IBC ERC20 Module

合約審計報告

VER 1.0

2022年6月14日

No. 2022061411090

項目總結

1. 項目介紹

IBC-ERC20的合約主要是服務於OKC的IBC功能，當有其他鏈通過IBC協定向OKC跨鏈新的資產的時候，OKC會自動為該資產部署一套對應的ERC20合約，包括：

- contracts/ModuleERC20. sol
- contracts/ModuleERC20Proxy. sol

同時，如果有部署在OKC上的原生ERC20資產，想要通過IBC協定跨到其他的鏈上，那麼該ERC20需要繼承以下合約：

- contracts/nativeERC20/NativeERC20Base. sol

2. 審計詳情

項目名稱	IBC ERC20 Module	平台	N/A
通證名稱	N/A	通證代號	N/A
開始時間	2022年6月10日	語言	Solidity
結束時間	2022年6月13日	官網	N/A
Github	https://github.com/okex/IBC-ERC20/tree/5989f7305276ce25274b04dfc2c7499afc38a571/contracts	白皮書	N/A

2022年6月14日

3. 審計範圍

ID	文件	SHA-256 checksum
contracts	REC20.sol	d5830e888ac60f02a2adbc46ac1de125809ff15d1f3add9cd65530f838c692f0
contracts	ModuleERC20.sol	bfcb78767353ff237c2940853a9e9d901513c60d0c59fb11e6d6bbc07ab2af48
contracts	ModuleERC20Proxy.sol	f408a817804e4501c340db9a1d89de77bde2cc12b6dc64ba51a2222bcc69eb74
contracts/ nativeERC20	NativeERC20Base.sol	98eafb512ec1330397757bff81ad76930db177c640b5cb2f9c9b68144c68ec6f

4. 代碼結構

```
├── ERC20.sol                    #基礎ERC20協定
├── ModuleERC20.sol              #通過IBC協定向OKC跨鏈的ERC20代幣範本
├── ModuleERC20Proxy.sol         #通過IBC協定向OKC跨鏈的ERC20代幣的可更新代理合約
└── nativeERC20
    └── NativeERC20Base.sol      #通過IBC協定由OKC向其他鏈跨鏈的ERC20代幣基類
```

2022年6月14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、運行原理和實現管道，稽核團隊對合約程式碼進行了深入的研究和分析。 在分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

2. 審計流程

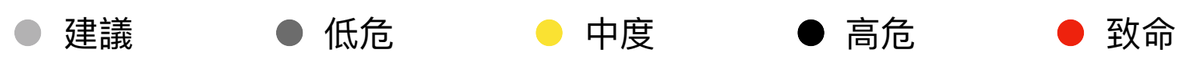
步驟	操作	詳細內容
1	背景研究	閱讀項目介紹、白皮書、合約源碼等項目方團隊提供的相關信息，確保正確理解項目功能
2	自動化檢測	主要用自動化工具掃描源碼，找到常見的潛在漏洞
3	人工審閱	工程師逐行閱讀代碼，找到潛在漏洞
4	邏輯校對	工程師將對代碼的理解和項目方提供的信息比較，檢查代碼實現是否符合項目白皮書信息
5	測試用例檢測	包括測試用例設計，測試範圍分析、符號執行等
6	優化審查	根據應用場景、調用方式及最新的研究成果從可維護性、安全性及可操作性等方面審查項目

2022年6月14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	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	

2022年6月14日

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	中	已修改
24	流動性枯竭風險	無	
25	中心化風險	無	
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	
36	領獎邏輯不當	無	
37	使用不推薦的方法	無	
38	未遵循基本編碼原則	無	
39	多次初始化風險	高	已修改

* 上述表格中，狀態欄內容若為**「已告知」**，則表示審計團隊已告知項目方項目存在的漏洞，但項目方未對漏洞進行修改，或未告知審計團隊漏洞的修改進度。若狀態欄中填寫**「已修改」**則表示項目方已進行對漏洞的修改，並通過審計團隊確認。

2022年6月14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。

1. 條件判斷不規範

位置	文件	風險状态	風險級別
Line 25	ERC20.sol	已修改	中風險

① 風險描述

條件判斷不規範是描述一類條件判斷語句編碼不規範的問題。 在需要條件判斷的地方，未使用require，或條件判斷的條件存在不規範的編碼。
由於條件判斷語句往往決定了合約的具體執行邏輯，為了避免合約出現預期外的執行邏輯，建議規範條件判斷程式碼。
在本項目中，ERC20. sol Line25，require（_decimals == 0，“ERC20: already initialized；”）； 由於合約並未限制初始化參數decimals_ 的值，所以存在部署合約時傳入decimals_== 0的情況，從而導致該語句希望起到的init一次的限制作用失效。

