CRACKEN

Smart Contract Security Audit

Project: ZF

Apr 04, 2023

Contract Address

0xaBA5bC952ECE24CDB8a394c247aD68C45B358848

Table of Contents

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the ZF Coin was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	**ZF**
Token Symbol	ZF
Token Decimal	18
Total Supply	88,480
Platform	BSC
Buy Tax Fee	5%
Sell Tax Fee	5%
Contract Creation Date	Apr 04, 2023
Liquidity Status	No liquidity when auditing
Compiler Version	v0.6.12+commit.27d51765
Optimization	Yes with 200 runs
Contract Address	0xaBA5bC952ECE24CDB8a394c247aD68C45B358848
Deployer Address	0x11b3b0ca7a706047b4709448de14c583350b3668
Owner Address	0x11b3b0ca7a706047b4709448de14c583350b3668

Source Code

CRACKEN was commissioned by ZF Coin to perform an audit based on the following smart contract:

https://bscscan.com/address/0xaBA5bC952ECE24CDB8a394c247aD68C45B358848

Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions with Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Grieving	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk

Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Manual Code Review

Classification of Issues

Severity	Description
🔴 High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
🟠 Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
🟡 Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
🔵 Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
🔴 High-Risk	0
🟠 Medium-Risk	4
🟡 Low-Risk	0
🔵 Informational	0
Total	4

● **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set blacklist users

Description:

The owner can set blacklist users

[Medium-Risk]

```
function multi_bclist(address[] calldata addresses, bool value) public onlyOwner{

        require(addresses.length < 201);

        for (uint256 i; i < addresses.length; ++i) {

            _isbclisted[addresses[i]] = value;

        }
```

Recommendation:

We recommend that the owner should disable the blacklist function.

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set max buy / sell tax fee

Description:

The owner can set the buy & sell fees up to 40%

[Medium-Risk]

```
function setBuyFee(uint256 mkt, uint256 reward) external onlyOwner{
        buy_marketingFee = mkt;
        buy_liquidityFee = 0;
        buy_ETHRewardsFee = reward;

        buy_totalFees =
buy_ETHRewardsFee.add(buy_liquidityFee).add(buy_marketingFee);
        require(buy_totalFees <= 400,"cant > 40");
    }

    function setSellFee(uint256 mkt, uint256 reward) external onlyOwner{
        sell_marketingFee = mkt;
        sell_liquidityFee = 0;
        sell_ETHRewardsFee = reward;

        sell_totalFees =
sell_ETHRewardsFee.add(sell_liquidityFee).add(sell_marketingFee);
        require(sell_totalFees <= 400,"cant > 40");

    }
```

● **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set max tx amount

Description:

The owner can set the max tx and wallet amount without limit.

[Medium-Risk]

```
function setMaxTxAndWalletAmount(uint256 txAmount, uint256 walletAmount) public

onlyOwner {

            _maxTxAmount = txAmount;

            _maxWalletAmount = walletAmount;

      }
```

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set trading function is enabled

Description:

The owner can set close trading [Medium-Risk]

```
function setSwapAndLiquifyEnabled(bool status) public onlyOwner(){

          swapAndLiquifyEnabled = status;

     }
```

Recommendation:

We recommend removing the trading function for safety.

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	public
bclistAddress	address account, uint256 amount	public
claim	None	external
decreaseAllowance	address spender, uint256 subtractedValue	public
increaseAllowance	address spender, uint256 addedValue	public
excludeFromDividends	address account	external
excludeFromFees	address account, bool excluded	public
excludeMultipleAccountsFromFees	address[] calldata accounts, bool excluded	public
increaseAllowance	address spender, uint256 addedValue	public
multi_bclist	address[] calldata addresses, bool value	public
processDividendTracker	uint256 gas)	external
renounceOwnership	None	public
setAntiBotEnable	bool status	public
setAutomatedMarketMakerPair	address pair, bool value	public
setBCNumber	uint256 newValue	public
setBurnEnable	bool status	public

