OKC-USDT

Audit Report

VER 1.0

27 May 2022

No. 20220527105111

Project Summary

1. Project Introduction

Based on the background that the official USDT was issued on OKC, the preparation and deployment of contracts based on KIP20 standard came into being. Delegate-proxy which is compiled based on EIP897 standard, an upgradeable proxy contract framework, was adopted to build the project. Furthermore, in terms of token function implementation, not only the basic functions under KIP20 standard, but also the freezing and management functions were developed and implemented.

2. Audit Summary

Project Name	OKC-USDT	**Platform**	N/A
Token	USDT	**Token symbol**	USDT
Start date	26 May 2022	**Language**	Solidity
End date	27 May 2022	**Website**	N/A
Github	N/A	**Whitepaper**	N/A

3. Audit Scope

ID	ADDRESS	File	SHA-256 checksum
1	0x382bb369d343125bfb2117af9c149795c6c65c50	Proxy.sol	283dd4cc66bd5a554e504822b0c28fa9462d1491b34d9220fdefc40afcea26b8
2	0x382bb369d343125bfb2117af9c149795c6c65c50	Address.sol	1766ef0b83305645016ab40e1c262d5db1e6a9cd51f1b89d295e3e1ec6b3240c
3	0x382bb369d343125bfb2117af9c149795c6c65c50	UpgradeabilityProxy.sol	362996d399a418801a3f643016d994d7bc5386a8d361e837328a240ee75804cf
4	0x382bb369d343125bfb2117af9c149795c6c65c50	OwnedUpgradeabilityProxy.sol	ed67759d7b707b61f4ab9497aa0ed8f8e41c03e055667c1b2067f73b5ceebfd2
5	0xc49cc300e4420767f4c2103d89d80fff327e7238	SafeMath.sol	93c99439f77ffea008a4da3520ec01e286a30b371e8bdbe9349c391af74a90a2
6	0xc49cc300e4420767f4c2103d89d80fff327e7238	USDTimpl.sol	9371e72541cc81460a895c1e94da2a7c1d1a8d36fbea74c643969b74252f2675

4. Code Source

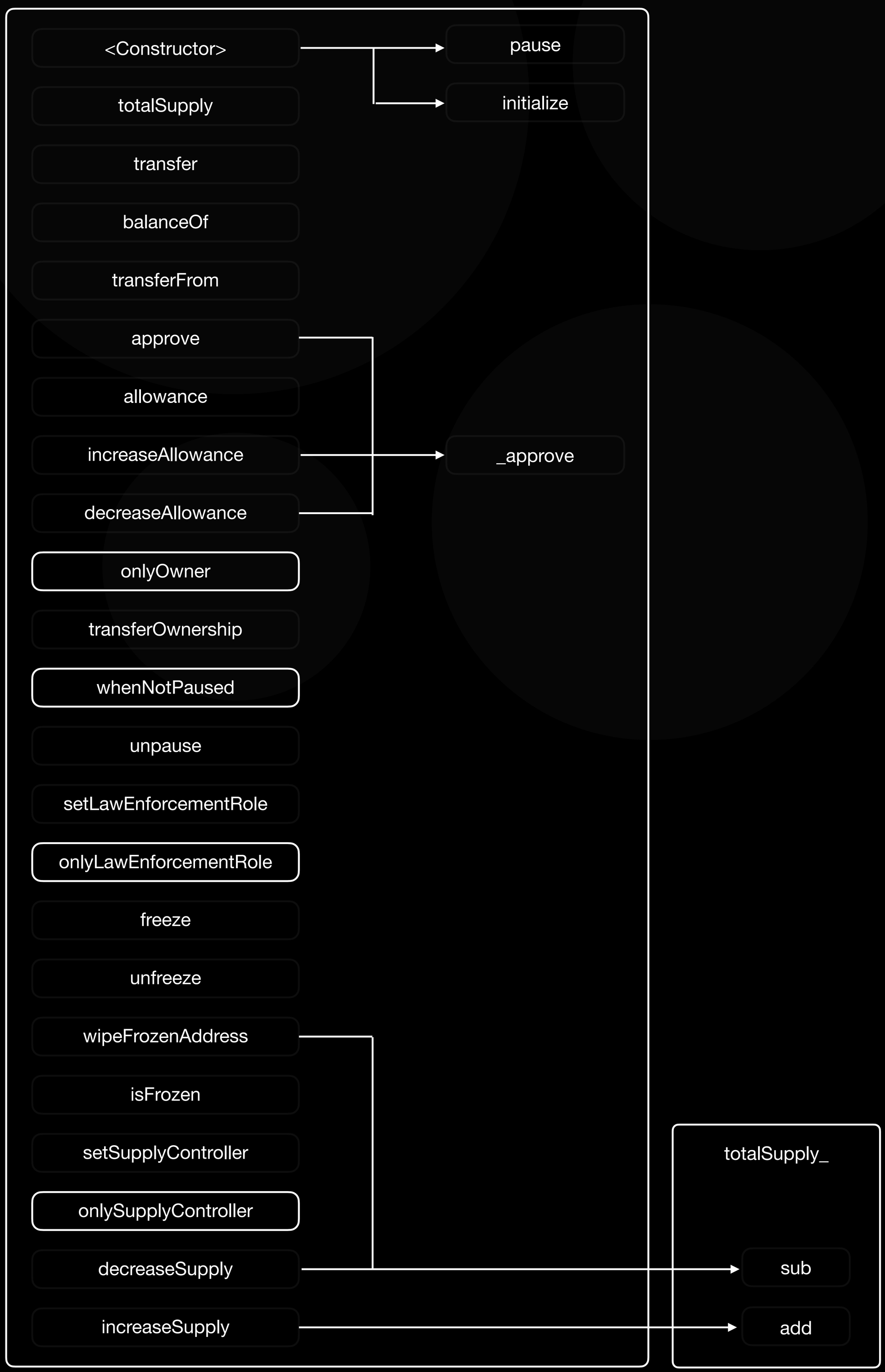
ID	Link
1	https://www.oklink.com/zh-cn/okc/address/0x382bb369d343125bfb2117af9c149795c6c65c50
2	https://www.oklink.com/zh-cn/okc/address/0xc49cc300e4420767f4c2103d89d80fff327e7238