② 修改建議

建議允許ERC20代幣的decimals為0，使用bool值來標記是否初始化。

③ 項目方迴響

A. 將ERC20. sol合約是否初始化修改為使用獨立的布林值判斷。
B. 將所有合約的solidity版本修改為確定的0.8.7，而不是使用^0.8.0。

③ 關聯程式碼

```JavaScript
    function __ERC20_init(
        string memory name_,
        string memory symbol_,
        uint8 decimals_
    ) internal {
        //@OKLink Audit Description: 存在條件失效的可能
        //@OKLink Audit Solution: 使用bool值作為初始化判斷flag
        require(_decimals == 0, "ERC20: already initialized;");

        _name = name_;
        _symbol = symbol_;
        _decimals = decimals_;
    }
```

2022年6月14日

2. 多次初始化風險

位置	文件	風險状态	風險級別
Line 13	MouduleERC20.sol	已修改	高風險

① 風險描述

初始化函數因設定明確的bool值作為是否已經初始的判斷條件，否則在合約鏈上執行初始化後，會出現預期之外的再次初始化調用，導致狀態變數被非安全的修改。
在本項目中，由於超類初始化函數中的條件判斷可能失效，所以會導致該初始化函數再次被執行的風險。

② 修改建議

建議使用bool值作為初始化判斷flag

③ 項目方迴響

A. 將ERC20. sol合約是否初始化修改為使用獨立的布林值判斷。
B. 將所有合約的solidity版本修改為確定的0.8.7，而不是使用^0.8.0。

2022年6月14日

③ 關聯程式碼

```JavaScript
    function initialize(string memory denom_, uint8 decimals_) public {
        //@OKLink Audit Description: 未進行是否已初始化判斷，__ ERC20_ init函數初始化判斷可能失效
        //@OKLink Audit Solution: 使用bool值作為初始化判斷flag
        __ERC20_init(denom_, denom_, decimals_);
    }
```

2022年6月14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 。

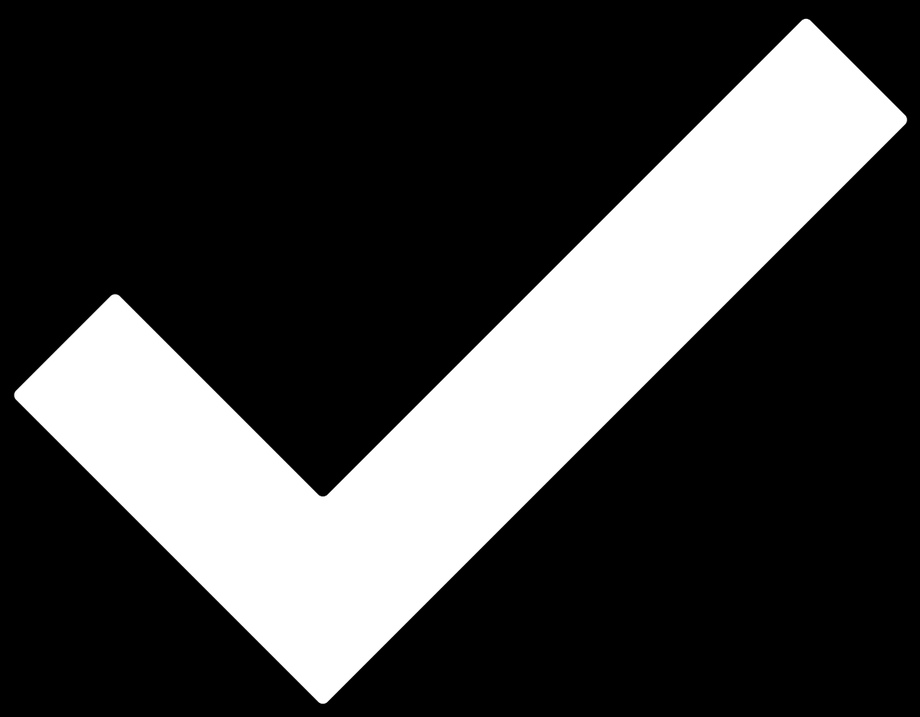
vi. 本審計報告不涉及合約的編譯器及任何超出智能合約編程語言的領域，所審計的智能合約因引用鏈下信息或資源所導致的風險及責任，由項目方自行承擔 。

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6月14日



審計通過.

日期 2022年6月14日

審計 歐科雲鏈

本次稽核的目的是為了審閱OKC基於Solidity語言編寫的用於IBC跨鏈的模組化ERC20合約，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。