Function Name	Parameters	Visibility
setBurnFee	uint256 newValue	public
setBuyFee	uint256 mkt, uint256 reward	external
setMarketingWallet	address payable wallet	external
setMaxTxAndWalletAmount	uint256 txAmount, uint256 walletAmount	public
setSellFee	uint256 mkt, uint256 reward	external
setSwapAndLiquifyEnabled	bool status	public
setTeamWallet	address payable wallet	external
setTransferFree	bool s	public
transfer	address recipient, uint256 amount	external
transferFrom	address sender,address recipient,uint256 amount	external
transferOwnership	address newOwner	public
updateClaimWait	uint256 claimWait	external
updateDividendTracker	address newAddress	public
updateGasForProcessing	uint256 newValue	public
updateUniswapV2Router	address newAddress	public

Contract Ownership

The contract ownership of ZF Coin is not currently being renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x11b3b0ca7a706047b4709448de14c583350b3668
which can be viewed: HERE

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right time if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

Parameter	Result
Pair Address	0xc794c2fdb9339a4c173a759739cd063c1e92d0cb
ZF Reserves	0.00 ZF
USDT Reserves	0.00 USDT
Liquidity Value	$0.00 USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit

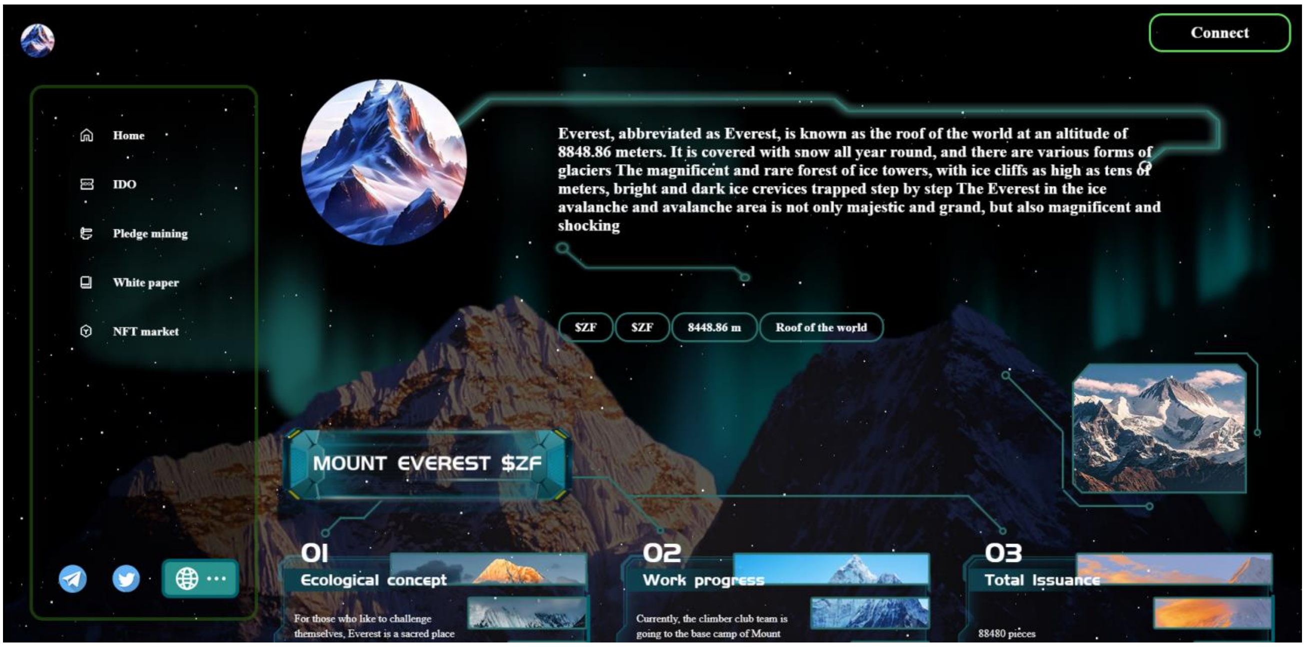
Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x68e2ae90568f6bfa61179e5a74ceb2c416dfe214	88,480	100.00%

Social Media Check

Social Media Type	Link	Result
Website	https://zfcoin.work/	Checked
Twitter	https://twitter.com/ZF8848_	Checked
Telegram	https://t.me/ZF8848	Checked

