MetaX-Bridge Aggregator

Contract Audit Report

VER 1.0

April 13, 2022

No. 20220413XXXX1

Project Summary

1. Project Introduction

MetaX-Bridge Aggregator is mainly to make a cross-chain swap product, which includes the bridge module to aggregate the third-party bridge. By providing API interfaces, the admin zone selects the optimal path and corresponding third-party contract to provide cross-chain services.

2. Audit Summary

Project Name	MetaX-Bridge Aggregator	Platform	N/A
Token	N/A	Token symbol	N/A
Start date	N/A	Language	Solidity
End date	Apr 13, 2022	Website	N/A
Github	https://github.com/okex/MetaX-Bridge-Core/tree/789eccd58131809bfcacd6a59331353544a69365	whitepaper	N/A

3. Audit Scope

ID	File	SHA-256 checksum
contracts	BridgeAdaptorBase.sol	8779852c28dc3d1c8c4f1520204bba3c9ef993147ceb183133b322308abe7fb7
contracts	XFacade.sol	0019075abf5cf261c4424709a673d8d05ce7ef7586def58d55c1060f7d7a1674
interfaces	IAnyswapV4Router.sol	e1d6950b0b353a451d2dc6ae1799af968cd1922ead1143b2cee229a76b5f6291
interfaces	IAnyswapV5ERC20.sol	f5ce5c7802726fcfd4e6c697c5b06cd253e36d57d61293dfaef87c6fcaf94164
interfaces	IAnyswapV6Router.sol	9dceff4c6829cfb7c8f7b4ae6a850c57b6c70ee86d77abc16f0d89732ad447aa
interfaces	ICBridge.sol	1759d9d03fd5a451e471719d515c5c831ae2392717c7a2feb00246ccd993c5c9
interfaces	IWETH.sol	ef82b0cca564715eb9a78d99371af7b4b9e196c9e4a18a187348fae9a21c01b1
helpers	Constants.sol	c0f90da34ba19b0909a7123dd3ad8a7348ce43342e376ff029a3d9dc85e98057
helpers	Errors.sol	b18908f0a9764b4aa08df61339e0faae3aefd565bf66f45604c66509b2437dd5
adaptor	AnyswapAdaptor.sol	00c2b5832fec0b5b463eda924cf0da1bd81664c33593ff3fe1ab32e0e3383489
adaptor	CBridgeAdaptor.sol	b0789a27c80c02a760ecf2d0d8a467e961d0722e1224a791f77bbd5023ef8d6a

4. Code Structure

```
contracts
 ├──── BridgeAdaptorBase.sol
 ├──── XFacade.sol
 ├──── adaptor
 |     ├──── AnyswapAdaptor.sol
 |     ├──── CBridgeAdaptor.sol
 ├──── helpers
 |     ├──── Constants.sol
 |     └──── Errors.sol
 └──── interfaces
       ├──── IAnyswapV4Router.sol
       ├──── IAnyswapV5ERC20.sol
       ├──── IAnyswapV6Router.sol
       ├──── ICBridge.sol
       └──── IWETH.sol
```

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review	**Key Components**	**-**

