Liquidcube

合約審計報告

VER 1.2

2022年4月1日

No. 2022040112160

項目總結

1. 項目介紹

LiquidCube是一個DeFi投資服務，交易員（trader）可以定義投資者可以參與的投資機會。整個平台建立在一套保護各方的持久利益智能合約之上。有了LiquidCube，交易員和投資者可以在一個安全的環境中直接透明的互動。
trader可以創建一個SudoCube。一個SudoCube有一些Cubelets。投資者可以購買一些Cubelets獲得LCNFT。如果一個SudoCube中的所有cubelets都售罄，則SudoCube狀態將更改為投資完成。所有Cubelets售出後，可以部署新的合同LCCube。投資者的基礎貨幣將被轉移到LCCube。SudoCube的創建者將是LCCube的交易員（trader）。LCCube中的基礎貨幣可以兌換成其他代幣。這些代幣可以添加到Uniswap_v3中以賺取手續費。在時間交易周期長度（默認為90天）之後，LCCube態將更改為已完成。如果LCCube狀態完成，LCCube的交易員和投資者可以清算該LCCube。開發團隊將獲得一些利潤（<=5%）。LCCube的創建者將獲得一些佣金。立方體的投資者將收回本金和剩餘利潤。

2. 審計詳情

項目名	Liquidcube	平台	N/A
代幣	N/A	代幣符號	N/A
開始日期	2022年3月27日	開發語言	Solidity
結束日期	2022年3月28日	網頁	https://www.liquidcube.io/#/home
代碼	https://github.com/LCube-Project/lcube-core/tree/ea28932f613e34a2967a56de09e7d7d3bdf7649a	介紹	https://liquidcube.gitbook.io/welcome-to-liquidcube/

2022年3月29日

3. 審計範圍

ID	文件	SHA-256
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. 代碼結構

```
├─── 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
```

審計報告匯總

1. 審計方式

通過清晰地理解該項目的設計目的、運行原理和實現方式，審計團隊對合約代碼進行了深入的研究和分析。在釐清各個合約及其函數的調用關係的基礎上，對合約可能存在的漏洞進行了定位及分析。最終產生問題描述和給出相應的修改意見。

審計方法	Static analysis, Manual Review	**Key Components**	**-**

2. 審計流程

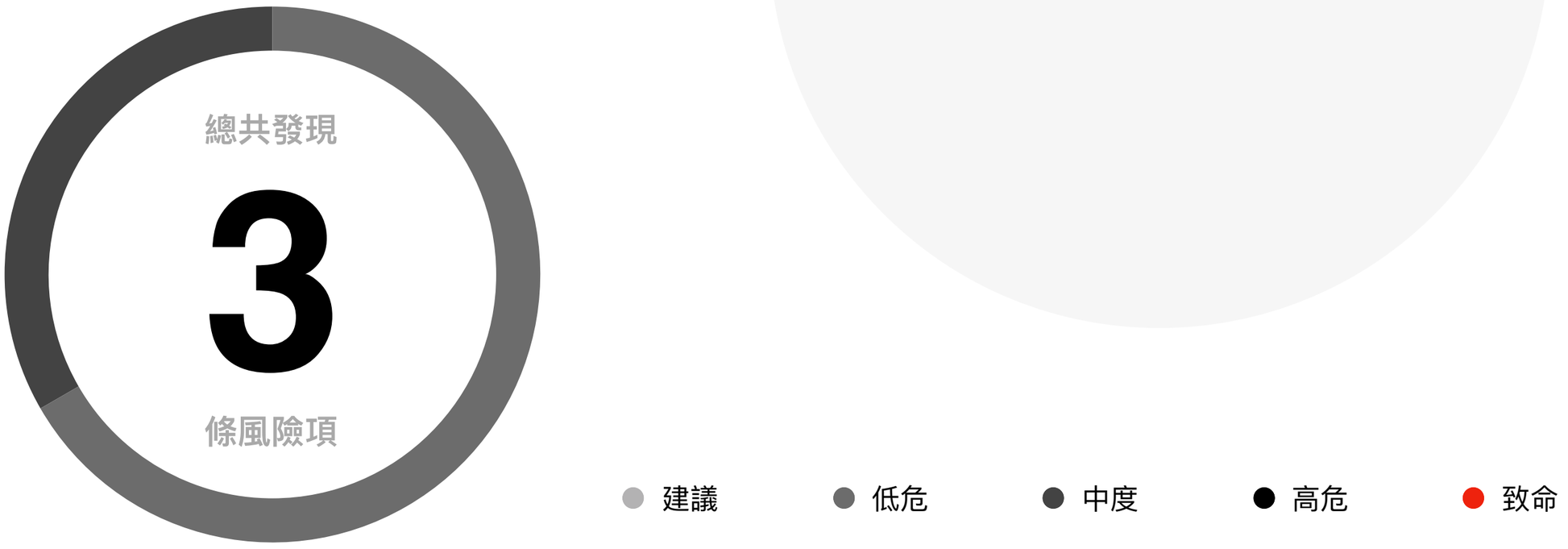
步驟	操作	詳細內容
1	背景研究	閱讀項目介紹、白皮書、合約源碼等項目方團隊提供的相關信息，確保正確理解項目功能
2	自動化檢測	主要用自動化工具掃描源碼，找到常見的潛在漏洞
3	人工審閱	工程師逐行閱讀代碼，找到潛在漏洞
4	邏輯校對	工程師將對代碼的理解和項目方提供的信息比較，檢查代碼實現是否符合項目白皮書信息
5	測試用例檢測	包括測試用例設計，測試範圍分析、符號執行等
6	優化審查	根據應用場景、調用方式及最新的研究成果從可維護性、安全性及可操作性等方面審查項目