Website Review



Connect

Home

IDO

Pledge mining

White paper

NFT market

Everest, abbreviated as Everest, is known as the roof of the world at an altitude of 8848.86 meters. It is covered with snow all year round, and there are various forms of glaciers The magnificent and rare forest of ice towers, with ice cliffs as high as tens of meters, bright and dark ice crevices trapped step by step The Everest in the ice avalanche and avalanche area is not only majestic and grand, but also magnificent and shocking

$ZF | $ZF | 8448.86 m | Roof of the world

MOUNT EVEREST $ZF

01 Ecological concept

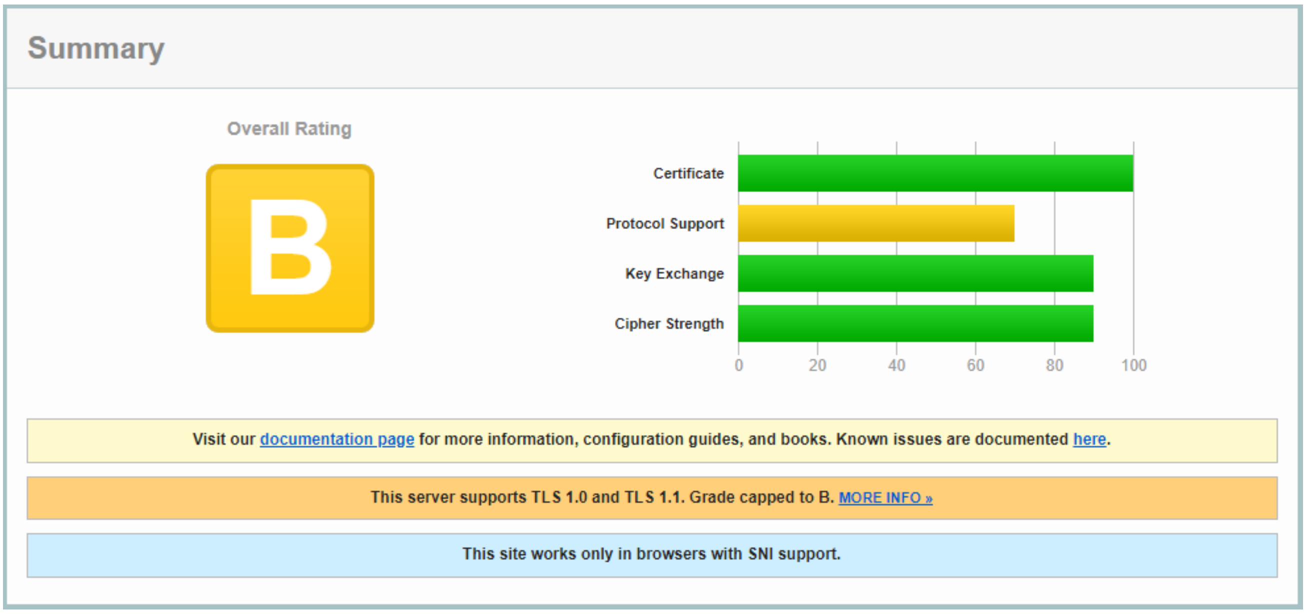
For those who like to challenge themselves, Everest is a sacred place

