Liquidcube

Contract Audit Report

VER 1.2

1 April 2022

No. 2022040112161

Project Summary

1. Project Introduction

LiquidCube is a Defi investment service where traders (traders) can define the investment opportunities in which investors can participate. The entire platform is built on a set of smart contracts that protect the lasting interests of all parties. With LiquidCube, traders and investors can interact directly and transparently in a secure environment. A trader can create a SudoCube. a SudoCube has several Cubelets. Investors can purchase several Cubelets to obtain LCNFT. If all cubelets in a SudoCube are sold out, the SudoCube status will be changed to investment complete. After all, Cubelets are sold, a new contract LCCube can be deployed. The investor's base currency will be transferred to the LCCube. The creator of the SudoCube will be the trader (trader) of the LCCube. The base currency in the LCCube can be exchanged for other tokens. These tokens can be added to Uniswap_v3 to earn fees. The LCCube state will change to complete after the length of the time transaction cycle (default is 90 days). If the LCCube state is achieved, traders and investors of the LCCube can liquidate the LCCube. The development team will receive some profit (<= 5%). The creator of the LCCube will receive some commission. The investors of the cube will recover the principal and the remaining profit.

2. Audit Summary

Project Name	Liquidcube	**Platform**	N/A
Token	N/A	**Token symbol**	N/A
Start date	27 Mar 2022	**Language**	Solidity
End date	1 Apr 2022	**Website**	https://www.liquidcube.io/#/home
Github	https://github.com/LCube-Project/lcube-core/tree/ea28932f613e34a2967a56de09e7d7d3bdf7649a	**Whitepaper**	https://liquidcube.gitbook.io/welcome-to-liquidcube/

1 April 2022

3. Audit Scope

ID	File	SHA-256 checksum
contracts	LCCube.sol	96bd8f80aa3daa26e5a367b977e6ae76531ac3a29169c9ad3bf3d0f685c40927
contracts	LCCubeDeployer.sol	a4022a4052c02e2a42329c8683d9602942a36b9de42890cf4de1169d09c1c95d
contracts	LCCubeManager.sol	6b95aa3807a5c00e397b80024b6c48a701f7fb2ada385e65964130c8544b1582
contracts	LCCubeStakingLogic.sol	1fbd41d6abb63d4ba1853dd7d23b15ade9fff372b8e4b255152ebadbe229fda1
contracts	LCCubeSwappingLogic.sol	349c1a6cc05912b0d3516344a04973c70cfa29c005a00f0880baa1ebd3fbdc45
contracts	LCFactory.sol	12046230599133f8c88577b76a3c1f640a7cac8a34923c02d906e56dce0774bf
contracts	LCPeriphery.sol	03990676bc1c52ccc2f6fe950d682c3a45c49690694b8fa424e1b6380b3d8e78
contracts/base	InternalWhitelistControl.sol	1354f1ba79dd7ed8d745f6adb16c713d31de0e66cbe81207d51514bf2f897771
contracts/base	Multicall.sol	4430da1c44911d30f308ee33eb74acadf069b1670b2a72867344ac5cd1d9f8ba

4. Code Structure

```
├─── LCCube.sol
├─── LCCubeDeployer.sol
├─── LCCubeManager.sol
├─── LCCubeStakingLogic.sol
├─── LCCubeSwappingLogic.sol
├─── LCFactory.sol
├─── LCPeriphery.sol
├─── base
|    ├─── InternalWhitelistControl.sol
|    └─── Multicall.sol
└─── interfaces
   ├─── ILCCube.sol
   ├─── ILCCubeDeployer.sol
   ├─── ILCCubeManager.sol
   ├─── ILCCubeStakingLogic.sol
   ├─── ILCCubeState.sol
   ├─── ILCCubeSwappingLogic.sol
   ├─── ILCFactory.sol
   ├─── ILCPeriphery.sol
   ├─── IMulticall.sol
   ├─── IPlatformSelector.sol
   ├─── IUseStaking.sol
   └─── IUseSwapping.sol
```

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review	**Key Components**	**-**

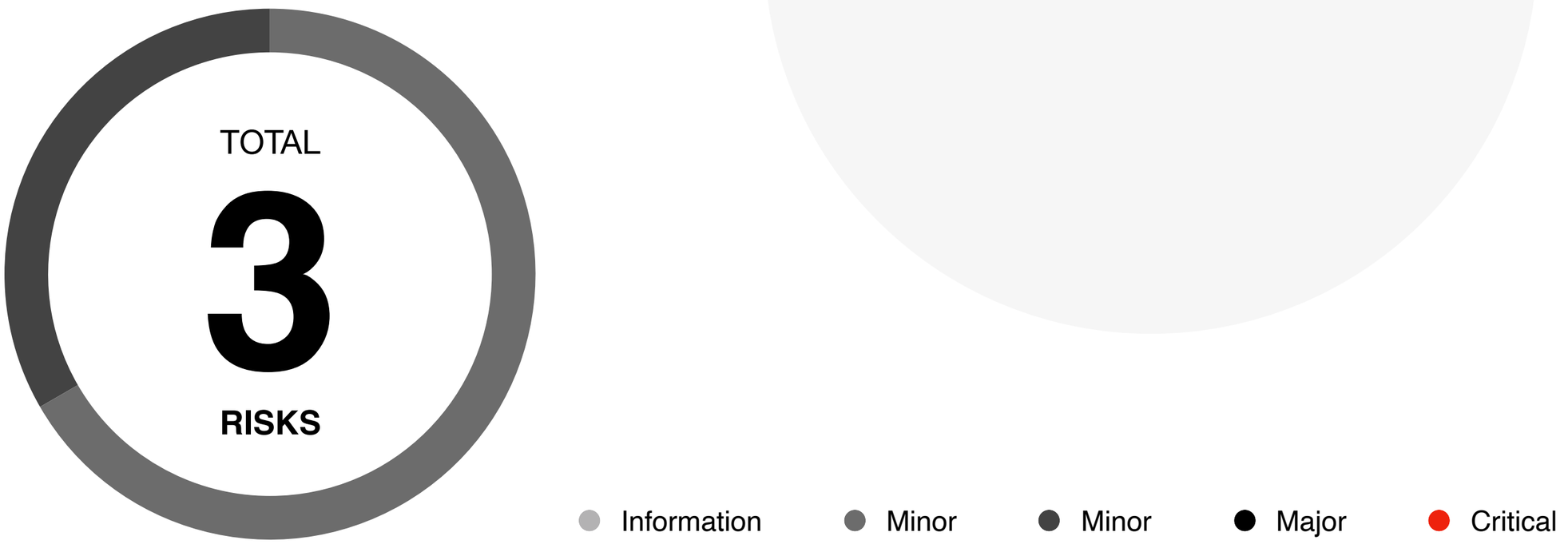
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	Minor	Acknowledge
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	None	
24	Risk of liquidity drain	None	
25	Centralization Risk	Medium	Acknowledge
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	Minor	Acknowledge
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Has collision	None	

