setOwner(address(0));
}
```

● Contract owner can transfer ownership

```
function transferOwnership(address payable adr) public onlyOwner {
    owner = adr;
    _intAddr[adr] = true;
    emit OwnershipTransferred(adr);
}
```

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.



CONCLUSION AND ANALYSIS



Smart Contracts within the scope were manually reviewed and analyzed with static tools.



Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.



Found 4 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	5%
Sell fees:	10%
Max TX:	10,000,000
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Detected
Modify Max TX:	Detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Others

Liquidity:	N/A
Holders:	Clean



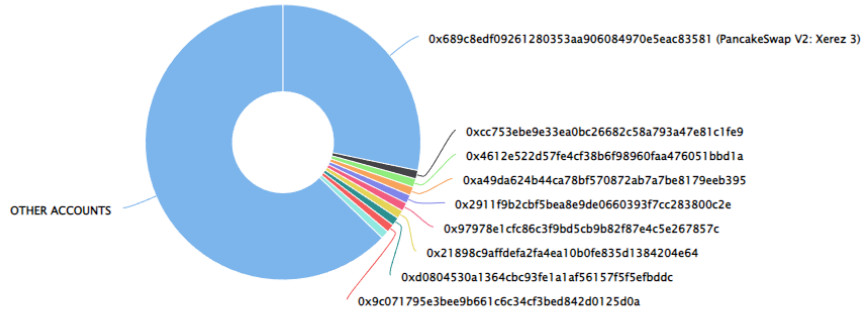
XEREZ TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 37.22% (372,228,414.84 Tokens) of Xerez Chain

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 526

Xerez Chain Top 10 Token Holders

Source: BscScan.com



(A total of 372,228,414.84 tokens held by the top 10 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: Xerez 3	283,020,398.189525131	28.3020%
2	0xcc753ebe9e33ea0bc26682c58a793a47e81c1fe9	10,000,000	1.0000%
3	0x4612e522d57fe4cf38b6f98960faa476051bbd1a	10,000,000	1.0000%
4	0xa49da624b44ca78bf570872ab7a7be8179eeb395	10,000,000	1.0000%
5	0x2911f9b2cbf5bea8e9de0660393f7cc283800c2e	10,000,000	1.0000%
6	0x97978e1cfc86c3f9bd5cb9b82f87e4c5e267857c	10,000,000	1.0000%
7	0x21898c9affdefa2fa4ea10b0fe835d1384204e64	9,976,025.092295393	0.9976%
8	0xd0804530a1364cbc93fe1a1af56157f5f5efbddd	9,778,988.406262554	0.9779%
9	0x9c071795e3bee9b661c6c34cf3bed842d0125d0a	9,733,712.35	0.9734%
10	0x6ef54997c0ffa5c6a0f00eff6f7bd5ac79e0a5f6	9,719,290.8	0.9719%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.

