MetaX Invest

合約審計報告

VER 1.0

2022年7月28日

No. 2022072815260

項目總結

1. 項目介紹

MetaX　Invest通過構建一系列的adapter合約來調用defi項目合約，形成一套聚合投資的defi協定，可支持swap、借貸和收益聚合器的合約類型，現時一期接入項目17個。

2. 審計詳情

項目名稱	MetaX Invest	平台	N/A
通證名稱	N/A	通證代號	N/A
開始時間	2022年7月19日	語言	Solidity
結束時間	2022年7月25日	官網	N/A
Github	https://github.com/okex/MetaX-Invest/tree/v1.0.0	白皮書	N/A

3. 審計範圍

ID	文件	SHA-256 checksum
contracts	Entrance.sol	138516f83cc2fa63656586fcd5660709d19c8c569d8ef8b382be29f15fb9734a
contracts	InvestBase.sol	c1196f024057637b8f46a620871b544f7e32b074b0bf9cb4a523dc845b665304
contracts	UnxswapRouter.sol	5121992881793462cc6b4034a06d80bed916d7c6b505a1d96190259b69f4ea20
contracts/libraries	Errors.sol	4a92dc6017475349bdf83f4be0af90aed00d198797357a0f1aa9d14fcebaba13

2022年7月28日

ID	文件	SHA-256 checksum
contracts/libraries	MetaXMath.sol	6aac7405087367e433f9bbdf10c52c127d7e4583670cd346b6a28e5d4f14daac
contracts/libraries	RevertReasonParser.sol	f72cf67651a7e2ed4b063c418dbe671a78a8268131e5ca4f96fb955f05779616
contracts/libraries/Balancer	BalancerMath.sol	10786441c4075aaa4e6c43603fbc71c0ec94d2e43e7a3b5764a93f7617d1a82f
contracts/libraries/Balancer	Math.sol	b4bbc771b556b6c9cfd6d592553ed1d6da189a0c3d40d6f47e60a6986f1434ae
contracts/libraries/Balancer	FixedPoint.sol	7e48632b2447f78de355a1ab0d23e3a873cc3e4b6bf21889a102565fcb5f992e
contracts/libraries/Balancer	LogExpMath.sol	e140f369ced1162735d87cea3e851a3c90194ea2ee3a322cb4637d94ee73d7d3
contracts/adapters	BaseAdapter.sol	aedad5b69e8156169bfd8ff5260f11a1865134b19c14cc3a151702ede9a94bb8
contracts/adapters/Platypus	PlatypusAdapter.sol	55131a2103a8667c723a141e5a88c5a8f6eed36c4d22a54db205576bb2f33618
contracts/adapters/aave	AaveAssetAdapter.sol	85ef990f014c9c019991790276ab03dbcedca50770f776345f85a61f6721f0bb
contracts/adapters/aave	AaveV3AssetAdapter.sol	b8dc05fe12bbea3d2414a995b912803cd9b6877d340278603d44f4fc22c69ce3
contracts/adapters/alpaca	AlpacaAdapter.sol	e71089e36ec872f985c789c12e1ef7771a8c3a2e5c439d3173ec82a3fef18f55
contracts/adapters/balancer	BalancerAdapter.sol	c4a6e0fe3e7bee895e48c62e2d7876b8fc1d2c87dec32a791dee99ec6a8f1c56
contracts/adapters/beefy	BeefyAdapter.sol	f0ca28e137ef620dd12f3a047cb08fe50a3ccc11674b3684db5b441639bc0329
contracts/adapters/bendDAO	BendDAOAdapter.sol	f40d2c835a466c51ee96a765a1567f199819190083424e87b917dd354aabc7b1
contracts/adapters/benqi	BenqiAdapter.sol	9e985640db06e355db5385abaa446fce5caa29d4c22cd3c6c1d1566779076062
contracts/adapters/compound	CompoundAssetAdapter.sol	91a7be9cf5c20f40b8cf5bcd7a1ccd8bc17d8615a13a198b49c975991a5b124b
contracts/adapters/convex	ConvexAdapter.sol	9d423a906a853021c6ef8a4cfbe7c5bed79133f239384088d9f1706496c39556
contracts/adapters/curve	CurveAVAXAdapter.sol	3ee84c725864fcf45d3aaed1a00a866d2e26702755d8a9028d35248c82b3e39b
contracts/adapters/curve	CurveAdapter.sol	316ef6bb2c96fa7aed04c685cdf12f7769a3a8d2c61be57ada83cdbb7422a088
contracts/adapters/curve	CurvePolygonAdapter.sol	7179a6deac2179f1e44411b8ed8a9894ffcdb7c287f50e284bcbd6d2a0538519
contracts/adapters/ellipsis	EllipsisAdapter.sol	b92bd42461b9bb48f4983bb4574638d90cb953c4609ea86bac304a31869ec22f
contracts/adapters/harvest	HarvestAssetAdapter.sol	75b52bd769db5649143e0e327649cefb3d84ccc5b196cf5726a982dc2c4283dc
contracts/adapters/horoma	HoromaAssetAdapter.sol	982c8c32f98cd914c2fe7a86df8ae3993a53ef7633e3a557ddbae90872dd0ef0

