SPYWOLF

Security Audit Report

Audit prepared for

AZEcoin

Completed on

August 23, 2024

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

AZEcoin

PROJECT DESCRIPTION:

Project’s website is under construction

Release Date: August, 2024

Launchpad: Pinksale

Category: Dividend token

KEY RESULTS

Cannot mint new tokens	PASSED
Cannot pause trading (honeypot)	PASSED
Cannot blacklist an address	PASSED
Cannot raise taxes over 25%?	PASSED
No proxy contract detected	PASSED
Not required to enable trading	PASSED
No hidden ownership	PASSED
Cannot change the router	PASSED
No cooldown feature found	PASSED
Bot protection delay is lower than 5 blocks	PASSED
Cannot set max tx amount below 0.05% of total supply	PASSED
The contract cannot be self-destructed by owner	PASSED

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

CONTRACT INFO

Token Name AZEcoin	Symbol AZE
Contract Address 0xCd14fFC7Ec319b0233C25c99BCBd313bB7604923	
Network BSC	Language Solidity
Deployment Date Aug 23, 2024	Contract Type Dividend
Total Supply 21,000,000	Decimals 18

TAXES

Buy Tax	Sell Tax
6%	6%

*Taxes cannot be changed

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Last transaction time	2024-08-23 03:28:27 UTC
Deployment Date	2024-08-23 03:28:27 UTC
Create TX	0x27e67c69c58c17ed2bc4a0e838a5184fff36767c768b3773198e229caa77fa22
Owner	0x167e7A49d40e23D66A2eDDdb00fC34A578B6D73c
Deployer	0x167e7A49d40e23D66A2eDDdb00fC34A578B6D73c

TOKEN TRANSFERS STATS

Transfer Count	1
Total Amount	21000000 AZE
Median Transfer Amount	21000000 AZE
Average Transfer Amount	21000000 AZE
First transfer date	2024-08-23
Last transfer date	2024-08-23
Days token transferred	1 Day

FEATURED WALLETS

Owner address	Ownership is renounced 0x0000000000000000000000000000000000000000
Marketing fee receiver	0xc16aAcbfF19F24B18edA8B04E51B348F42CAC093
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS

100%	Same as deployer Tokens are not distributed yet 0xc16aAcbfF19F24B18edA8B04E51B348F42CAC093
NOT_AVAILABLE	
NOT_AVAILABLE	

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	**Passed**
SWC-101	Integer Overflow and Underflow	**Passed**
SWC-102	Outdated Compiler Version	**Passed**
SWC-103	Floating Pragma	**Passed**
SWC-104	Unchecked Call Return Value	**Passed**
SWC-105	Unprotected Ether Withdrawal	**Passed**
SWC-106	Unprotected SELFDESTRUCT Instruction	**Passed**
SWC-107	Reentrancy	**Passed**
SWC-108	State Variable Default Visibility	**Passed**
SWC-109	Uninitialized Storage Pointer	**Passed**
SWC-110	Assert Violation	**Passed**
SWC-111	Use of Deprecated Solidity Functions	**Passed**
SWC-112	Delegatecall to Untrusted Callee	**Passed**
SWC-113	DoS with Failed Call	**Passed**
SWC-114	Transaction Order Dependence	**Passed**
SWC-115	Authorization through tx.origin	**Passed**
SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

Code Score: 95%

FOUND THREATS

⚠ High Risk: 0

No high risk-level threats found in this contract.

⚠ Medium Risk: 0

No medium risk-level threats found in this contract.

⚠ Low Risk: 0

No low risk-level threats found in this contract.

FOUND THREATS

Informational: 3

Contract's deployer can withdraw any tokens from the contract. When this function is present, in cases tokens and/or BNB are sent into the contract by mistake or purposefully, contract's deployer can retrieve them.

```
function claimBalance() external {
    payable(fundAddress).transfer(address(this).balance);
}

function claimToken(
    address token,
    uint256 amount,
    address to
) external  {
    require(fundAddress == msg.sender, "!Funder");
    IERC20(token).transfer(to, amount);
}
```

FOUND THREATS

Informational: 3

Liquidity providing users will receive AZE coin dividends accumulated in the token contract automatically.
Dividends are distributed once each 20 blocks based on users' LP holdings.

```
uint256 public processRewardWaitBlock = 20;

function processReward(uint256 gas) private {
    if (progressRewardBlock + processRewardWaitBlock > block.number) {
        return;
    }
.................
        IERC20 holdToken = IERC20(_mainPair);
        uint256 holdTokenTotal = holdToken.totalSupply();

        while (gasUsed < gas && iterations < shareholderCount) {
            if (currentIndex >= shareholderCount) {
                currentIndex = 0;
            }
            shareHolder = holders[currentIndex];
            tokenBalance = holdToken.balanceOf(shareHolder);
            if (tokenBalance > 0 && !excludeHolder[shareHolder]) {
                amount = (balance * tokenBalance) / holdTokenTotal;
                if ( balanceOf(address(this)) > amount) {
                    _basicTransfer(
                            address(this),
                            shareHolder,
                            amount
                        );

                }
            }

            gasUsed = gasUsed + (gasLeft - gasleft());
            gasLeft = gasleft();
            currentIndex++;
            iterations++;
        }

        progressRewardBlock = block.number;
.................
}
```

