Smart Observer

Lishicoin Audit

November, 2021

Introduction

Smart Observer team was commissioned by Lishicoin team to perform project audit.

Audit Notes

Project Name: Lishicoin

Project Website: https://lishicoinlsc.com/

Audit Date: Oct 31 2021 - Nov 1 2021

Audit Scope: Website, Smart Contract

Disclaimer

Smart Observer Disclaimer

You agree to the terms of this disclaimer by reading this report or any portion thereof. This audit is not financial, investment, or any other kind of advice and is for informational purposes only. No one shall be entitled to depend on the report or its contents, and Smart Observer and its affiliates shall not be held responsible to you or anyone else, nor shall Smart Observer provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. The report is provided as "as is" and does not contain any terms and conditions.
This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

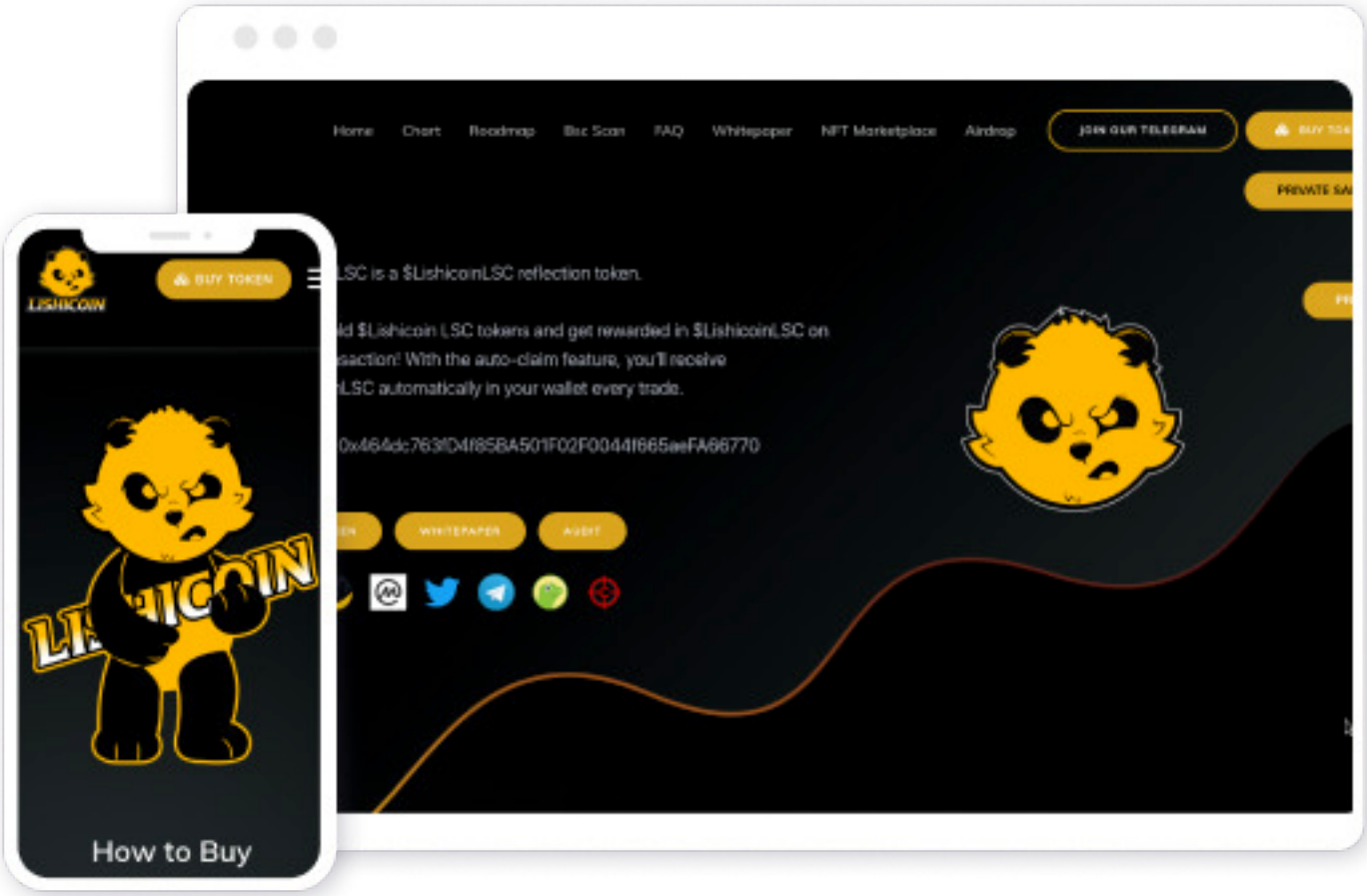
Technical Disclaimer

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 their own vulnerabilities that can lead to hacks. Thus, the audit can not guarantee explicit security of the audited smart contracts.

Table Of Contents

Website Audit

Basic Information



https://lishicoinlsc.com/

Design & Usability

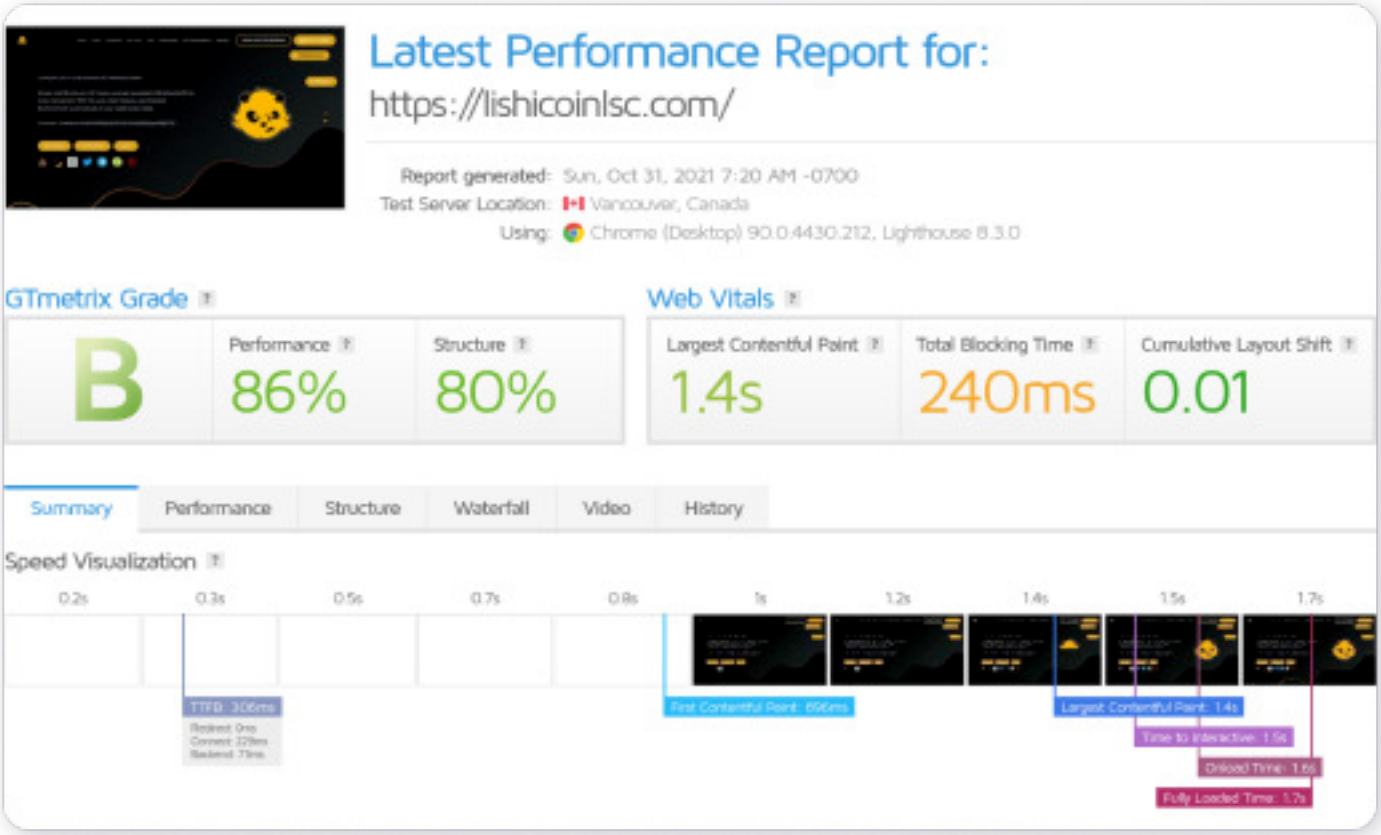
The user experience is great, both on the big screen and on mobile devices. There are no errors in the console. There are no spelling errors either. We think this site is good enough both visually and technically.

