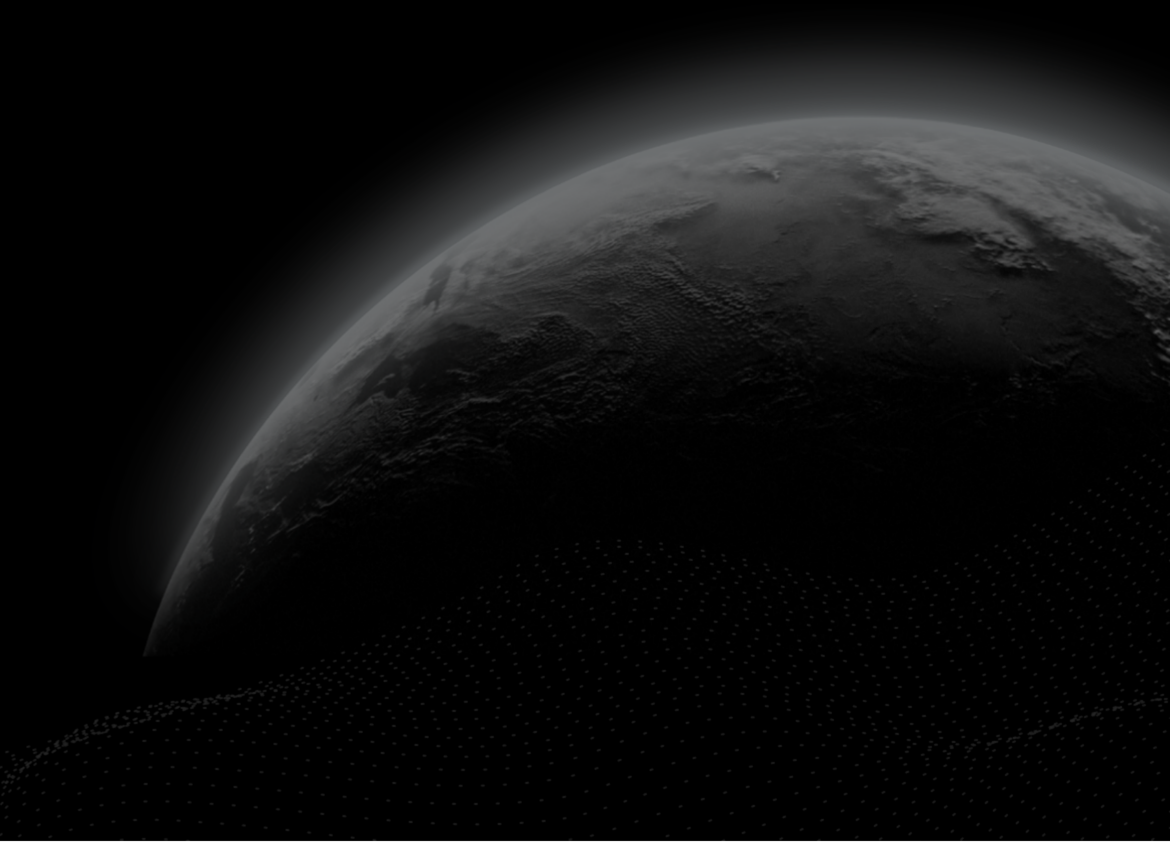
Security Assessment

Ailey

CertiK Assessed on Sept 19th, 2023



CertiK Assessed on Sept 19th, 2023

Ailey

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
BEP-20	Binance Smart Chain (BSC)	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 09/19/2023	N/A

CODEBASE

mainnet

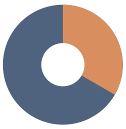
View All in Codebase Page

COMMITS

0x9dce13e71b11eb5df66ca269bd657696587fd4e2

View All in Codebase Page

Vulnerability Summary



3	0	0	0	3	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

🟥	0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
🟧	1	Major	1 Acknowledged	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟨	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	0	Minor		Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
🟦	2	Informational	2 Acknowledged	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | AILEY

CODEBASE | AILEY

Repository

mainnet

Commit

0x9dce13e71b11eb5df66ca269bd657696587fd4e2

AUDIT SCOPE | AILEY

1 file audited ● 1 file with Acknowledged findings

ID	File	SHA256 Checksum
● AIL	Ailey.sol	a6e61d12ad513d94637ded005454d26cfccc75d0c8d1119956d8133ffbf6de04

APPROACH & METHODS | AILEY

This report has been prepared for Ailey to discover issues and vulnerabilities in the source code of the Ailey project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

REVIEW NOTES | AILEY

Overview

The `Ailey` is a standard ERC20 token project. The focus of this audit is the token contract.