2022年7月28日

ID	文件	SHA-256 checksum
contracts/adapters/uniswap	UniswapV2Adapter.sol	7cf553de3a88d48b109290f716e5ab33874f552a311a71d69f0fade88af64285
contracts/adapters/venus	VenusAdapter.sol	a3e9a3359570d3d5e05394b04878917595b2ea74ffb3d166d59b96872a761e6d
contracts/adapters/wepiggy	WepiggyAssetAdapter.sol	d459f9542c54f7f3be69f37b93e5a5319e324ad175bd4d7072244af69deaa3eb
contracts/adapters/yearn	YearnVaultAssetAdapter.sol	bafd9a4c314ac540257110235d891d43164b0723577540050f12bf9e13ad8f7b

4. 代碼結構

```
├── Entrance.sol                          #入口合約
├── InvestBase.sol                        #投資基類
├── UnxswapRouter.sol                     #聚合交易路由
├── adapters                              #17個項目轉接器
|   ├── BaseAdapter.sol
|   ├── BaseFlashAdapter.sol
|   ├── Platypus
|   |   └── PlatypusAdapter.sol
|   ├── aave
|   |   ├── AaveAssetAdapter.sol
|   |   └── AaveV3AssetAdapter.sol
|   ├── alpaca
|   |   └── AlpacaAdapter.sol
|   ├── balancer
|   |   └── BalancerAdapter.sol
|   ├── beefy
|   |   └── BeefyAdapter.sol
|   ├── bendDAO
|   |   └── BendDAOAdapter.sol
```

```
|   ├── benqi
|   |   └── BenqiAdapter.sol
|   ├── compound
|   |   └── CompoundAssetAdapter.sol
|   ├── convex
|   |   └── ConvexAdapter.sol
|   ├── curve
|   |   ├── CurveAVAXAdapter.sol
|   |   ├── CurveAdapter.sol
|   |   └── CurvePolygonAdapter.sol
|   ├── ellipsis
|   |   └── EllipsisAdapter.sol
|   ├── flashloan
|   |   └── FBalancer.sol
|   ├── harvest
|   |   └── HarvestAssetAdapter.sol
|   ├── horoma
|   |   └── HoromaAssetAdapter.sol
|   ├── uniswap
|   |   └── UniswapV2Adapter.sol
|   ├── venus
|   |   └── VenusAdapter.sol
|   ├── wepiggy
|   |   └── WepiggyAssetAdapter.sol
|   └── yearn
|       └── YearnVaultAssetAdapter.sol
├── interfaces                                  #介面
|   ├── IAaveInterface.sol
|   ├── IAaveV3.sol
|   ├── IAdapter.sol
|   ├── IAlpacaInterface.sol
|   ├── IApproveProxy.sol
|   ├── IAsset.sol
|   ├── IBalancerInterface.sol
|   ├── IBancorInterface.sol
|   ├── IBeefyVault.sol
|   ├── IBendDAO.sol
|   ├── IBenqi.sol
```