Domain Lookup

Created	2021-09-15
Updated	2022-09-15
Expiration	2021-09-16
Data Provider	ICANN | LOOKUP

Since the domain name was purchased several weeks before the launch of the project, we can conclude that the project team was prepared in advance and it is not a one-day project.

Performance Test



Data Provider GTmetrix

We consider this a good enough result for a site that has such heavy design elements like video demonstrations and high-quality illustrations

Static Scan

SSL & Protection

The site is fully protected by hosting. This means having a fresh security certificate at all times, which will ensure that your data is transmitted securely. It also implies protection against DDOS attacks, which means you will always be able to access the site.

Automated Scan

Automated vulnerability scanning of the website did not reveal any critical threats

Performed by OWASP ZAP on Kali Linux

Manual Scan

OWASP TOP10 Scan

A manual scan for the top 10 web applicati on security threats did not reveal any critical vulnerabilities. The functionality of the website is fairly simple and has no potential for serious threats

#	Name	Result
A1	Injection	Not Found
A2	Broken Authentication	Not Found
A3	Sensitive Data Exposure	Not Found
A4	XML External Entities (XXE)	Not Found
A5	Broken access control	Not Found
A6	Security Misconfigurations	Not Found
A7	Cross Site Scripting (XSS)	Not Found
A8	Insecure Deserialization	Not Found
A9	Using Components with Known Vulnerabilities	Not Found
A10	Insufficient Logging & Monitoring	Not Found

Within the audit stage the website does not provide registration and personal profile, in terms of functionality the resource should be considered as purely informational. The presale page offers integration with Metamask wallet and works satisfactorily. In case additional functionality is introduced, another audit is required.

