



# MetaX跨链Swap

## 合約審計報告

VER 1.1

2022年6月8日

No. 2022060816580

# 項目總結

## 1. 項目介紹

MetaX聚合橋跨鏈項目主要是做一款跨鏈swap產品，其中包含跨鏈橋模塊，聚合協力廠商跨鏈橋。通過對外提供api介面，由後端選擇最優跨鏈路徑，選擇對應的協力廠商合約提供跨鏈服務。同時接入了dex的swap功能，用戶可選擇在swap後進行跨鏈行為。

## 2. 審計詳情

項目名稱	MetaX跨链Swap	平台	N/A
通證名稱	N/A	通證代號	N/A
開始時間	2022年5月30日	語言	Solidity
結束時間	2022年6月2日	官網	N/A
Github	<a href="https://github.com/okex/MetaX-Bridge-Core">https://github.com/okex/MetaX-Bridge-Core</a>	白皮書	N/A

## 3. 審計範圍

ID	文件	SHA-256 checksum
contracts	XBridge.sol	ca6c22679e6a4d507deaa655beb25d34dec0d435ed9774a ae5ff4cc7aec2405b
contracts	BridgeAdaptorBase.sol	268fcced2637b53e4b36de23326b5a9b63df82fb7c5a32123 5b07a0ee43ded74
contracts/adaptor	AnyswapAdaptor.sol	93819f85ce6eda8db531355bca0f482d1b12578ffa0749f612 648a95edf481df
contracts/adaptor	CBridgeAdaptor.sol	8d93dcd66e789aac0ec3304e342af67c889cdd138c18d953 0f9517c9e3de4a9a
contracts/libraries	Pb.sol	6ce3019660da99f51737db5aa81a795420b5b410fc6c6c10 4157674208de8f78
contracts/libraries	PbPool.sol	d6122ac4039bee1b863b86e6f9c34adf4a7c7c762a802027ff 2955fdddce06dd

## 4. 代碼結構

- └── BridgeAdaptorBase.sol
- └── BridgeAdaptorBase.sol
- └── XBridge.sol
- └── adaptor
  - └── AnyswapAdaptor.sol
  - └── CBridgeAdaptor.sol
- └── libraries
  - └── Pb.sol
  - └── PbPool.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

### 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	建議	未修改
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	建議	未修改
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	低	部分修改
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	

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。

## 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	協力廠商依賴風險	風險級別	低風險
位置	All	合約文件	XBridge.sol
問題描述	對協力廠商dex的安全性依賴較高		
修改建議	即時監控協力廠商dex安全風險，及時暫停合約功能		
項目方反饋	已通知項目方，未進行修改，此風險項依賴於協力廠商項目安全性，且本項目已包含合約帳戶資金緊急選取功能		

風險類型	中心化風險	風險級別	低風險
位置	Line 48	合約文件	CBridgeAdaptor.sol
問題描述	管理員owner可能會因輸入錯誤意外的修改某個transferId的退款地址		
修改建議	在參數中加入服務端簽名校驗		
項目方反饋	已修改，在setRecords函數中添加了針對修改操作的日誌記錄		

風險類型	中心化風險	風險級別	低風險
位置	Line 180	合約文件	XBridge.sol
問題描述	項目調用合約的管道為服務端包裝參數後傳給前端再調用合約abi，需注意防範服務端入侵、中間人攻擊、釣魚等風險		
修改建議	在參數中加入服務端簽名校驗		
項目方反饋	已通知項目方，未進行修改，因風險項依賴於非合約端安全性，且合約端已包含了關鍵參數驗證邏輯		

風險類型	鑒權不當	風險級別	建議
位置	Line 181	合約文件	XBridge.sol
問題描述	在某些攻擊發生時，攻擊者可能會利用此項目合約，依賴adaptor進行跨鏈		
修改建議	可在此合約中添加跨鏈金額上限，對某些攻擊造成的大額跨鏈行為進行攔截		
項目方反饋	已通知項目方，攔截行為由adaptor對應的協力廠商跨鏈橋負責，本項目不需修改		