External Dependencies

The following are external contracts referred to in the contracts. The contract mainly uses OpenZeppelin contracts and libraries for the templates and setup of contracts:

- `Counters` , `IERC5267` , `StorageSlot` , `ShortStrings` , `SignedMath` , `Math` , `Strings` , `ECDSA` , `EIP712` , `IERC20Permit` , `Context` , `IERC20` , `IERC20Metadata` , `ERC20` & `ERC20Permit` .

Since the OpenZeppelin contracts are actively developed, we recommend the team continuously monitor the library change to avoid unexpected failure.

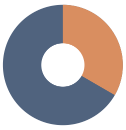
On-chain analysis

The contract `Ailey` is deployed at BSC 0x9dce13e71b11eb5df66ca269bd657696587fd4e2 by the EOA account 0x653f5c544b0053f32d04407c1ceec5789c8a9e12.

As the time of 09/14/2023, all the `Ailey` tokens have been transferred to the following accounts by the initial token holder 0x653f5c544b0053f32d04407c1ceec5789c8a9e12.

- 0x3726B181FF6aeC590932044410ff4A07Ab232073 - 400,000,000 EOA
- 0x4933f82e6cd2b6aee34f25e330b49F7609E50236 - 155,000,000 TokenVesting contract
- 0xbc9dC203abe6E93F1392FFc0A1c23cB1a4934a32 - 132,500,000 TokenVesting contract
- 0x5adfa7257dC7E445B3fA1e0B4b37317C25F448a1 - 100,000,000 TokenVesting contract
- 0x7c4f6Fc652c95aB24024d4Cbd321d6260BF2eFB9 - 70,000,000 TokenVesting contract
- 0x87deE7E40eE255440b3cC98E97f56F182f947930 - 50,000,000 EOA
- 0xB38c3FAe7410AD98fcFAbca5b2e2F5f7f386E2D2 - 33,750,000 TokenVesting contract
- 0xB9fB1ede5abF2b399523CF75F62eF3047002eFF1 - 20,000,000 TokenVesting contract
- 0x7f5f695034E230E3D671576448089f59188A2aEC - 18,750,000 EOA
- 0xF5D14976190B974457e33D402D35154D2ecC05e7 - 10,000,000 EOA
- 0xA73937a719D6E68c2df426cDA420D4C7059d2505 - 10,000,000 EOA

FINDINGS | AILEY



Total Findings	Critical	Major	Medium	Minor	Informational
3	0	1	0	0	2

This report has been prepared to discover issues and vulnerabilities for Ailey. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
AIL-02	**Initial Token Distribution**	**Centralization**	**Major**	● **Acknowledged**
AIL-01	Discussion On `permit()` Function	Design Issue	Informational	● Acknowledged
AIL-03	Solidity Version 0.8.20 May Not Work On Other Chains Due To `PUSH0`	Logical Issue	Informational	● Acknowledged

AIL-02 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization	● **Major**	**Ailey.sol: 1856**	● **Acknowledged**

Description

All of the `Ailey` tokens are sent to the contract deployer or one or several externally-owned account (EOA) addresses. This is a centralization risk because the deployer or the owner(s) of the EOAs can distribute tokens without obtaining the consensus of the community. Any compromise to these addresses may allow a hacker to steal and sell tokens on the market, resulting in severe damage to the project.

On-chain analysis

As the time of 09/14/2023, all the `Ailey` tokens have been transferred to the following accounts by the initial token holder 0x653f5c544b0053f32d04407c1ceec5789c8a9e12.

