ZAC Stablecoin Contract Audit Report

Version 1.0.0

2021.12.14

No. 202112141353

Summary of project information

1. Project introduction

OneCash Stablecoin Factory has industry-leading product technical capabilities and top-level compliance operation capabilities, providing users with safe, compliant

A series of stable currency products that are regulated and efficient. ZAC is a Hong Kong dollar stablecoin issued by OneCash. Through exchange with Hong Kong dollar fixed exchange rate

The exchange system achieves price stability and is audited by a well-known accounting firm to ensure a certain amount of legal currency reserves.

2. Audit Information

Project NameOneCash		**platform**	N/A
Token **name** ZAC		Token **code** ZAC	
Start time December 13, 2021		**language**	Solidity
End time December 14, 2021		**Official website**	https://onecash.asia/
Github	N/A	**white paper**	Whitepaper
Commit	N/A		

3. Scope of the audit

directory	**Case**	**SHA-256 hash value**
contracts ZAC.sol ÿÿ	82725455da15c2eb0351	acac4fd436268d80831c3c505d4707b97ac6a1728b49

4. Audit Purpose

The purpose of this audit is to review the ERC20 protocol written by the ZAC project based on the Solidity language and find potential security risks.

Study its design, architecture, and try to find possible vulnerabilities.

5. Main functions of the contract

1) Issuance of governance token ZAC

• Token issuance cap

• Minting and burning permissions

2) Pause function of token contract

• Administrators can suspend the use of token contracts, including transfer, authorization and other functions

3) Blacklist function of token contract

• Administrators can add specified addresses to the blacklist and destroy their account balances

• Administrators can remove specified addresses from the blacklist

6. Code Structure

N/A

Audit report summary

1. Audit method

The purpose of this audit is to clearly understand how the project is implemented and how it works. The audit team conducted in-depth research on the project code researched, analyzed and tested, and collected detailed data. The audit team will detail each issue, issue found in this report

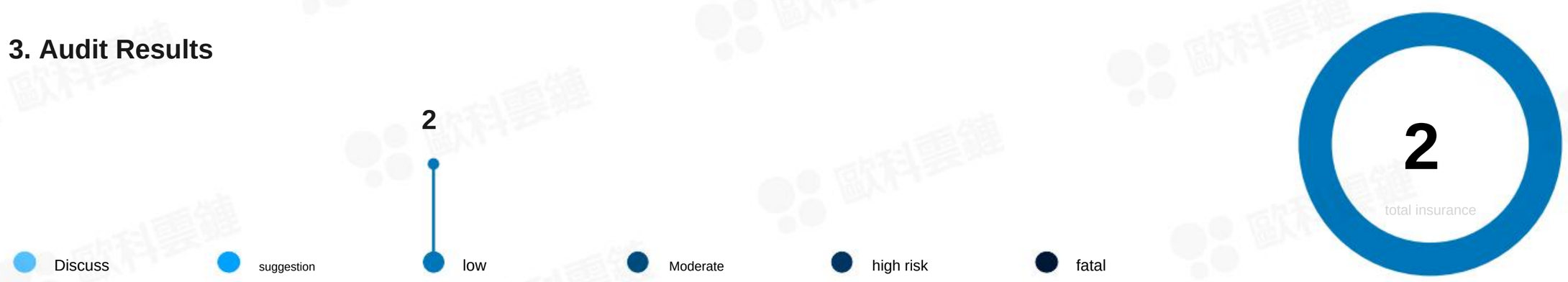
The location, the source of the problem, the description of the problem, and the corresponding modification suggestions for the problem.

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

2. Audit Process

step operation	details
1 Background research	Read the relevant information provided by the project team, such as the project introduction, white paper, contract source code, etc., to ensure a correct understanding of the project functions
2 Automated detection	Mainly use automated tools to scan source code to find regular potential vulnerabilities
3 Manual review	The engineer reads the code line by line to find potential vulnerabilities
4 Logical proofreading	The engineer will compare the understanding of the code with the information provided by the project party, and check whether the code implementation conforms to the information in the project white paper
5Test case detection includes test case design, test scope analysis, symbolic execution, etc.	
6 Optimization Review	Review the project from the aspects of maintainability, security and operability based on application scenarios, calling methods and the latest research results

3. Audit Results



Serial Number	Audit Item	Types of	Risk level	condition
1	token issuance	Admin rights hidden dangers	low risk	Project has been notified
2	Token Balance Check	Admin rights hidden dangers	low risk	Project has been notified

4. Risk classification

Risk Level	Risk Description
fatal	There are fatal dangers and hidden dangers that need to be resolved immediately
high risk	There are high risks and hidden dangers, which will cause related problems and must be resolved
Moderate	There are moderate risks and hidden dangers, which may lead to potential risks and still need to be resolved in the end
low	There are low risks and hidden dangers, mainly referring to various details that are improperly handled or cause warning messages, and such issues can be put on hold for the time being
suggestion	There are parts that can be optimized, such problems can be shelved, but it is recommended to solve them eventually
Discuss	There are detailed issues that can be discussed with the project party, and such issues are not insurance items

5. Insurance items and modification plan

The following sections are the details of the insurance items obtained after the audit, including the insurance type, insurance level, problem location,

Problem description, modification suggestions and project party feedback.