02 Work progress

Currently, the climber club team is going to the base camp of Mount

03 Total Issuance

88480 pieces



Summary

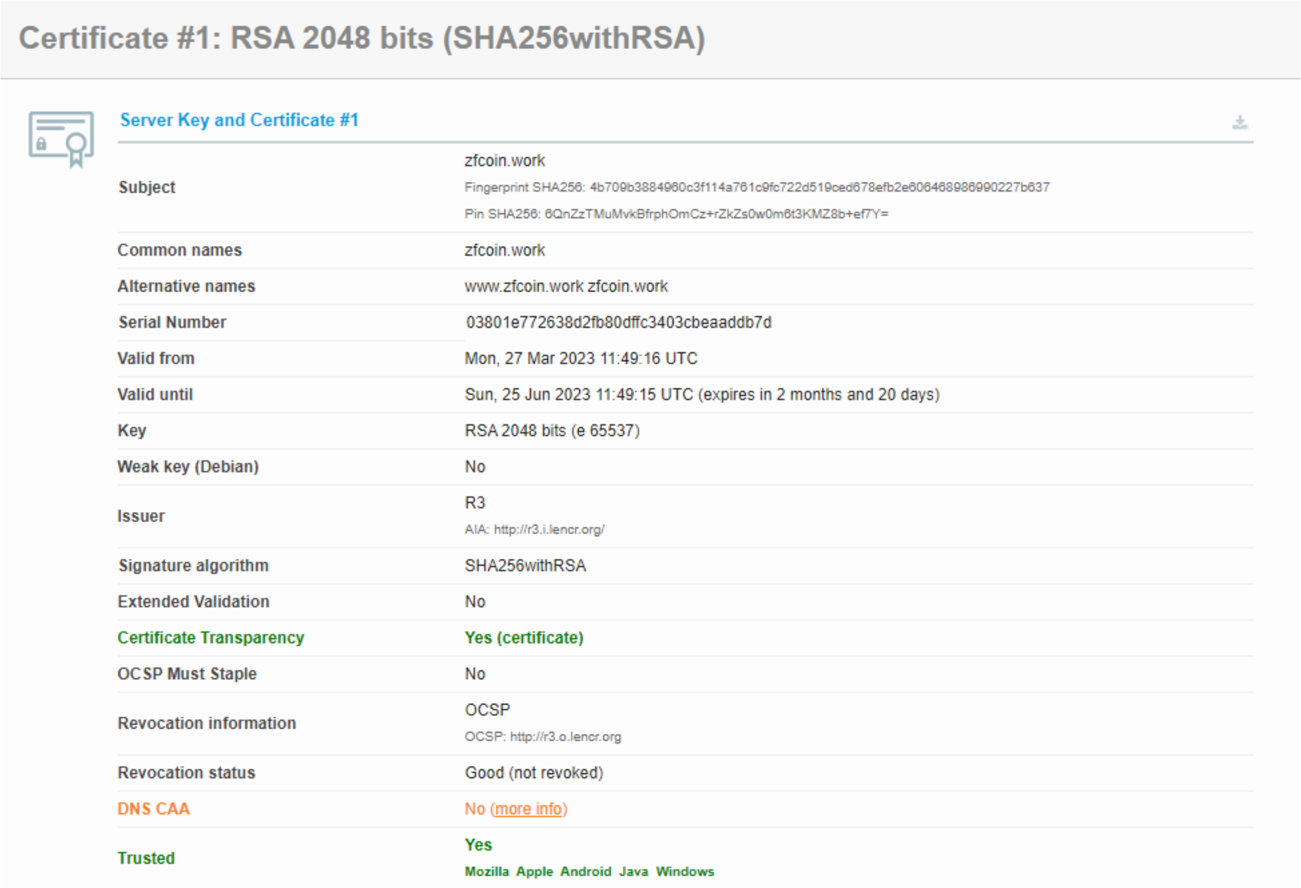
Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	zfcoin.work Fingerprint SHA256: 4b709b3884960c3f114a761c9fc722d519ced678efb2e606468986990227b637 Pin SHA256: 6QnZzTMuMvkBfrphOmCz+rZkZs0w0m6t3KMZ8b+ef7Y=
Common names	zfcoin.work
Alternative names	www.zfcoin.work zfcoin.work
Serial Number	03801e772638d2fb80dffc3403cbeaaddb7d
Valid from	Mon, 27 Mar 2023 11:49:16 UTC
Valid until	Sun, 25 Jun 2023 11:49:15 UTC (expires in 2 months and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors

Audit Conclusion

- **The owner can pause trading [Medium-Risk]**
- The owner cannot mint new tokens
- **The owner can blacklist users [Medium-Risk]**
- **The owner can change the max tx and wallet amount [Medium-Risk]**
- **The owner cannot change buy/sell fees up to 40% [Medium-Risk]**
- The owner can set whitelist wallets.

(No functions can be used if the ownership is being renounced)