OKCSwap

合約審計報告

VER 1.0

2022年4月11日

No. 2022041119220

項目總結

1. 項目介紹

OKC 的願景為「構築元宇宙的數字基石」，並在近期主要發力 GameFi、SocialFi 等賽道，存在海量資產交換的潛在需求。為補齊OKC上Swap賽道短板，推出官方項目OKCSwap，用穩定的國庫激勵回饋用戶。OKCSwap核心功能包含資產兌換、提供資產流動性以及流動性挖礦。合約代碼主要參考Uniswap V2以及Sushiswap。第一期OKCSwap僅支持交易對LP（liquidity provider）質押挖礦，不支持單幣質押挖礦，一期所有挖礦池僅提供OKT獎勵，不支持其它代幣獎勵。

2. 審計詳情

項目名	OKCSwap	平台	N/A
代幣	N/A	代幣符號	N/A
開始日期	2022年3月28日	開發語言	Solidity
結束日期	2022年4月11日	網頁	N/A
代碼	https://github.com/okex/OECSwap/tree/a130b2c56af22502234f0dca65e14e4acf098ea1	介紹	N/A

3. 審計範圍

ID	文件	SHA-256
farm	StakingRewards.sol	268685746cd62c5330e5016cf0e60b6c25b5b99145b1a895ffa2b49fb6a71722
farm	StakingRewardsFactory.sol	15554906d609007b1b136f24b74b6ea6e846a218003b4a762cf87279907ebfca
interfaces	IERC20.sol	4c3eb92afca9f12d682595ce5ee7381de2ab6b752e6f880a428795afede52497
interfaces	IOKCSwapCallee.sol	0de42dda65d3199707c12503c74c4cf4a744892a0d68cc94cfd0c599bf55c785

ID	文件	SHA-256
interfaces	IOKCSwapERC20.sol	08a197b39ca55561709b1ae9d55a83193918877fcb8d3fc8d7fc28f6cf35363a
interfaces	IOKCSwapFactory.sol	288c304729b04cba2beab1361334ea72511d06376b0d513a9e96eb27120ec81e
interfaces	IOKCSwapPair.sol	484b37ba6332afca20b065021a37376e41a364082bbde92fbd1c8b2385681e3c
interfaces	IOKCSwapRouter01.sol	2259360819e12e5c767be95f46a76bb94737492751f1d12928d3ef4044ce10a0
interfaces	IOKCSwapRouter02.sol	3173ef5d7253b558defc2498ade7731225a70854e9c0ff89f7b9a8f6f3eb2d6b
interfaces	IStakingRewards.sol	e0724813ceaf4acf4fd196502d70517261857eda7f88d3dbf84614bedb4a239a
interfaces	IWOKT.sol	c3eeda5f5057932ac963cff3635660d777ccc5ff424aac170811f3d4bb2cd748
libraries	Math.sol	e68b7c4743a8b6b14a2e7e42df7b7fdc8364092a97601f1d4452606bf948f4dd
libraries	OKCSwapLibrary.sol	410cfa6eb1dd7fca4f72b66c9f1ef57385e74c344e149cbc8f7b87cac5b5e206
libraries	OKCSwapOracleLibrary.sol	b0f84906fdd4b4e131fc5a1d99ce396b26a87cbc618d0c61521cf07f78efe59e
libraries	RewardsDistributionRecipient.sol	04383c6f197e9b9a380739aa1c233b1007a4d59d0b39e675ed72a36e425f246d
libraries	SafeMath.sol	a1b95b64f8a15b15ecbb725d372985f1499cf86be38557a4cac784d58dfcf5ba
libraries	UQ112x112.sol	5c7f8b7dc61af3440ce5782d25b210dc92b5d898862d2bb5651a25ff34c8df70
mocks	mockERC20.sol	9191e5ce80b3258dc8f621716dc584b23b8a8e2673c06e80baf6e594187e371f
mocks	mockWETH.sol	d013b3e0d26df562b672cd79b03321e4fe0fc63361a05a5d069481854678e495
pair	OKCSwapERC20.sol	f9ee6b6aa000f4caba0d84b6009ea710c8cd3fe535d4ffb78b4610a6cc835ed5
pair	OKCSwapFactory.sol	9c7450c1bf6738a62b7b641bc635aed8e5f0bda256384ae36416446e256c883a
pair	OKCSwapPair.sol	23ce6bb79ce8833ac86e05ba5ff701fbbe64953daa2cfd27ba2d074224ef721a
router	OKCSwapRouter02.sol	9544742257dd23d1ff6404a483912a6d905689111da0b49abc962b78b1807015