5. Storage Order Of State Variables

ID	Name	Type	Slot	Offset
1	USDTImplementation.initialized	bool	0	0
2	USDTImplementation.balances	mapping(address => uint256)	1	0
3	USDTImplementation.totalSupply_	uint256	2	0
4	USDTImplementation._allowed	mapping(address => mapping(address => uint256))	3	0
5	USDTImplementation.owner	address	4	0
6	USDTImplementation.paused	bool	4	20
7	USDTImplementation.lawEnforcementRole	address	5	0
8	USDTImplementation.frozen	mapping(address => bool)	6	0
9	USDTImplementation.supplyController	address	7	0

May 27 2022

6. Interpretation Of Calling Contracts



Audit Report Summary

1. Audit Methods

By clearly understanding the design purpose, operation principle and implementation mode of the project, the audit team conducted in-depth research and analysis of the contract code. Based on clarifying the calling relationship between each contract and its functions, the possible loopholes in the contract are located and analyzed. Finally, a document containing the problem descriptions and corresponding modification suggestions is formed.

Audit methods	Static analysis, Manual Review

2. Audit Process

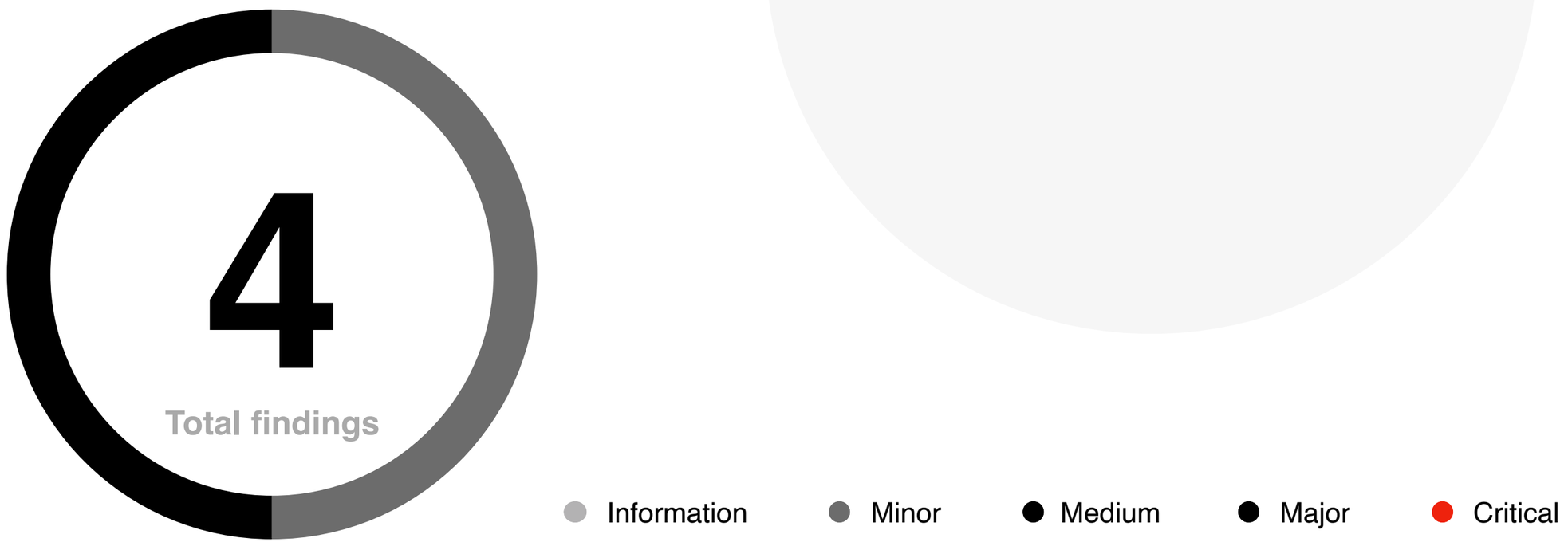
Steps	Operation	Description
1	Background	Reading the descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Automated detection tools will be mainly used to scan the source code to find common potential vulnerabilities
3	Manual reveiw	The code will be thoroughly reviewed line by line by engineers 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 white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review the project from the aspects of maintainability, security and operability according to the application scenarios, call methods and the latest research results