2022年4月1日

3. 風險分級

風險級別	風險描述
致命	存在致命風險及隱患，需要立即解決
高危	存在高危風險及隱患，將引發相同問題，必須解決
中度	存在中度風險及隱患，可能導致潛在風險，最終仍然需要解決
低危	存在低風險及隱患，指各類處理不當或會引發警告信息的細節，這類問題可暫時擱置
建議	存在可優化的部分，這類問題可以擱置，但建議最終解決

4. 審計結果



編號	審計項目	風險級別	狀態
1	重入	無	
2	注入	無	
3	權限繞過	無	
4	Mempool搶跑	無	
5	回滾	無	
6	條件競爭	無	
7	循環耗盡gas	低	已告知
8	閃電貸高影響	無	
9	經濟模型不合理	無	
10	可預見的隨機數	無	
11	投票權管理混亂	無	

編號	審計項目	風險級別	狀態
12	數據隱私洩露	無	
13	鏈上時間使用不當	無	
14	Fallback函數編碼不當	無	
15	鑒權不當	無	
16	Opcode使用不當	無	
17	內聯匯編使用不當	無	
18	構造函數不規範	無	
19	返回值不規範	無	
20	Event不規範	低	
21	關鍵字使用不規範	無	
22	未遵循ERC標準	無	
23	條件判斷不規範	無	
24	流動性枯竭風險	無	
25	中心化風險	中	已告知
26	邏輯變更風險	無	
27	整數溢出	無	
28	函數可見性不當	無	
29	變量初始化不當	低	已告知
30	合約間調用不當	無	
31	變量不規範	無	
32	重放	無	
33	隨機存儲位置寫入	無	
34	蜜罐邏輯	無	
35	哈希碰撞	無	

2022年4月1日

5. 風險項與修改方案

以下部分為審計後得知的風險項相關詳細信息，其中內容包括風險類型、風險級別、問題位置、問題描述、修改建議及項目方反饋。

風險類型	循環耗盡gas	風險級別	低風險
位置	Line 506	合約文件	LCCube.sol
問題描述	存在循環，且大小未知，循環中存在外部調用		
修改建議	限定循環次數，或不在循環中進行外部調用		
項目方反饋	項目方承諾會限制循環的大小		

風險類型	中心化風險	風險級別	中風險
位置	Line211、Line233、Line280、Line314	合約文件	All
問題描述	Trader處置資產權限過大，容易產生不當影響		
修改建議	使用timelock或多簽		
項目方反饋	交易員對資產的處置受到平臺選擇、代幣白名單、cubelet數量和單個cubelet價值的限制。 這些字段中的每一個都聲明了交易員行為的邊界。 平臺選擇限制了平臺的交易，代幣白名單限制了可用於交易的代幣的類型，cubelet的數量和cubelet單價限制了委託人的規模。 這些字段對投資者都是透明的。 因此，投資者可以在投資任何cube之前評估風險。 此外，在整個過程中，cube資產只能在LC協定內移動或移動到交易平臺（uniswap V3）。 因此，交易員不能將這些資產用於其他目的。 為了將不當影響的風險降至最低，一旦交易期結束，投資者可以使用cube清算功能（LiquidateCuberlay）。 因此，即使交易者缺席，項目投資者也可以拿回他們的錢。 交易員的歷史記錄也在鏈上，每個人都可以看到。 我們將密切關注交易員的任何可疑行為，並警告投資者。		

風險類型	變量初始化不當	風險級別	低風險
位置	Line 26~28、Line23~24、 Line24~25、Line26~28	合約文件	LCCubeManager.sol、 LCCubeSwappingLogic.sol、 LCCubeStakingLogic.sol、 LCCube.sol
問題描述	硬編碼的狀態變量		
修改建議	使用abi傳參形式賦值狀態變量		
項目方反饋	項目方業務邏輯依賴硬編碼的uniswap v3地址		