風險類型	重入	風險級別	建議
位置	ALL	合約文件	XBridge.sol CBridgeAdaptor.sol
問題描述	經排查，項目合約內部出現互相重入的可能性較低，但可能出現跨項目跨合約重入		
修改建議	在對資金敏感操作時，儘量限制調用destination的身份為外部帳戶； 在進行代幣轉帳時，儘量對代幣添加黑白名單		
項目方反饋	已通知項目方，攔截行為由adaptor對應的協力廠商跨鏈橋負責，本項目不需修改		

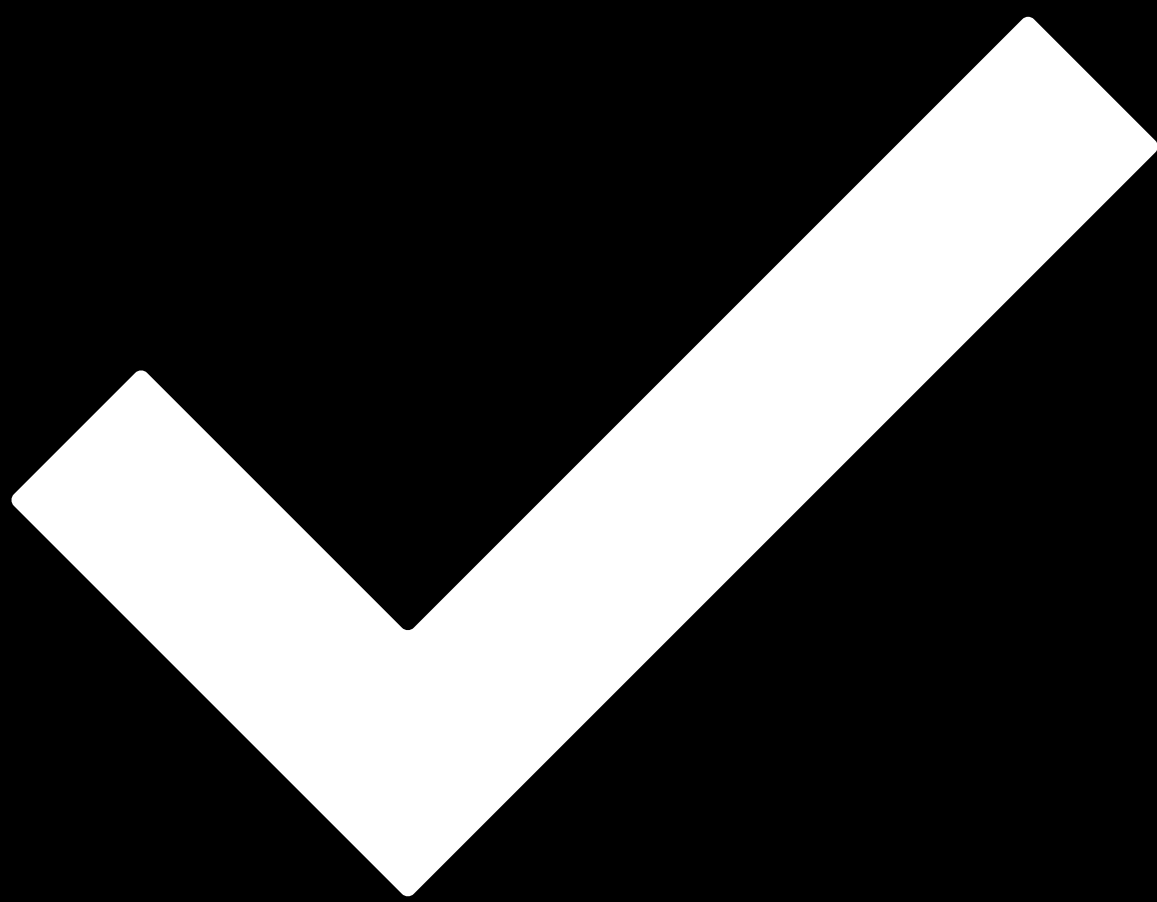
## 6. 增強建議

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。



# 審計通過.

日期 2022年6月8日

審計 歐科雲鏈

本次稽核的目的是為了審閱metaX自研聚合跨鏈項目基於Solidity語言編寫的swap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。