Smart Contract Audit

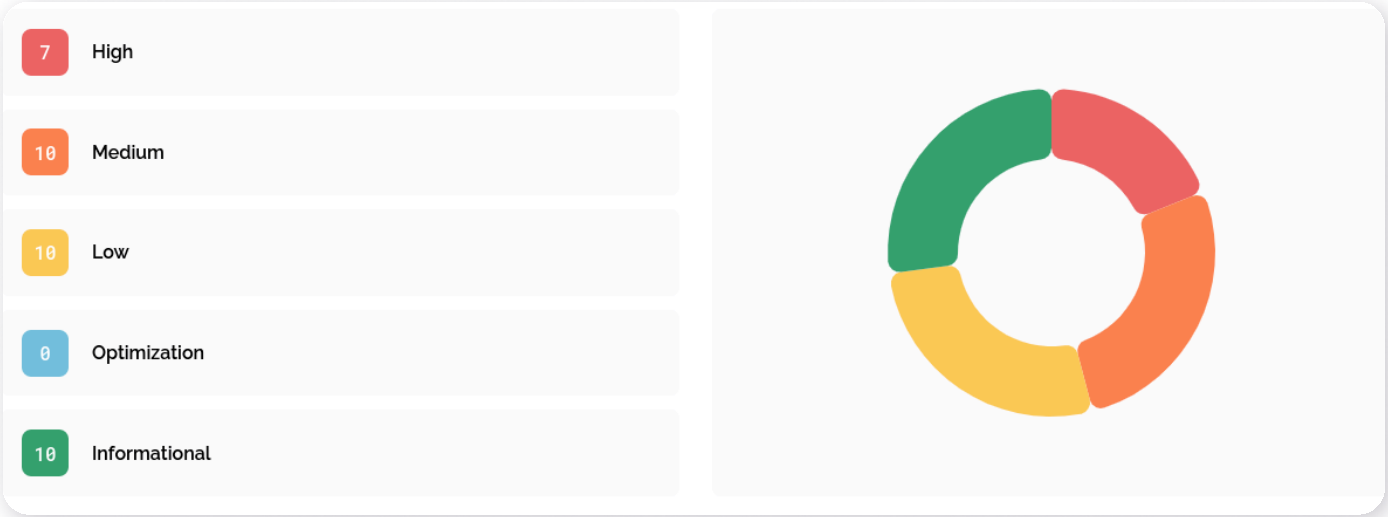
Basic information

Contract Details

Contract address	0x464dc763fD4f85BA501F02F0044f665aeFA66770
Token supply	100,000,000 LSC
Token ticker	LSC
Decimals	9
Deployer address	0xc233Dc511D81CC6D5CAd3B2F8321d5EBD9A1044d
Current owner address	0xc233Dc511D81CC6D5CAd3B2F8321d5EBD9A1044d