6. 增強建議

N/A

免責聲明

i. 本審計報告僅針對最終出具報告中載明的審計類型進行審計，其他未知安全漏洞不在本次審計責任範圍之內，我方無需為此承擔責任。

ii. 我方僅應根據審計報告發布之前存在或發生的攻擊或漏洞發布審計報告。對於將來存在或發生的新攻擊或漏洞，我方無法確定對其項目安全狀態的可能影響，對此概不負責。

iii. 我方發布的審計報告中的安全審計分析及其他內容應僅基於項目方在發布審計報告之前向我方提供的文件和材料（包括但不限於合約代碼），並且上述文件和資料不應該存在缺乏信息、被篡改、刪除或隱藏的情況，如果項目方提供的文件和資料存在不真實、不準確、缺乏信息、被篡改、刪除或隱藏的情況，或者對上述文件和資料的改動是在發布審計報告之後作出的，我方不承擔因反映情況與實際情況不一致引起的損失和不利影響 。

iv. 項目方知曉我方出具的審計報告系根據項目方提供的文件和資料、依靠我方現掌握的技術而作出的。但由於任何機構均存在技術的局限性，我方作出的審計報告仍存在無法完整檢測出全部風險的可能性。我方審計團隊鼓勵項目的開發團隊以及任何相關利益方對項目進行後續的測試及審計。

v. 項目方保證其委托我方提供審計或測試服務的項目合法、合規，且不違反適用法律。審計報告僅用於項目方參考，審計報告的內容、獲取方式、使用以及任何其所涉及的服務或資源都不能作為任何形式的投資、稅務、法律、監管及建議等的依據，我方不因此承擔相關責任。在未經我方書面同意之前，項目方不得將審計報告的全部或部分內容以任何形式提及、引用、展示或發送給任何第三方，否則由此產生的任何損失和責任由項目方自行承擔。我方對任何人依賴審計報告或將之用於任何目的概不承擔責任 。

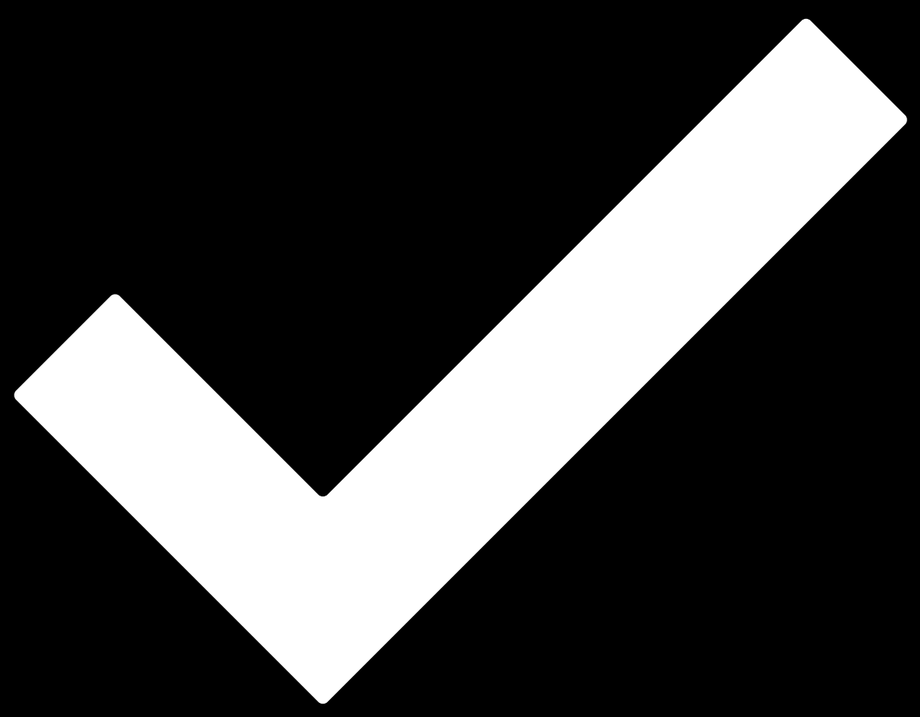
vi. 本審計報告不涉及合約的編譯器及任何超出智能合約編程語言的領域，所審計的智能合約因引用鏈下信息或資源所導致的風險及責任，由項目方自行承擔 。

vii. 不可抗力。不可抗力是指雙方在訂立合同時不能預見、對其發生和後果不能避免且不能克服的事件，包括但不限於戰爭、臺風、水災、火災、地震、潮汐、雷電、天災、罷工、核爆炸、流行病等自然災害和法律、法規和政策變更及政府行為等其它不可預見，對其發生和後果不能防止或避免的事件，且該事件妨礙、影響或延誤任何一方根據合同履行其全部或部分義務。

viii. 如果有一方認為不可抗力發生影響履行本協議義務，應迅速通知另一方，按事件對履約影響的程度，由雙方協商決定是否終止合同或部分免除履約的責任，或者延期履約。

ix. 當不可抗力發生時，任何一方都不能被視作違約或不履行本協議義務。在事件前存在的經濟上的責任，不應受到影響，項目方應對我方已完成工作做出支付。

2022年4月1日



審計通過.

日期 2022年4月1日

審計 歐科雲鏈

本次審計的目的是為了審閱liquidcube項目基於Solidity語言編寫的投資、質押、uniswapv3流動性清結算、NFT憑證等協議，研究其設計、架構，發現潛在的安全隱患，並試圖找到可能存在的漏洞。