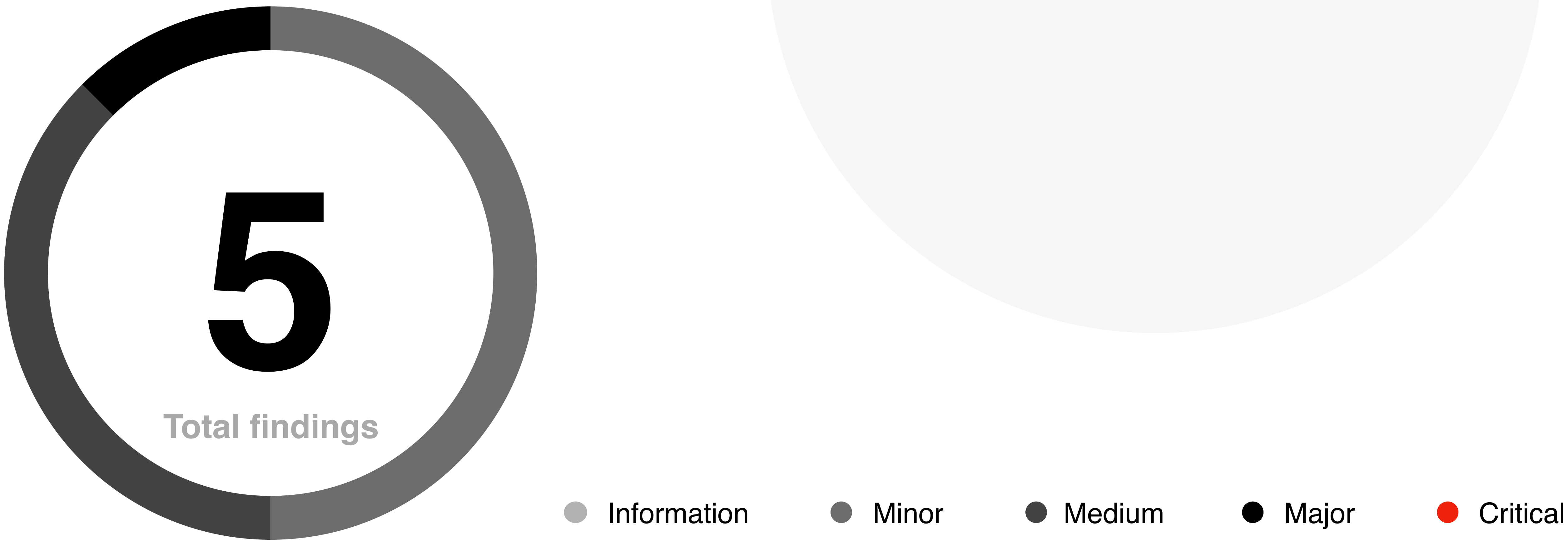
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	None	
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	Minor	INFMD
24	Risk of liquidity drain	None	
25	Centralization Risk	Medium	INFMD
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	None	
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Has collision	None	

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	Centralization Risk	**Risk level**	**Medium**
Location	L52~58	Contract file	XFacade.sol
Description	Contract functions involving permission control do not have timelock mechanism or multi sign mechanism		
Recommedation	Disperse the permissions of a single private key, and use timelock and multi sign mechanism		
Update			

Risk type	Centralization Risk	**Risk level**	**Medium**
Location	L63	Contract file	XFacade.sol
Description	Contract functions involving permission control do not have timelock mechanism or multi sign mechanism		
Recommedation	The way of calling the contract for the project is to pass the packaging parameters to the front-end and then call the contract abi. The risks of server intrusion, intermediate one attack, fishing and so on need to be considered		
Update			

Risk type	Irregularity of condition judgment	**Risk level**	**Minor**
Location	L17	Contract file	AnyswapAdaptor.sol
Description	The non-zero judgment of the transmission entry address is not considered		
Recommedation	Launch the non-zero judgment with transmission entry address to prevent contract invalidation due to address setting error		
Update			

Risk type	Irregularity of condition judgment	**Risk level**	**Minor**
Location	L16	Contract file	CBridgeAdaptor.sol
Description	The non-zero judgment of the transmission entry address is not considered		
Recommedation	Launch the non-zero judgment with transmission entry address to prevent contract invalidation due to address setting error		
Update			

Risk type	Third-party dependency risk	**Risk level**	**Minor**
Location	All	Contract file	XFacade.sol
Description	It is highly dependent on the safety of the third-party cross-chain bridge		
Recommedation	Monitor the safety risk of the third-party bridge in real time and suspend the contract function in time		
Update			

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

Disclaimer

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.

Passed.

Date	April 13, 2022
Audit Team	歐科雲鏈

This audit aimed to review the aggregation cross-chain function written by MetaX-Bridge Aggregator based on the solid language, examine its design architecture, identify potential security risks, and attempt to find possible vulnerabilities.