CFG NINJA AUDITS

Security Assessment

zkSync Labs Token

June 6, 2023

Audit Status: Pass

Audit Edition: Advance

zkSync. Labs

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 Sale	Pass
Cannot Sale	Pass
Max Tax	0
Modify Tax	Not 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?	Pass
Is Anti Whale?	Not 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	no
Self Destruct?	Not Detected
External Call?	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	0x8A0C816A52e71A1e9b6719580ebE754709C55198
Name	zkSync Labs
Token Tracker	zkSync Labs (ZKLAB)
Decimals	18
Supply	100,000,000
Platform	Ethereum
compiler	v0.8.18+commit.87f61d96
Contract Name	zkSyncLabs
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0x8A0C816A52e71A1e9b6719580ebE754709C55198#code
Payment Tx	0xab0f5b83f27cff6ffcf9c025f8aa1575edac749e7b2613c679e7f14541ec912b

Main Contract Assessed
Contract Name

Name	Contract	Live
zkSync Labs	0x8A0C816A52e71A1e9b6719580ebE754709C55198	Yes

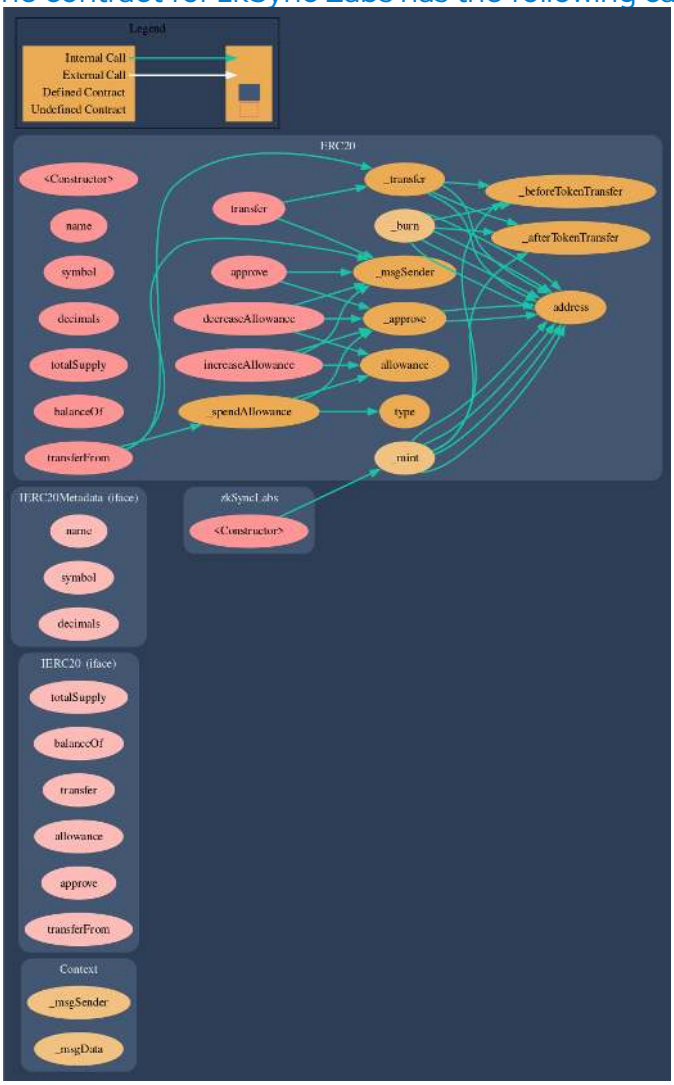
TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
zkSyncLabs	d05a82b586d19a6525f725cb827b241ec853005e	zkSyncLabs.sol
zkSyncLabs		
zkSyncLabs		
zkSyncLabs		