2022年7月28日

```
|   ├── ICompoundToken.sol
|   ├── IConvexPool.sol
|   ├── ICurveAllInterface.sol
|   ├── ICurvePool.sol
|   ├── IDaiLikePermit.sol
|   ├── IERC20.sol
|   ├── IERC20Permit.sol
|   ├── IEllipsis.sol
|   ├── IEntrance.sol
|   ├── IFlashAdapter.sol
|   ├── IFluxFinanceToken.sol
|   ├── IHarvestInterface.sol
|   ├── IHomoraToken.sol
|   ├── IJoeRouter.sol
|   ├── IMasterChefV2.sol
|   ├── IMasterPlatypusV2.sol
|   ├── IMooniswap.sol
|   ├── IPlatyPool.sol
|   ├── IPlatypusRouter01.sol
|   ├── IPool.sol
|   ├── IQuerry.sol
|   ├── IUniswapV2Pair.sol
|   ├── IUniswapV2Router02.sol
|   ├── IVenusToken.sol
|   ├── IWETH.sol
|   ├── IWepiggyToken.sol
|   └── IYearnVaultToken.sol
├── libraries                                   #庫
|   ├── Balancer
|   |   ├── BalancerMath.sol
|   |   ├── FixedPoint.sol
|   |   ├── LogExpMath.sol
|   |   └── Math.sol
|   ├── Errors.sol
|   ├── MetaXMath.sol
|   └── RevertReasonParser.sol
```

2022年7月28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

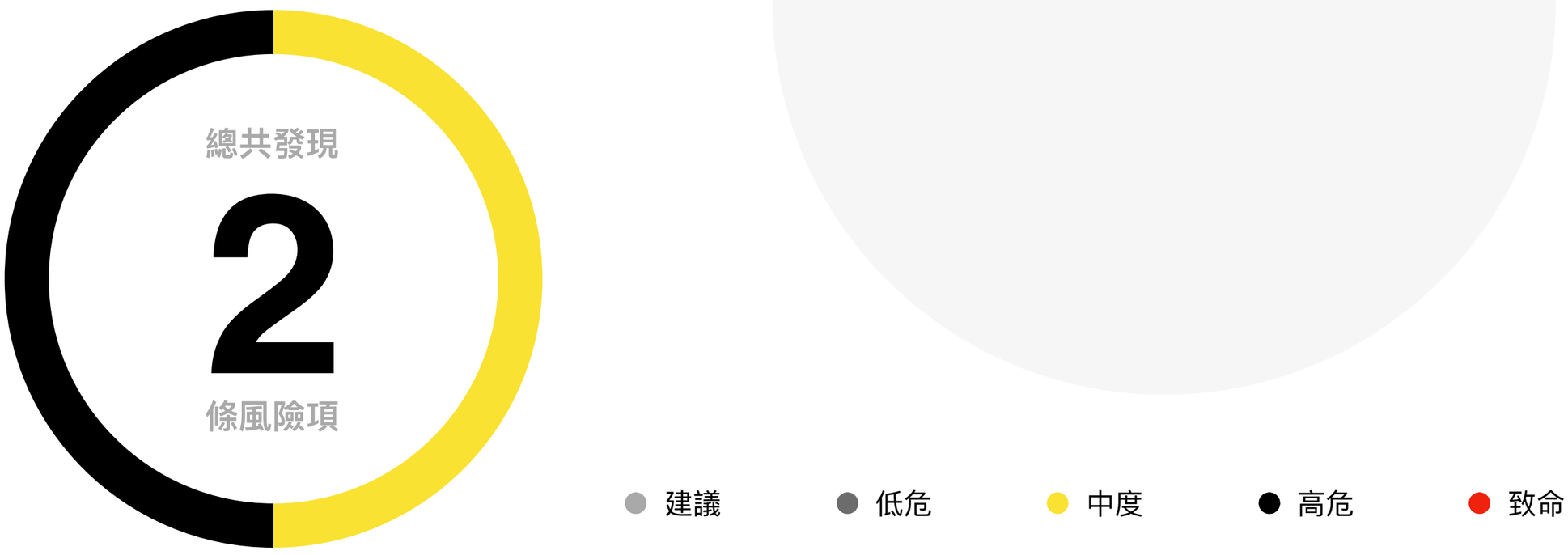
步驟	操作	詳細內容
1	背景研究	閱讀項目介紹、白皮書、合約源碼等項目方團隊提供的相關信息，確保正確理解項目功能
2	自動化檢測	主要用自動化工具掃描源碼，找到常見的潛在漏洞
3	人工審閱	工程師逐行閱讀代碼，找到潛在漏洞
4	邏輯校對	工程師將對代碼的理解和項目方提供的信息比較，檢查代碼實現是否符合項目白皮書信息
5	測試用例檢測	包括測試用例設計，測試範圍分析、符號執行等
6	優化審查	根據應用場景、調用方式及最新的研究成果從可維護性、安全性及可操作性等方面審查項目