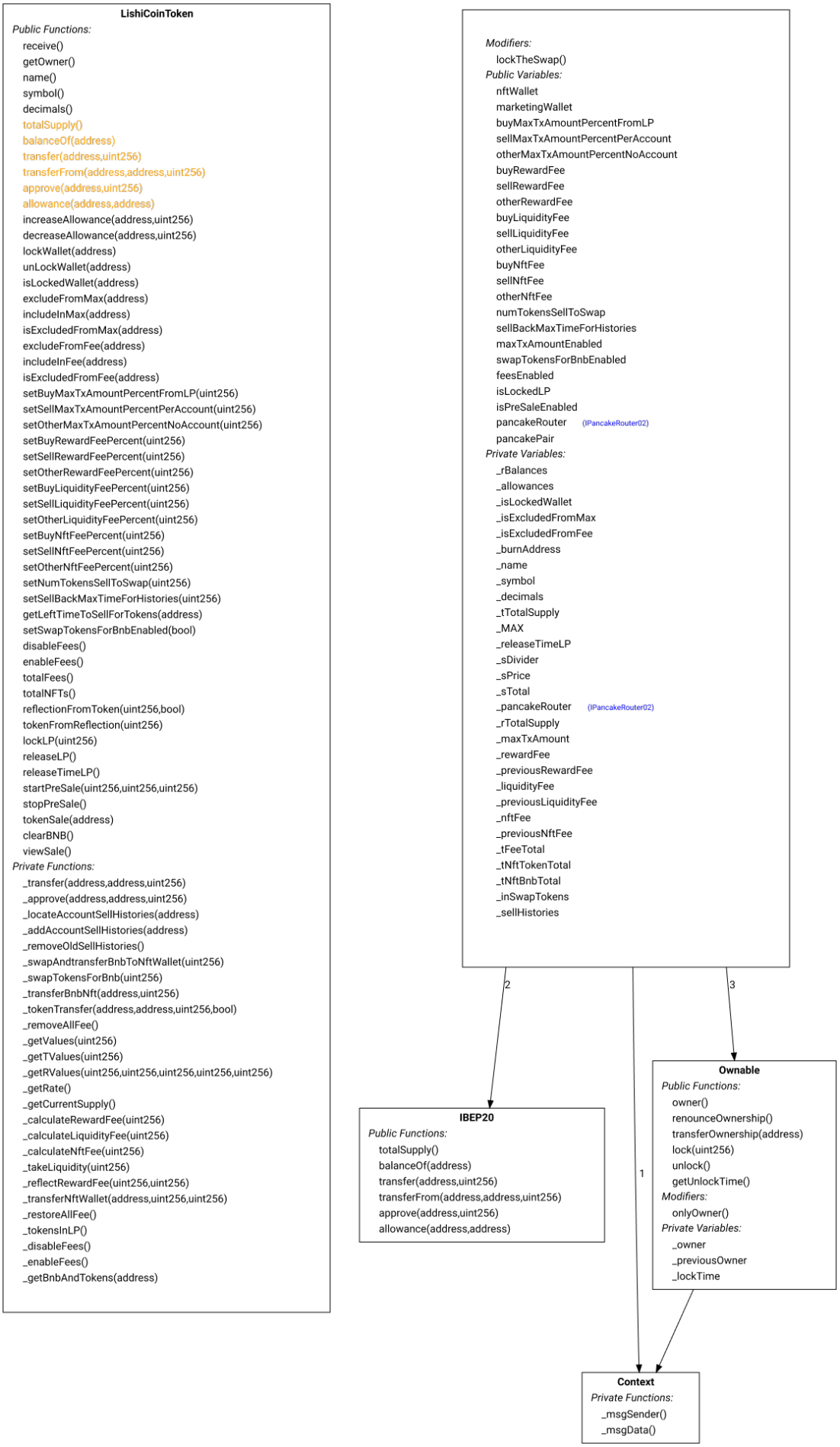
Contract on BscScan

Smart Observer Scan Page

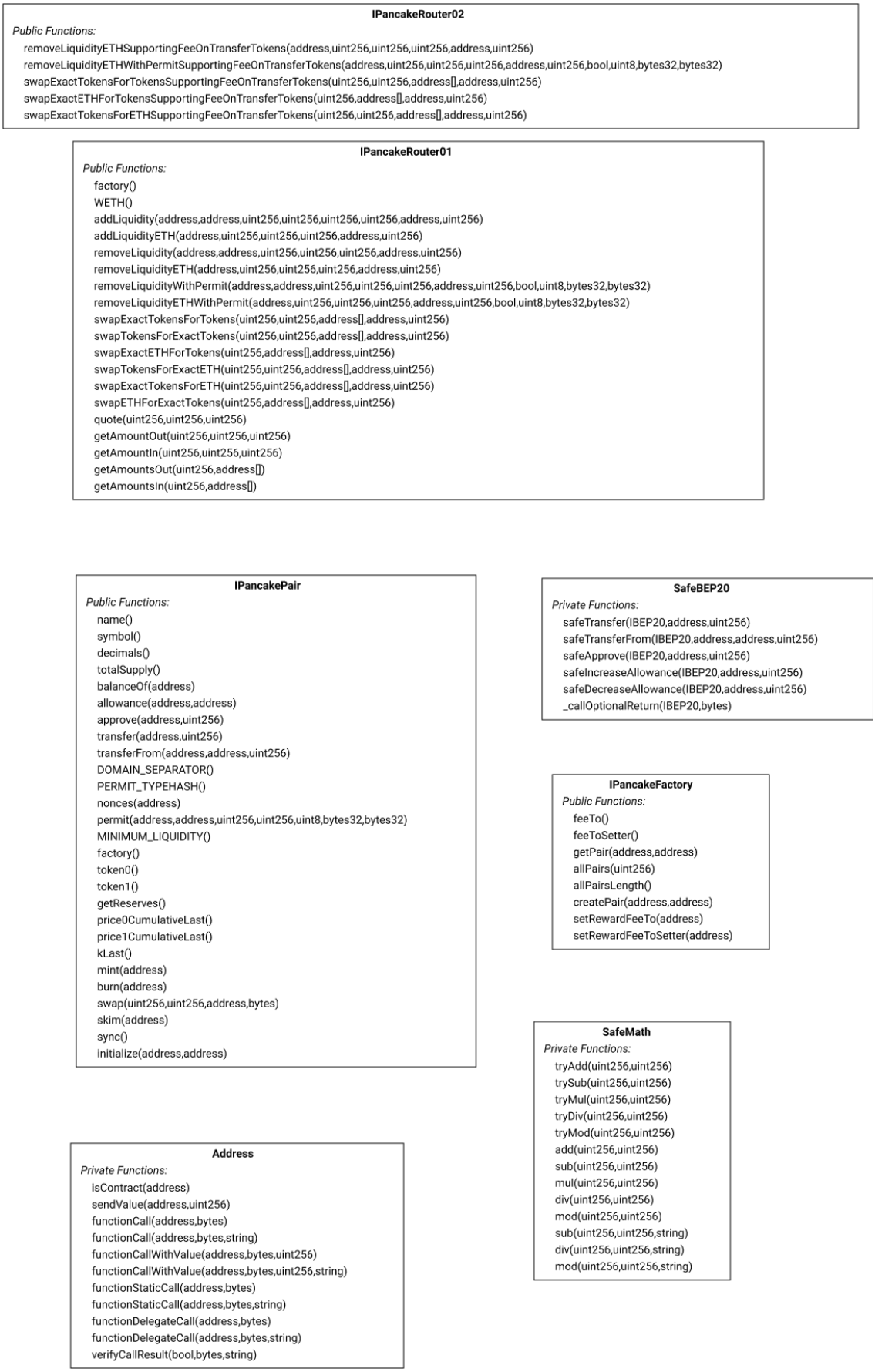


Smart Observer Scan Page

Inheritance Graph



Inheritance Graph



Static Scan

ERC Compliance

```
## Check functions
[✓] totalSupply() is present
 [✓] totalSupply() -> () (correct return value)
 [✓] totalSupply() is view
[✓] balanceOf(address) is present
 [✓] balanceOf(address) -> () (correct return value)
 [✓] balanceOf(address) is view
[✓] transfer(address,uint256) is present
 [✓] transfer(address,uint256) -> () (correct return value)
 [✓] Transfer(address,address,uint256) is emitted
[✓] transferFrom(address,address,uint256) is present
 [✓] transferFrom(address,address,uint256) -> () (correct return value)
 [✓] Transfer(address,address,uint256) is emitted
[✓] approve(address,uint256) is present
 [✓] approve(address,uint256) -> () (correct return value)
 [✓] Approval(address,address,uint256) is emitted
[✓] allowance(address,address) is present
 [✓] allowance(address,address) -> () (correct return value)
 [✓] allowance(address,address) is view
[✓] name() is present
 [✓] name() -> () (correct return value)
 [✓] name() is view
[✓] symbol() is present
 [✓] symbol() -> () (correct return value)
 [✓] symbol() is view
[✓] decimals() is present
 [✓] decimals() -> () (correct return value)
 [✓] decimals() is view
## Check events
[✓] Transfer(address,address,uint256) is present
 [✓] parameter 0 is indexed
 [✓] parameter 1 is indexed
[✓] Approval(address,address,uint256) is present
 [✓] parameter 0 is indexed
 [✓] parameter 1 is indexed
```

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access
Medium	Medium-level vulnerabilities are important to fix; however, they can not lead to assets loss or data manipulations
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can not have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can not affect smart contract execution and can be ignored

Vulnerabilities Scan

Critical

No critical severity vulnerabilities were found

High

1. Sends eth to arbitrary user

```
LishiCoinToken.clearBNB() (LishiCoinToken.sol#1389-1392) sends eth