Call Graph

The contract for zkSync Labs 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	zkSyncLabs.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	zkSyncLabs.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	zkSyncLabs.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	zkSyncLabs.sol	L: 0 C: 0
SWC-104	Low	Unchecked Call Return Value.	zkSyncLabs.sol	L: 12 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	zkSyncLabs.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	zkSyncLabs.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	zkSyncLabs.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	zkSyncLabs.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	zkSyncLabs.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	zkSyncLabs.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	zkSyncLabs.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	zkSyncLabs.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	zkSyncLabs.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	zkSyncLabs.sol	L: 0 C: 0
SWC-115	Low	Authorization through tx.origin.	zkSyncLabs.sol	L: 1144 C: 97
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	zkSyncLabs.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	zkSyncLabs.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	zkSyncLabs.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	zkSyncLabs.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	zkSyncLabs.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	zkSyncLabs.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	zkSyncLabs.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	zkSyncLabs.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	zkSyncLabs.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	zkSyncLabs.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	zkSyncLabs.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	zkSyncLabs.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	zkSyncLabs.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	zkSyncLabs.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	zkSyncLabs.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	zkSyncLabs.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	zkSyncLabs.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	zkSyncLabs.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	zkSyncLabs.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	zkSyncLabs.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	zkSyncLabs.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-104 - Unchecked Call Return Value.

CWE-252: Unchecked Return Value.

Description:

The return value of a message call is not checked. Execution will resume even if the called contract throws an exception. If the call fails accidentally or an attacker forces the call to fail, this may cause unexpected behaviour in the subsequent program logic.

Remediation:

If you choose to use low-level call methods, make sure to handle the possibility that the call will fail by checking the return value.

References:

Ethereum Smart Contract Best Practices - Handle errors in external calls.

Smart Contract Vulnerability Details

SWC-115 - Authorization through tx.origin

CWE-477: Use of Obsolete Function

Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

References:

