freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Euro Digitale

$EURD

30/03/2025

TOKEN OVERVIEW

Fees

• **Buy fees:** N/A

• **Sell fees:** N/A

Fees privileges

• Can't change fees

Ownership

• Owned

Minting

• No mint function

Max Tx Amount / Max Wallet Amount

• Can't change max tx amount and / or max wallet amount

Blacklist

• Blacklist function detected

Other privileges

• The contract inherits Pausable which allows the owner to pause all operations

---

TABLE OF CONTENTS

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
Euro Digitale (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x662cFA4a451b7E05FFfFd8B5c976df5d4f31f3a4

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 30/03/2025

Euro Digitale
$EURD

WEBSITE DIAGNOSTIC

https://www.eurodigitalebsc.com/

0-49	50-89	90-100

98	94	98	95	NA
Performance	Accessibility	Best Practices	SEO	Progressive Web App

Socials

X (Twitter)

https://x.com/eurodigitalbsc

Telegram

https://t.me/EURODIGITALBSC

AUDIT OVERVIEW

66

Security Score
HIGH RISK

93 Static Scan
Automatic scanning for common vulnerabilities

62 ERC Scan
Automatic checks for ERC's conformance

3 High

2 Medium

0 Low

0 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Low
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 setBlacklist(address user, bool status) external onlyOwner {
    require(user != address(0), "Invalid address");
    _blacklist[user] = status;
    emit Blacklisted(user, status);
}
```

● **Reward Distribution**

If owner's balance is depleted, the entire reward system breaks. No mechanism to replenish owner's balance

```
require(_balances[owner()] >= reward, "Insufficient owner balance for rewards");
```

● **Pausable Functionality**

The contract inherits Pausable, which means the owner can pause/unpause the contract

When paused, all functions with whenNotPaused modifier will be blocked

This affects critical functions like:

stake()

unstake()

transfer()

approve()

transferFrom()

activateNode()

deactivateNode()

claimNodeRewards()

claimRewards()

```
function _pause() internal virtual whenNotPaused {
    _paused = true;
    emit Paused(_msgSender());
}

function _unpause() internal virtual whenPaused {
    _paused = false;
    emit Unpaused(_msgSender());
}
```

● APY and Reward Adjustments

APY can be reduced significantly. No minimum APY guarantee (only checks for max APY)

Could lead to very low or zero rewards

```
function updateAPY() internal {
    if (totalRewardsDistributed >= STAKING_REWARD_THRESHOLD) {
        uint256 reduction = dailyAPY.mul(25).div(100);
        dailyAPY = dailyAPY.sub(reduction);
        // ...
    }
}
```

● Economic Concerns

High APY

Extremely high APY rates are unsustainable. Could lead to rapid token inflation.

Potential for economic collapse

```
uint256 public constant MAX_DAILY_APY = 30000; // 300% APY massimo (30x)
uint256 public dailyAPY = 15000; // 150% APY iniziale
```

Reward Thresholds

High thresholds could make it difficult to reach reward milestones. Could lead to stagnation in the ecosystem

```
uint256 public constant NODE_REWARD_THRESHOLD = 500000 * 10**18;
uint256 public constant STAKING_REWARD_THRESHOLD = 1000000 * 10**18;
```

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 3 HIGH issue during the first review.

TOKEN DETAILS

Details

Buy fees:	N/A
Sell fees:	N/A
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

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

Rug Pull Risk

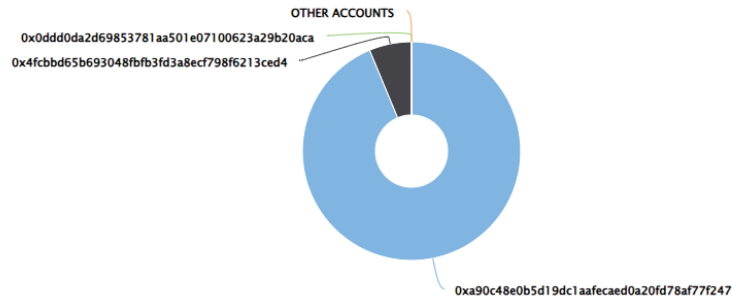|	
Liquidity:	N/A
Holders:	100% unlocked tokens

EURD TOKEN ANALYTICS
& TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00%
(148,644,234,000,000,000,000,000,000.00 Tokens) of 0x662cFA4a451b7...

Token Total Supply: 148,649,994,900,000,000,000,000,000.00 Token | Total Token Holders: 3

0x662cFA4a451b7... Top 10 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0x0ddd0da2d69853781aa501e07100623a29b20aca

0x4fcbbd65b693048fbfb3fd3a8ecf798f6213ced4

0xa90c48e0b5d19dc1aafecaed0a20fd78af77f247

(A total of 148,644,234,000,000,000,000,000,000.00 tokens held by the top 10 accounts from the total supply of 148,649,994,900,000,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xA90C48e0...8Af77f247	139,344,214,000,000,000,000,000,000	93.7398%
2	0x4fcBbd65...F6213cED4	9,300,000,000,000,000,000,000,000	6.2563%
3	0x0DdD0DA2...a29B20AcA	20,000,000,000,000,000,000	0.0000%

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.