



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Acadex Network
\$ACDX



05/03/2022



TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- 3 WEBSITE DIAGNOSTIC
- 4-5 AUDIT OVERVIEW
- 6 OWNER PRIVILEGES
- 7 CONCLUSION AND ANALYSIS
- 8 TOKEN DETAILS
- 9 ACADEX NETWORK TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS
- 10 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 Acadex Network (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x2AD421077D38bF23497b0d9770D7C57C1913f4cA

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 05/03/2022



WEBSITE DIAGNOSTIC

<https://acadex.network/>



0-49



50-89



90-100



Performance



Accessibility



Best Practices



SEO



Progressive
Web App

Metrics



First Contentful Paint

3.4 s



Time to interactive

8.2 s



Speed Index

6.6 s



Total Blocking Time

510 ms



Large Contentful Paint

6.3 s



Cumulative Layout Shift

0.031

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't disable trading.

Contract owner can't exclude an address from transactions.

Contract owner can't set / change buy & sell taxes.

Contract owner can't change swap settings.

Contract owner can't change tx amount.

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {  
    emit OwnershipTransferred(_owner, address(0));  
    _owner = address(0);  
}
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {  
    require(newOwner != address(0), "Ownable: new owner is the zero address");  
    emit OwnershipTransferred(_owner, newOwner);  
    _owner = newOwner;  
}
```



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 no 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: Not detected

Modify Max TX: Not detected

Modify Max Sell: Not detected

Disable Trading: Not detected

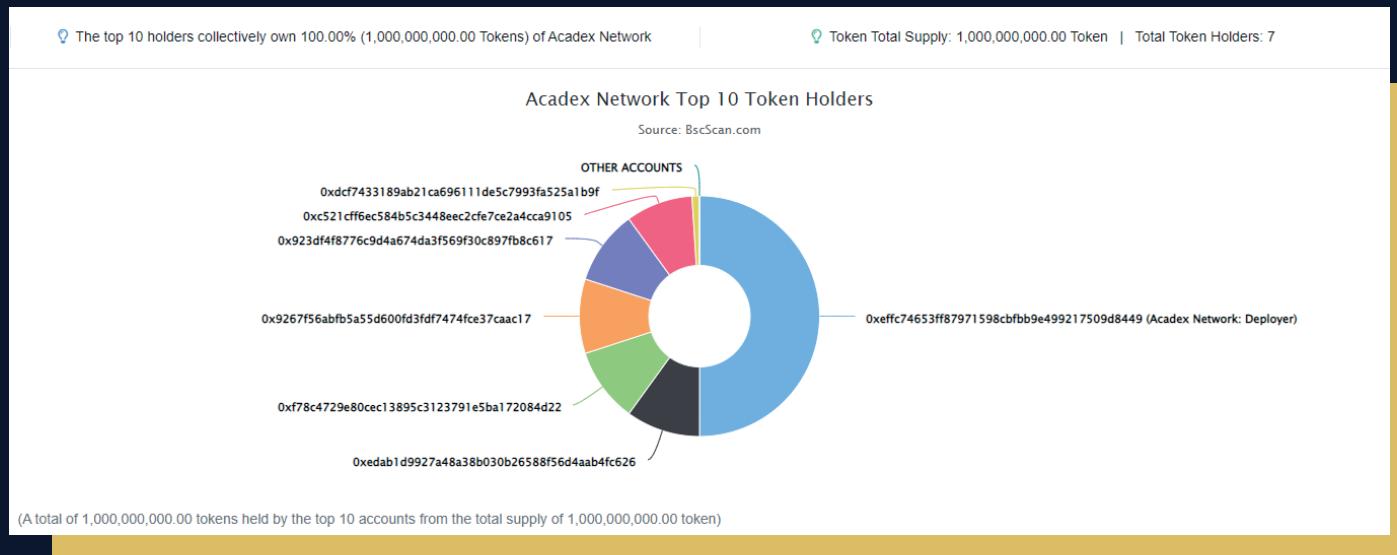
Rug Pull Risk

Liquidity: N/A

Holders: Clean



ACADEX TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	Acadex Network: Deployer	500,000,000	50.0000%
2	0xedab1d9927a48a38b030b26588f56d4aab4fc626	100,000,000	10.0000%
3	0xf78c4729e80cec13895c3123791e5ba172084d22	100,000,000	10.0000%
4	0x9267f56abfb5a55d600fd3fdf7474fce37caac17	100,000,000	10.0000%
5	0x923df4f8776c9d4a674da3f569f30c897fb8c617	100,000,000	10.0000%
6	0xc521cff6ec584b5c3448eec2cf7ce2a4cca9105	90,000,000	9.0000%
7	0xdcf7433189ab21ca696111de5c7993fa525a1b9f	10,000,000	1.0000%

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.