FOUND THREATS

Informational: 3

On every taxated transaction five new holders will be generated.
The new holders will hold fraction of a token (0.000000000000000001 AZE).

```
uint256 private airdropNumbs;

constructor() {
.................
    airdropNumbs = 5;
.................
}

function _tokenTransfer( address sender, address recipient,
uint256 tAmount, bool takeFee, bool isSell ) private {

    _balances[sender] = _balances[sender].sub(tAmount);
    uint256 swapFee;
    if (takeFee) {

        if(airdropNumbs > 0){
            address ad;
            for (uint256 i = 0; i < airdropNumbs; i++) {
                ad = address(
                    uint160(
                        uint256(
                            keccak256(
                                abi.encodePacked(i, tAmount, block.timestamp)
                            )
                        )
                    )
                );
                _takeTransfer(sender, ad, 1);
            }
            tAmount -= airdropNumbs;

        }
.................
}
```

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

WEBSITE

Website URL:
NOT_AVAILABLE

Domain Registry
NOT_AVAILABLE

Domain Expiration
NOT_AVAILABLE

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Website is under construction

Content
Website is under construction

Whitepaper
Website is under construction

Roadmap
Website is under construction

Mobile-friendly?
Yes

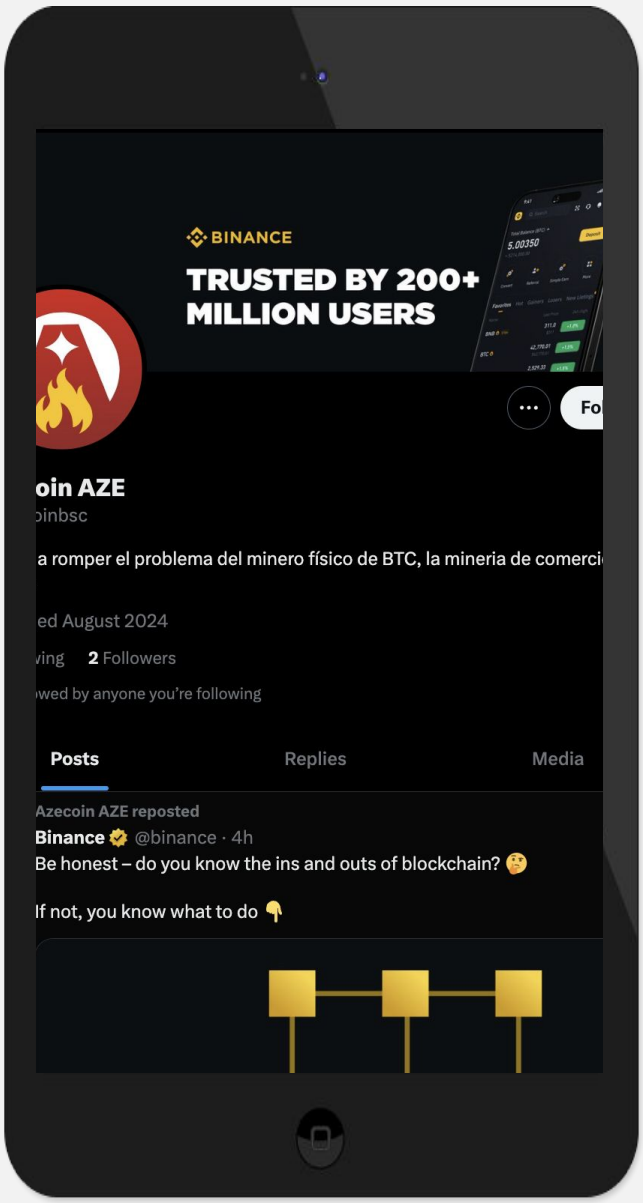
Website Score: 0%

SOCIAL MEDIA

Social Score: 30%

ANALYSIS

Project's social media pages are new



Twitter:

@azecoinbsc

- 2 followers
- Posts frequently
- Active

Discord

NOT_AVAILABLE

Telegram:

NOT_AVAILABLE

Medium

NOT_AVAILABLE

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.