2022年4月11日

4. 代碼結構

```
contracts
├── farm
|   ├── OKCSwap.svg
|   ├── StakingRewards.sol
|   └── StakingRewardsFactory.sol
├── interfaces
|   ├── IERC20.sol
|   ├── IOKCSwapCallee.sol
|   ├── IOKCSwapERC20.sol
|   ├── IOKCSwapFactory.sol
|   ├── IOKCSwapPair.sol
|   ├── IOKCSwapRouter01.sol
|   ├── IOKCSwapRouter02.sol
|   ├── IStakingRewards.sol
|   └── IWOKT.sol
├── libraries
|   ├── Math.sol
|   ├── OKCSwapLibrary.sol
|   ├── OKCSwapOracleLibrary.sol
|   ├── RewardsDistributionRecipient.sol
|   ├── SafeMath.sol
|   └── UQ112x112.sol
├── mocks
|   ├── mockERC20.sol
|   └── mockWETH.sol
├── pair
|   ├── OKCSwapERC20.sol
|   ├── OKCSwapFactory.sol
|   └── OKCSwapPair.sol
└── router
    └── OKCSwapRouter02.sol
```

2022年4月11日

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。在厘清各個合約及其函數的調用關系的基礎上，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**	-

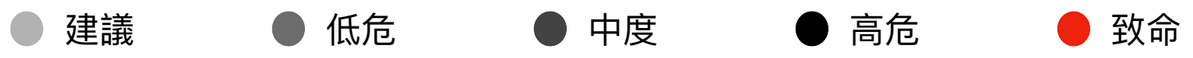
2. 審計流程

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

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	無	
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	無	
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	無	
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11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	中心化風險	風險級別	中風險
位置	all	合約文件	StakingRewardsFactory.sol
問題描述	涉及權限控製的合約函數，都沒有timelock機製，或多簽機製		
修改建議	將單個私鑰權限分散，且使用timelock和多簽機製		
項目方反饋			

6. 增強建議

N/A

2022年4月11日

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 。

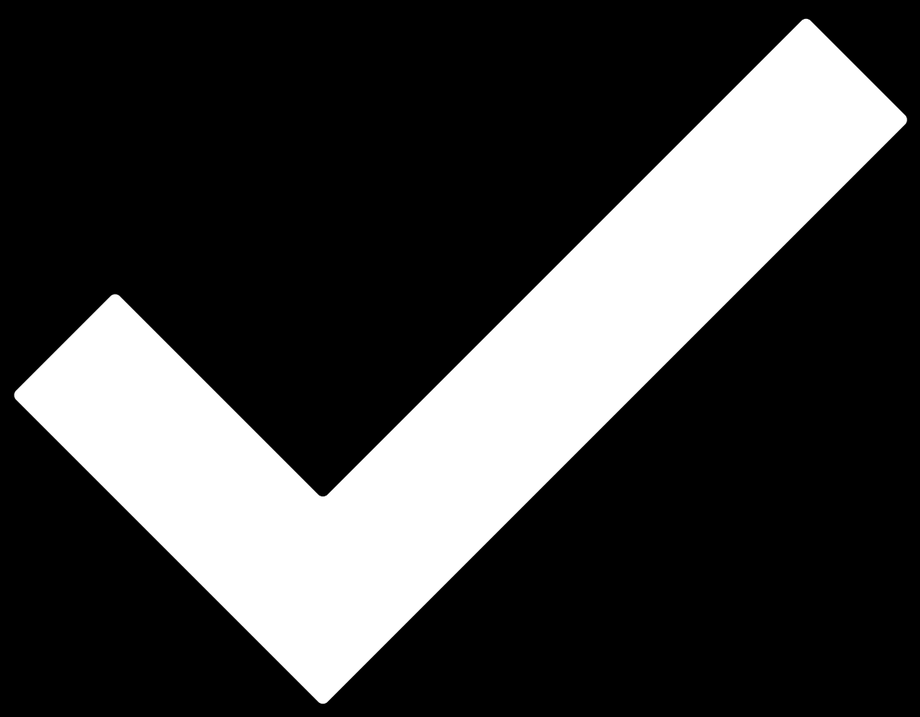
vi. 本審計報告不涉及合約的編譯器及任何超出智能合約編程語言的領域，所審計的智能合約因引用鏈下信息或資源所導致的風險及責任，由項目方自行承擔 。

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11日



審計通過.

日期 2022年4月11日

審計 歐科雲鏈

本次審計的目的是為了審閱OKCSwap項目基於Solidity語言編寫的DEX及流動性挖礦功能，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。