Type of insurance	**Admin rights hidden dangers**	**Risk level**	**low risk**
Location	**Line 223**	**contract document**	**zac.sol**
Problem Description	The owner permission address in the token contract can set a blacklist address and destroy the token balance held by the address		
Proposed changes	Hand over the token contract owner to community governance or use multi-signature wallet management		
The **project** party has reported that the project party has learned that this part is a function required by stablecoins, and the project party has an internal control mechanism to control the use rights.			

Type of insurance	**Admin rights hidden dangers**	**Risk level**	**low risk**
Location	**Line 372**	**contract document**	**zac.sol**
Problem Description	The owner permission address in the token contract can call the issue function to issue its tokens infinitely		
Proposed changes	Hand over the token contract owner to community governance or use multi-signature wallet management		
The **project** party has reported that the project party has learned that this part is a function required by stablecoins, and the project party has an internal control mechanism to control the use rights.			

6. Enhancement suggestions

N/A

Disclaimer

i. This audit report only audits the audit types specified in the final report. Other unknown security vulnerabilities are not within the scope of this audit responsibility, and we do not need to
Take responsibility for this.

ii. We shall only issue audit reports based on attacks or vulnerabilities that existed or occurred prior to the release of the audit report. We have no responsibility for new attacks or vulnerabilities that exist or occur in the future
and shall not be responsible for any legal determination of the possible impact on the security state of its projects.

iii. The security audit analysis and other content in the audit report issued by us shall be based solely on the documents and materials provided to us by the project party prior to the issuance of the audit report (including
But not limited to contract code), and the above documents and materials should not be lack of information, tampered with, deleted or hidden, if the documents provided by the project party
and data are untrue, inaccurate, lack of information, tampered with, deleted or hidden, or changes to the above-mentioned documents and data are in the release of audit reports
After that, we will not be liable for any losses and adverse effects caused by the inconsistency between the reflected situation and the actual situation.

iv. The project party knows that the audit report issued by us is based on the documents and materials provided by the project party and relies on the technology we currently have. However, since any institution is
Due to technical limitations, the audit report made by us still may not be able to completely detect all the risks. Our audit team encourages the development team of the project
and any relevant stakeholders to conduct subsequent testing and auditing of the project.

v. The project party warrants that the project for which it entrusts us to provide auditing or testing services is legal, compliant, and does not violate applicable laws. The audit report is only for the reference of the project party, audit
The content of the report, how to obtain it, how to use it, and any services or resources involved in it are not intended to be used as any form of investment, tax, legal, regulatory or advice, etc.
basis, we shall not be liable for it. Without our written consent, the project party shall not submit the whole or part of the audit report in any form.
and, reference, display or send to any third party, otherwise any loss and liability arising therefrom shall be borne by the project party itself. We rely on audit reports for anyone
or use it for any purpose.

vi. This audit report does not involve contract compilers and any areas beyond the programming language of smart contracts. The audited smart contracts are caused by referencing off-chain information or resources.
The risk and responsibility of the project shall be borne by the project party.

vii. Force Majeure. Force majeure refers to events that cannot be foreseen, unavoidable and insurmountable for the occurrence and consequences of both parties at the time of entering into the contract, including but not limited to war.
natural disasters such as disputes, Taiwan disasters, floods, fires, earthquakes, tides, lightning, natural disasters, strikes, nuclear explosions, epidemics, and changes in laws, regulations and policies, and government
Other unforeseen events such as acts, the occurrence and consequences of which cannot be prevented or avoided, and which prevent, affect or delay any party's performance of its full performance under the contract
part or part of the obligation.

viii. If one party believes that force majeure affects the performance of the obligations of this agreement, it shall promptly notify the other party. According to the extent of the impact of the event on the performance of the contract, the two parties shall negotiate to decide whether to
Whether to terminate the contract or partially exempt from the responsibility for performance, or delay performance.

ix. When force majeure occurs, neither party can be regarded as a breach of contract or non-performance of the obligations of this agreement. Financial responsibilities that existed prior to the event should not be affected,
The Project Party shall pay us for the work we have completed.