5. Risk and Modification program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	**Insufficient Gas Griefing**	**Risk level**	**Minor**
Location	Line 506	**Contract file**	LCCube.sol
Description	There is a loop of unknown size, and there are external calls in the loop		
Recommedation	Limit the number of loops, or do not make external calls in the loop		
Update	The project owner promises to limit the size of the loop		

Risk type	**Centralization risk**	**Risk level**	**Medium**
Location	Line 211、Line 233、 Line 280、Line 314	**Contract file**	**All**
Description	The trader has too much authority to dispose of assets and is prone to undue influence		
Recommedation	Use timelock or multi-signature		
Update	Traders’ dispose of assets is limited by the platform selection, token whitelist, number of cubelets and the single cubelet value. Each of these fields declares a boundary on traders’ behavior. The platform selection limits the platform for trading, the token whitelist limits the types principal. These fields are all transparent to investors. Therefore, Investors can evaluate the risk before they invest in any cube. Furthermore, the cube assets can only be moved inside the LC protocol or to the trading platform(uniswap V3)throughout the entire process. So traders cannot use these assets for other purposes. To minimize risk of undue influence, investors have access to the cube liquidate function(liquidateCubeRelay) once the trading period is over. Therefore, the cube investors can have their money back even if the trader is absent. Traders’ history records are also on-chain and visible to everyone. We’ll take a close look at any suspicious behavior from traders and warn the investors.		

Risk type	Improper initialization of variables	Risk level	Minor
Location	Line 26~28、Line23~24、Line24~25、Line26~28	**Contract file**	LCCubeManager.sol、LCCubeSwappingLogic.sol、LCCubeStakingLogic.sol、LCCube.sol
Description	Hard-coded state variables		
Recommendation	Assigning state variables using Abi pass-through form		
Update	The project's business logic relies on hard-coded uniswap v3 addresses		

6. Recommendation

N/A

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

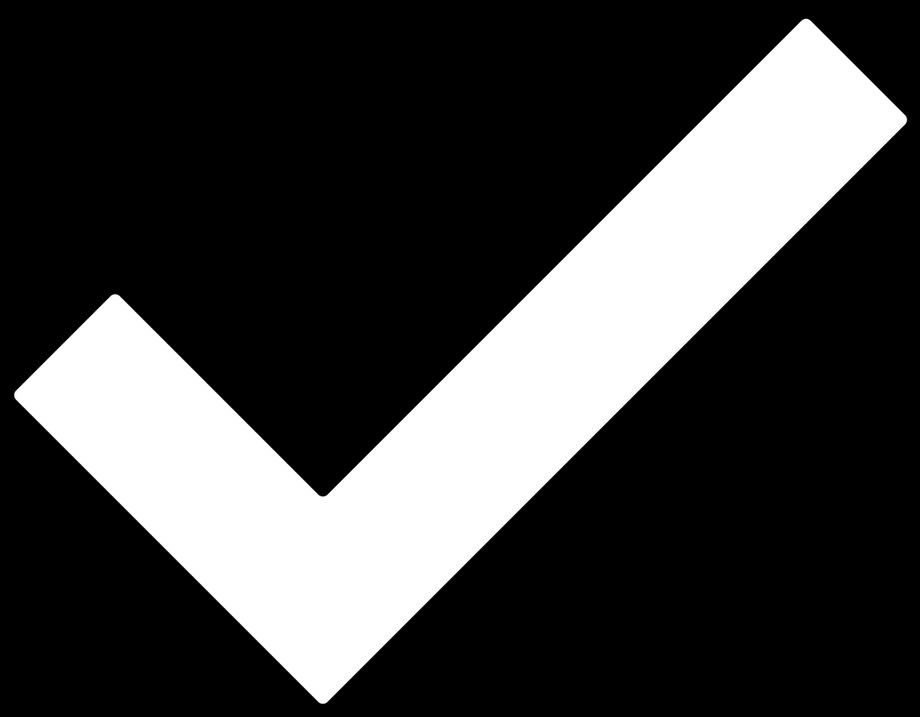
Disclaimer

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.

1 April 2022



PASSED.

DATE 1 April 2022

AUDITOR 歐科雲鏈

This audit aims to review the investment, pledge, uniswapv3 liquidity clearing, and NFT credentials protocols written in Solidity language based on the liquidcube project, study its design architecture, discover potential security risks, and try to find possible vulnerabilities.