27 May 2022

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	Medium	**Acknowledged**
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	

27 May 2022

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	None	
24	Risk of liquidity drain	None	
25	Centralization Risk	Medium	**Acknowledged**
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	Hash collision	None	
36	Decimal conflicts	Information	**Acknowledged**
37	Proxy Irregularity	Information	**Acknowledged**

* In the above table, if the status column is **Acknowledged**, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is **Resolved**, the project owner has changed the exposure, and the audit team has confirmed the changes.

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	MEV Possibility	**Risk level**	**Medium**
Location	Line 325	Contract file	USDTimpl.sol
Description	MEV attack will happen，if attacker monitor mempool and transfer assets to other address before freeze executed		
Recommedation	Call freeze method by privacy transaction or track transfer path in states to freeze related addresses one time		
Update			

Risk type	Centralization Risk	**Risk level**	**Medium**
Location	Line 260	Contract file	USDTimpl.sol
Description	The owner address in this contract is an account address, which may cause the risk of pk lost or centralized authority Owner value in implement contract on OKC： 0x0f94450293b32c7812e758dbc86d0a4636589ba3address Owner value in proxy contract on OKC： 0x4a164ca582d169f7caad471250991dd861dda981address		
Recommedation	Update owner to multi-sig contract or timelock contract address		
Update			

Risk type	Decimal conflicts	**Risk level**	**Information**
Location	Line 40	Contract file	USDTimpl.sol
Description	The decimal of USDT on Eth and Tron is 6, but here is 18, which may cause unnecessary decimal conflicts		
Recommedation	Update decimal to 6		
Update			

Risk type	Proxy Irregularity	**Risk level**	**Information**
Location	Line 71	Contract file	OwnedUpgradeabilityProxy.sol
Description	Lack of version control mechanism for upgradeable contract		
Recommedation	Use version control mechanism		
Update			

27 May 2022

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.

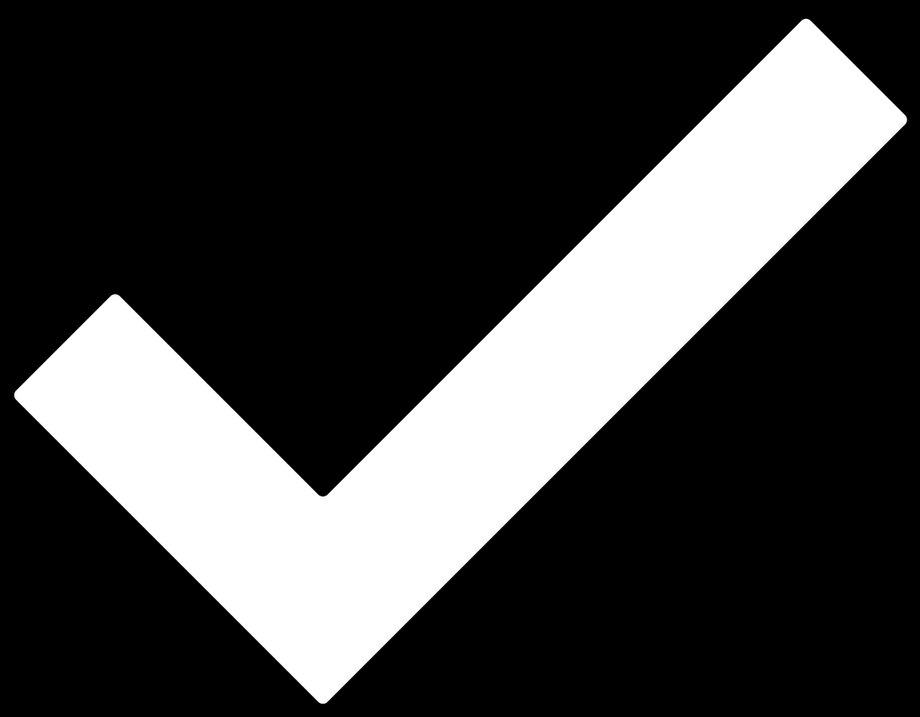
27 May 2022

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.

27 May 2022



Passed.

Date	27 May 2022
Audit Team	歐科雲鏈

Based on the background that the official USDT contract was introduced by OKC, the purpose of this audit is to review the Erc20 contract. The design and architecture will be studied to find potential security risks and try to find possible vulnerabilities.