



CFG NINJA AUDITS

Security Assessment

Zero Knowledge

Network Token

August 4, 2023

Audit Status: Fail

Audit Edition: Advance














POWERED BY
BLADE POOL

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 Major	Be Careful or Fail test.
 Minor	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
 Buy Tax	0
 Sale Tax	0
 Cannot Buy	Pass
 Cannot Sale	Pass
 Max Tax	10
 Modify Tax	Detected
 Fee Check	Pass
 Is Honeypot?	Not detected
 Trading Cooldown	Not Detected
 Can Pause Trade?	Pass
 Pause Transfer?	Not-Detected



Contract Priviledge	Description
🟡 Max Tx?	Fail
🟡 Is Anti Whale?	Detected
🟢 Is Anti Bot?	Not Detected
🟢 Is Blacklist?	Not Detected
📘 Blacklist Check	Pass
🟢 is Whitelist?	Not Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not detected
🟢 Hidden Owner?	Not detected
📘 Owner	0xcfe9f6d04bad9e79e5e55a0921ce267fe20f4528
🟢 Self Destruct?	Not Detected
📘 Other?	Not detected
🟢 Other?	Not detected
🟢 Holders	1
🟢 Auditor Confidence	High

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

Parameter	Result
Address	
Name	Zero Knowledge Network
Token Tracker	Zero Knowledge Network (OKN)
Decimals	18
Supply	10,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.19+commit.7dd6d404
Contract Name	OKN
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/#code
Payment Tx	0x67d4f7dd5d1dcb1e2b7f218975fa8bd520b296c2ffe5bdd1257974818d5aa8dc

MainNet Contract was Not Assessed

TestNet Contract Assessed



Contract Name

Name	Contract	Live
Zero Knowledge Network	0x1d370884F738318Da03e148BBA5615155d0E78Ad	Yes

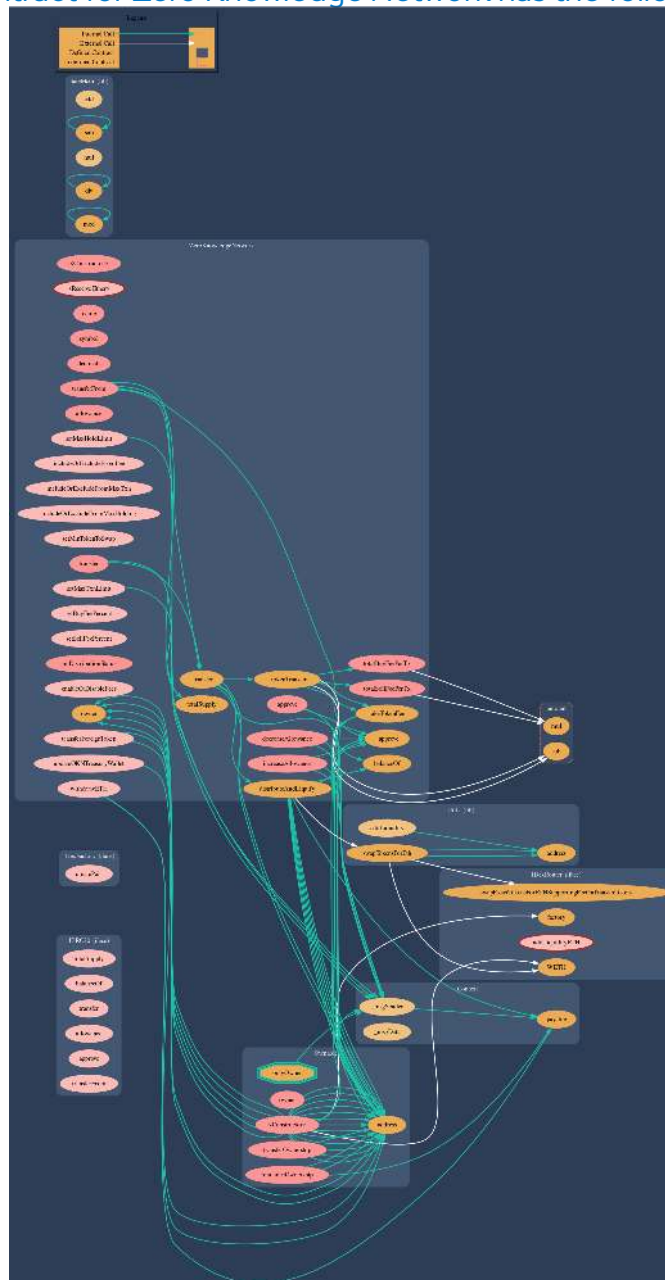
Solidity Code Provided

SolID	File Sha-1	FileName
OKN	d4f0f89ff25c69dfa15dede63bb474f5a9f66b07	OKN.sol
OKN		
OKN		
OKN		