to arbitrary user
 Dangerous calls:
 - _msgSender().transfer(address(this).balance)
(LishiCoinToken.sol#1391)
```

Explanation: It is considered safe as long as the exchange address is correct

Medium

1. Uninitialized storage variables

```
LishiCoinToken.reflectionFromToken(uint256,bool)._rv_scope_0
(LishiCoinToken.sol#1310) is a storage variable never initialized

LishiCoinToken.reflectionFromToken(uint256,bool)._tv_scope_1
(LishiCoinToken.sol#1310) is a storage variable never initialized
```

Description: An uninitialized storage variable will act as a reference to the first state variable, and can override a critical variable.
Recommendation: Initialize all storage variables. (Can be left as is.)

2. Local variable shadowing

```
LishiCoinToken.allowance(address,address).owner
(LishiCoinToken.sol#1144) shadows:
 - Ownable.owner() (LishiCoinToken.sol#902-904) (function)

LishiCoinToken._approve(address,address,uint256).owner
(LishiCoinToken.sol#1498) shadows:
 - Ownable.owner() (LishiCoinToken.sol#902-904) (function)
```

Description: Detection of shadowing using local variables.
Recommendation: Rename the local variables that shadow another component. (In this case, it can be left as is.)

Low / Lowes

Several low severity vulnerabilities were found
Description: Some minor vulnerabilities (weak documentation for some functions, minor vulnerabilities in already tested libraries)
Recommendation: This vulnerabilities can not affect smart contract execution and can be ignored.

Manual Scan

No critical severity vulnerabilities were found.

Issue Description	Checking Status
Compiler Errors	Passed
Outdated Complier Version	Passed
Re-entrancy	Passed
Possible delays in data delivery	Passed
Shadowing State Variables	Passed
Assert Violation	Passed
Oracle calls	Passed
Front running	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
DoS with Revert	Passed
Malicious Event log	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed

Audit Conclusion

👌 We find this project quite safe.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

✌️ Thank You

smartobserver.online