2022年7月28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7月28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	內寘函數使用不當	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	中	已告知
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	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	邏輯不當	高	已修改
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。

2022年7月28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. Event不規範

位置	文件	風險状态	風險級別
Line 36~45	BaseAdapter.sol	⚠️已告知	中風險

① 風險描述

event是鏈上數據溯源和服務端監聽合約交易的重要機制，event處理不規範，或參數不正確，有可能會對產品資料產生極大的影響，從而導致項目失敗。
本項目的event，僅記錄了代幣地址和數量，而未對產生交易的雙方做記錄，即用戶地址和項目合約地址的日誌記錄。
當然記錄event參數會導致消耗更多的gas，所以在業務和效能的取捨上，項目方應當有恰當的考慮。

② 修改建議

建議event本著一事一地原則，記錄真實匹配合約交易結果的數據。

③ 關聯程式碼

```
/**
 *
    //@OKLink Audit Description: event记录信息较少
    //@OKLink Audit Solution: 添加deposit池标记，以区分操作日志
    event Deposit(address shareToken, uint256 amount);


    /// @dev burnToken & burnAmount
    event Withdraw(address shareToken, uint256 amount);


    /// @dev stakeToken & stakeAmount
    event Stake(address stakedToken, uint256 amount);


    /// @dev unStakeToken & unStakeAmount
    event UnStake(address unStakedToken, uint256 amount);
}
```

2022年7月28日

2. 邏輯不當

位置	文件	風險状态	風險級別
Line 170~174	ConvexAdapter.sol	已修改	高風險

① 風險描述

程式碼的基本邏輯由於粗心或未驗算而導致漏洞的情況，有可能會因為bug，讓用戶的資產受損或合約無法工作。
本項目的ConvexAdapter合約在迴圈邏輯上有錯誤，會導致數組越界，從而無分發有效執行正確的程式邏輯，在rewardPool == CVXRewarder的分支條件下出現revert。

② 修改建議

建議迴圈寫在條件分支內，注意檢查其他邏輯是否正確。

③ 項目方迴響

已修改

2022年7月28日

③ 關聯程式碼

```
/**
function claimableReward(
    address rewardPool,
    address user,
    bytes calldata
) external view override returns (TokenAmount[] memory tokenAmounts){

    uint256 amount = IConvexRewarder(rewardPool).earned(user);

    uint256 extraLength = IConvexRewarder(rewardPool).extraRewardsLength();

    if (rewardPool == CVXRewarder) { // Do Not have CVX reward
        tokenAmounts = new TokenAmount[](1+extraLength);
        tokenAmounts[0].token = cvxCRV;
        tokenAmounts[0].amount = amount;
    } else {
        tokenAmounts = new TokenAmount[](2+extraLength);
        tokenAmounts[0].token = CRV;
        tokenAmounts[0].amount = amount;
        tokenAmounts[1].token = CVX;
        tokenAmounts[1].amount = _cvxAmount(amount);
    }

    for (uint256 i; i < extraLength; i++) {
        IConvexRewarder _rewards =
IConvexRewarder(IConvexRewarder(rewardPool).extraRewards(i));
```

//@OKLink Audit Description: 这里如果上面是走 *rewardPool == CVXRewarder,*
1+extraLength 的分支,会导致越界。

//@OKLink Audit Solution: 分之内进行循环操作

```
        tokenAmounts[i+2].token = _rewards.rewardToken();
        tokenAmounts[i+2].amount = _rewards.earned(user);
    }

}
```

2022年7月28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7月28日

審計通過.

日期 2022年7月28日

審計 歐科雲鏈

本次稽核的目的是為了審閱MetaX Invest聚合投資協定部署在支持EVM的鏈上的投資合適配器合約，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。