Call Graph

The contract for Zero Knowledge Network has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	OKN.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	OKN.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	OKN.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	OKN.sol	L: 13 C: 0
SWC-104	Pass	Unchecked Call Return Value.	OKN.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	OKN.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	OKN.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	OKN.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	OKN.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	OKN.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	OKN.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	OKN.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	OKN.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	OKN.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	OKN.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	OKN.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	OKN.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	OKN.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	OKN.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	OKN.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randommness.	OKN.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	OKN.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	OKN.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	OKN.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	OKN.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	OKN.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	OKN.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	OKN.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	OKN.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	OKN.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	OKN.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	OKN.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	OKN.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	OKN.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	OKN.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	OKN.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	OKN.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Smart Contract Vulnerability Details

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (<https://github.com/ethereum/solidity/releases>) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

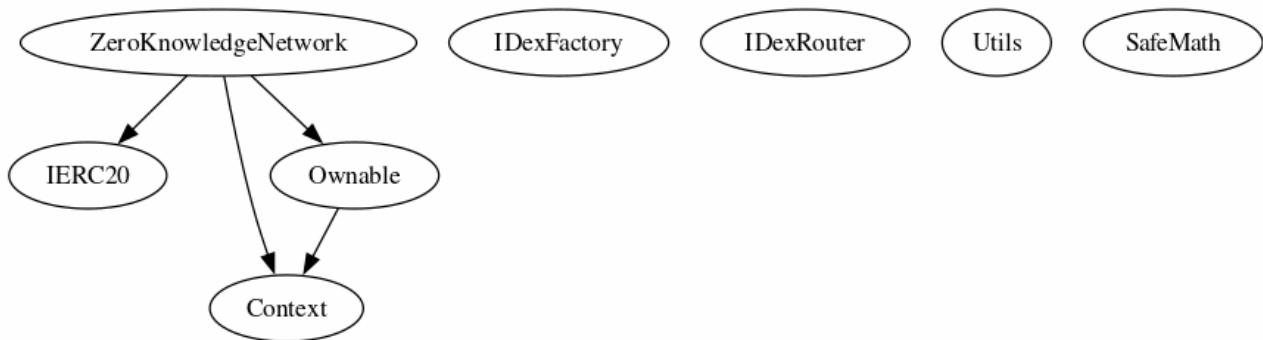
References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.



Inheritance

The contract for Zero Knowledge Network has the following inheritance structure.



Smart Contract Advance Checks



ID	Severity	Name	Result	Status
OKN-01	Minor	Potential Sandwich Attacks.	Fail	Detected
OKN-02	Minor	Function Visibility Optimization	Pass	Not-Detected
OKN-03	Minor	Lack of Input Validation.	Fail	Detected
OKN-04	Major	Centralized Risk In addLiquidity.	Fail	Detected
OKN-05	Minor	Missing Event Emission.	Fail	Detected
OKN-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Detected
OKN-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
OKN-08	Minor	Dead Code Elimination.	Pass	Not-Found
OKN-09	Major	Third Party Dependencies.	Pass	Not-Found
OKN-10	Major	Initial Token Distribution.	Fail	Detected
OKN-11	Minor	transferForeignToken can take own tokens from contract.	Fail	Detected
OKN-12	Major	Centralization Risks In The X Role	Pass	Not-Found
OKN-13	Informational	Extra Gas Cost For User..	Fail	Detected
OKN-6	Medium	Unnecessary Use Of SafeMath	Fail	Detected



ID	Severity	Name	Result	Status
OKN-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found
OKN-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found
OKN-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
OKN-18	Critical	Stop Transactions by using Enable Trade.	Pass	Not-Detected



OKN-01 | Potential Sandwich Attacks.

Category	Severity	Location	Status
Security	 Minor	OKN.sol: 739,14	 Detected

Description

A sandwich attack might happen when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by frontrunning (before the transaction being attacked) a transaction to purchase one of the assets and make profits by back running (after the transaction being attacked) a transaction to sell the asset. The following functions are called without setting restrictions on slippage or minimum output amount, so transactions triggering these functions are vulnerable to sandwich attacks, especially when the input amount is large:

- swapExactTokensForETHSupportingFeeOnTransferTokens()
- addLiquidityETH()

Remediation



We recommend setting reasonable minimum output amounts, instead of 0, based on token prices when calling the aforementioned functions.