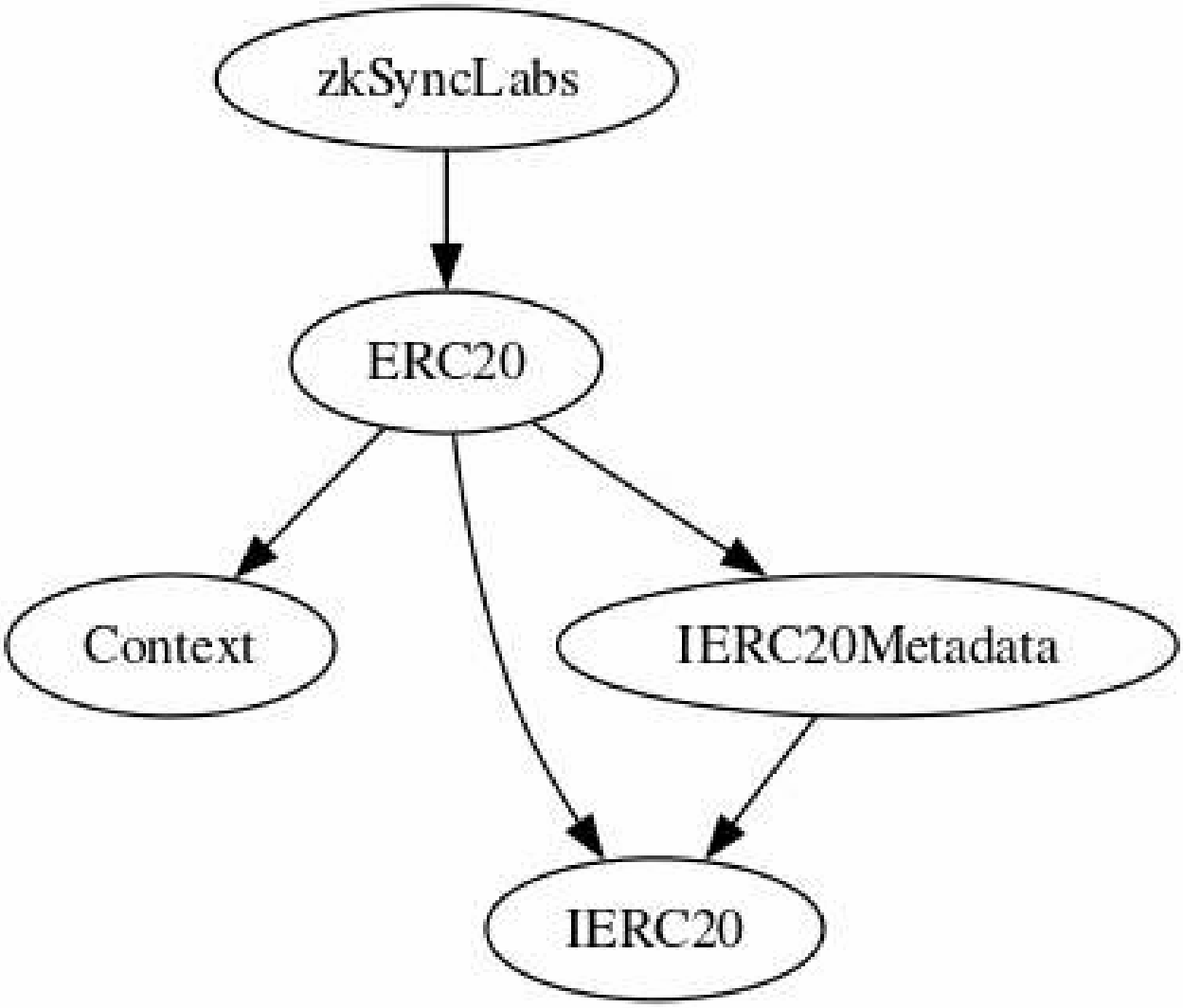
Solidity Documentation - tx.origin

Ethereum Smart Contract Best Practices - Avoid using tx.origin

SigmaPrime - Visibility.

Inheritance

The contract for zkSync Labs has the following inheritance structure.



Smart Contract Advance Checks

ID	Severity	Name	Result	Status
ZKLAB-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
ZKLAB-02	Minor	Function Visibility Optimization	Pass	Not Detected
ZKLAB-03	Minor	Lack of Input Validation.	Pass	Not Detected
ZKLAB-04	Major	Centralized Risk In addLiquidity.	Pass	Not Detected
ZKLAB-05	Minor	Missing Event Emission.	Pass	Not Detected
ZKLAB-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not Detected
ZKLAB-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
ZKLAB-08	Minor	Dead Code Elimination.	Pass	Not-Found
ZKLAB-09	Major	Third Party Dependencies.	Pass	Not Detected
ZKLAB-10	Major	Initial Token Distribution.	Pass	Not-Found
ZKLAB-11	Minor	AntiBot is present on the transfer.	Pass	Not Detected
ZKLAB-12	Major	Centralization Risks In The X Role	Pass	Not-Found
ZKLAB-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
ZKLAB-14	Medium	Unnecessary Use Of SafeMath	Pass	Not Detected
ZKLAB-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found

ID	Severity	Name	Result	Status
ZKLAB-16	Medium	Taxes can be up to 100%	Pass	Not-Found
ZKLAB-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
ZKLAB-18	Medium	Stop Transactions by using Enable Trade.	Pass	Not Detected

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	0	0	0
Medium	0	0	0
Minor	0	0	0
Informational	0	0	0
Total	0	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/ZKSynclabs_io	Pass
Other	https://discord.gg/zksynclabs	Pass
Website	http://zksynclabs.io	Pass
Telegram	https://t.me/zkSyncLabs_Official	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	100/100
Auditor Score	95/100
Review by Section	**Score**
Manual Scan Score	55/53
SWC Scan Score	34 /37
Advance Check Score	24 /19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most 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 Passed

Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- The contract is zero tax.
- Please DYOR on the project.

Auditor Score =95
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

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

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM 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 howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing 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 mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe 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 require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias 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 advocation 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.