- 0x3726B181FF6aeC590932044410ff4A07Ab232073 - 400,000,000 EOA
- 0x4933f82e6cd2b6aee34f25e330b49F7609E50236 - 155,000,000 TokenVesting contract
- 0xbc9dC203abe6E93F1392FFc0A1c23cB1a4934a32 - 132,500,000 TokenVesting contract
- 0x5adfa7257dC7E445B3fA1e0B4b37317C25F448a1 - 100,000,000 TokenVesting contract
- 0x7c4f6Fc652c95aB24024d4Cbd321d6260BF2eFB9 - 70,000,000 TokenVesting contract
- 0x87deE7E40eE255440b3cC98E97f56F182f947930 - 50,000,000 EOA
- 0xB38c3FAe7410AD98fcFAbca5b2e2F5f7f386E2D2 - 33,750,000 TokenVesting contract
- 0xB9fB1ede5abF2b399523CF75F62eF3047002eFF1 - 20,000,000 TokenVesting contract
- 0x7f5f695034E230E3D671576448089f59188A2aEC - 18,750,000 EOA
- 0xF5D14976190B974457e33D402D35154D2ecC05e7 - 10,000,000 EOA
- 0xA73937a719D6E68c2df426cDA420D4C7059d2505 - 10,000,000 EOA

Recommendation

It is recommended that the team be transparent regarding the initial token distribution process. The token distribution plan should be published in a public location that the community can access. The team should make efforts to restrict access to the private keys of the deployer account or EOAs. A multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. Additionally, the team can lock up a portion of tokens, release them with a vesting schedule for long-term success, and deanonymize the project team with a third-party KYC provider to create greater accountability.

Alleviation

[Ailey Team, 09/15/2023]: The team acknowledged this issue and decided not to change the codebase this time.

[CertiK, 09/15/2023]: It is suggested to implement the aforementioned methods to increase the transparency and security regarding the initial token distribution process and avoid the centralized failure. Also, it strongly encourages the project team periodically revisit the private key security management of all addresses related to centralized roles.

[Ailey Team, 09/19/2023]: The team shared a link to the token distribution plan: https://project-ailey.gitbook.io/project-ailey/project-ailey/tokenomics/vesting-plan.

They also stated that the tokens in these four EOA accounts will also be used for vesting.

- 0x87deE7E40eE255440b3cC98E97f56F182f947930 - 50,000,000 EOA
- 0x7f5f695034E230E3D671576448089f59188A2aEC - 18,750,000 EOA
- 0xF5D14976190B974457e33D402D35154D2ecC05e7 - 10,000,000 EOA
- 0xA73937a719D6E68c2df426cDA420D4C7059d2505 - 10,000,000 EOA

[CertiK, 09/19/2023]: The measures taken by the team have improved the transparency of the initial token distribution. It is suggested to maintain the transparency in a timely manner and take measures to increase security regarding the initial token distribution process and avoid centralized failure. Also, it strongly encourages the project team periodically revisit the private key security management of all addresses related to centralized roles.

AIL-01 | DISCUSSION ON `permit()` FUNCTION

Category	Severity	Location	Status
Design Issue	● Informational	Ailey.sol: 1810	● Acknowledged

Description

In the contract `ERC20Permit` , the `permit()` function is able to perform the approval. However, it is noted that the structure of `_nonces` is a mapping of addresses to `Counters.Counter` and the `_nonces[owner]` will increase after used successfully, which implies the `owner` has at most one valid signature, even for different `spender` .

Recommendation

We would like to confirm if current implementation matches the intended design.

Alleviation

[Ailey Team, 09/15/2023]: The team acknowledged this issue and decided not to change the codebase this time.

AIL-03 | SOLIDITY VERSION 0.8.20 MAY NOT WORK ON OTHER CHAINS DUE TO `PUSH0`

Category	Severity	Location	Status
Logical Issue	● Informational	Ailey.sol: 1850	● Acknowledged

Description

The compiler for Solidity 0.8.20 switches the default target EVM version to Shanghai, which includes the new `PUSH0` op code. This op code may not yet be implemented on all L2s, so deployment on these chains will fail. To work around this issue, use an earlier EVM version

Recommendation

It's recommended to pay attention to the EVM complier version when using 0.8.20 solidity version in your contract.

Alleviation

[Ailey Team, 09/15/2023]: The team acknowledged this issue and decided not to change the codebase this time.

APPENDIX | AILEY

Finding Categories

Categories	Description
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.