References:

What Are Sandwich Attacks in DeFi – and How Can You Avoid Them?.



OKN-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Minor	OKN.sol: 125,14	 Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the unSetPair is missing required function.

Remediation



We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...  
    require(receiver != address(0), "Receiver is the zero address");  
...  
...  
    require(value X limitation, "Your not able to do this function");  
...
```

We also recommend customer to review the following function that is missing a required validation. unSetPair is missing required function.



OKN-04 | Centralized Risk In addLiquidity.

Category	Severity	Location	Status
Coding Style	 Major	OKN.sol: 162,13	 Detected

Description

`uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this), tokenAmount, 0, 0, owner(), block.timestamp);`

The `addLiquidity` function calls the `uniswapV2Router.addLiquidityETH` function with the `to` address specified as `owner()` for acquiring the generated LP tokens from the OKN-WBNB pool.

As a result, over time the `_owner` address will accumulate a significant portion of LP tokens. If the `_owner` is an EOA (Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

Remediation

We advise the `to` address of the `uniswapV2Router.addLiquidityETH` function call to be replaced by the contract itself, i.e. `address(this)`, and to restrict the management of the LP tokens within the scope of the contract's business logic. This will also protect the LP tokens from being stolen if the `_owner` account is compromised. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract based accounts with enhanced security practices, f.e. Multisignature wallets.

1. Indicatively, here are some feasible solutions that would also mitigate the potential risk:
2. Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
3. Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to the private key;



Introduction of a DAO / governance / voting module to increase transparency and user involvement

Project Action

liquidity is set to owner



OKN-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Minor	OKN.sol: 125, 14	 Detected

Description



Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes. The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.



OKN-10 | Initial Token Distribution.

Category	Severity	Location	Status
Centralization / Privilege	 Major	OKN.sol: 461,13	 Detected

Description

All of the Zero Knowledge Network tokens are sent to the contract deployer when deploying the contract. This could be a centralization risk as the deployer can distribute tokens without obtaining the consensus of the community.

Remediation



We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key.

Project Action

```
emit Transfer(address(0), owner(), _tTotal);
```



OKN-11 | transferForeignToken can take own tokens from contract..

Category	Severity	Location	Status
Optimization	 Minor	OKN.sol: 305,14	 Detected

Description

transferForeignToken need to add a require function to prevent contract from withdrawing own tokens, since this can create problems with the swapandliquify function.



Remediation

Add require function to limit address.this

Project Action



OKN-13 | Extra Gas Cost For User.

Category	Severity	Location	Status
Logical Issue	 Informational	OKN.sol: 787, 13	 Detected

Description

The user may trigger a tax distribution during the transfer process, which will cost a lot of gas and it is unfair to let a single user bear it.

Remediation



We advise the client to make the owner responsible for the gas costs of the tax distribution.

Project Action

is declared public



OKN-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	 Medium	OKN.sol: 7,9	 Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations

will automatically revert in case of integer overflow or underflow.

library SafeMath {

An implementation of SafeMath library is found.

using SafeMath for uint256;

SafeMath library is used for uint256 type in contract.

Remediation

We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the

Solidity programming language

Project Action








Technical Findings Summary

Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 Major	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Minor	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	0	0	0
 Major	3	0	0
 Medium	1	0	0
 Minor	3	0	0
 Informational	1	0	0
Total	8	0	0



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/OKnowledge_net	Pass
Other	https://t.me/announcementOKN , https://0101010011.xyz/OKN-Litepaper.pdf , https://000z.gitbook.io/0/	Pass
Website	https://0101010011.xyz/	Pass
Telegram	https://t.me/Entry_Portal_OKN	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

Review	Score
Overall Score	76/100
Auditor Score	60/100
Review by Section	Score
Manual Scan Score	33/53
SWC Scan Score	36 /37
Advance Check Score	7 /19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Fail



Assessment Results

Important Notes:

- Owner needs to enable trade.
- Contract has no taxes.
- Owner can't set max tx amount.
- the following contract need improvements overall. The safemath library used is outdated and should be removed from contract to avoid potential problems.

Auditor Score =60
Audit Fail



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

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. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

