Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: AEXC Token
Platform: Ethereum
Language: Solidity
Date: September 17th, 2022

Table of contents

Email: audit@EtherAuthority.io

`

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Introduction

EtherAuthority was contracted by the AEXC Token team to perform the Security audit of the AEXC Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on September 17th, 2022.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

- AEXC is an ERC20 token contract which has functionalities like the owner can mint, burn anyone's tokens after getting approval from all the 3 admins, the owner can add multiple admins, etc.
- AEXC contract inherits the ERC20, ERC20Burnable, Ownable standard smart contracts from the OpenZeppelin library.
- These OpenZeppelin contracts are considered community-audited and time-tested, and hence are not part of the audit scope.

Audit scope

Name	Code Review and Security Analysis Report for AEXC Token Smart Contract
Platform	**Ethereum / Solidity**
File	AEXC.sol
File MD5 Hash	88C6318724A31EC2D908D9942624B9ED
Updated File MD5 Hash	8803B821CA171C6C8F0098AB9FB468C4
Audit Date	September 17th, 2022
Revised Audit Date	September 20th, 2022

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Maximum Supply: 25 Million	**YES, This is valid.**
Other Specifications ● Open Zeppelin standard code is used. ● Owner can add users to tiers. ● Admin can mint tokens to specific addresses. ● Token holders can burn their own tokens without any burn request.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **"Secured".** Also, these contracts do contain owner control, which does not make them fully decentralized.

We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 1 low and some very low level issues.

All the issues have been resolved / acknowledged in the revised code.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	"Out of Gas" Issue	Passed
	High consumption 'for/while' loop	Passed
	High consumption 'storage' storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

Overall Audit Result: PASSED

Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the AEXC Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the AEXC Token.

The AEXC team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are not well commented on in the smart contracts. Ethereum's NatSpec commenting style is used, which is a good thing.

Documentation

We were given AEXC Token smart contract code in the form of a file. The hash of that code is mentioned above in the table.

As mentioned above, code parts are not well commented but the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are not used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	burn	write	Passed	No Issue
8	burnFrom	write	Passed	No Issue
9	onlyAdmins	modifier	Passed	No Issue
10	mint	write	access only Admins	No Issue
11	createBurnRequest	write	access only Admins	No Issue
12	fulfillBurn	internal	Passed	No Issue
13	fulfillBurnRequest	write	Passed	No Issue
14	authorizedTierUser	internal	Passed	No Issue
15	addAdmin	write	access only Admins	No Issue
16	editTierUser	write	access only Admins	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

No Very Low severity vulnerabilities were found.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- mint: Admin can mint tokens to specific addresses .
- createBurnRequest: Admin can initiate the request to burn the token from any address.
- addAdmin: Owner can add new admin addresses.
- editTierUser: Owner can use this function to add users to tiers.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of a file and we have used all possible tests based on given objects as files. We have observed 1 low severity issue and some Informational issues in the token smart contract. and those issues have been resolved / acknowledged in the revised code. **So, the smart contracts are ready for the mainnet deployment**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

The security state of the reviewed smart contract, based on standard audit procedure scope, is **"Secured".**

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:
In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:
Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

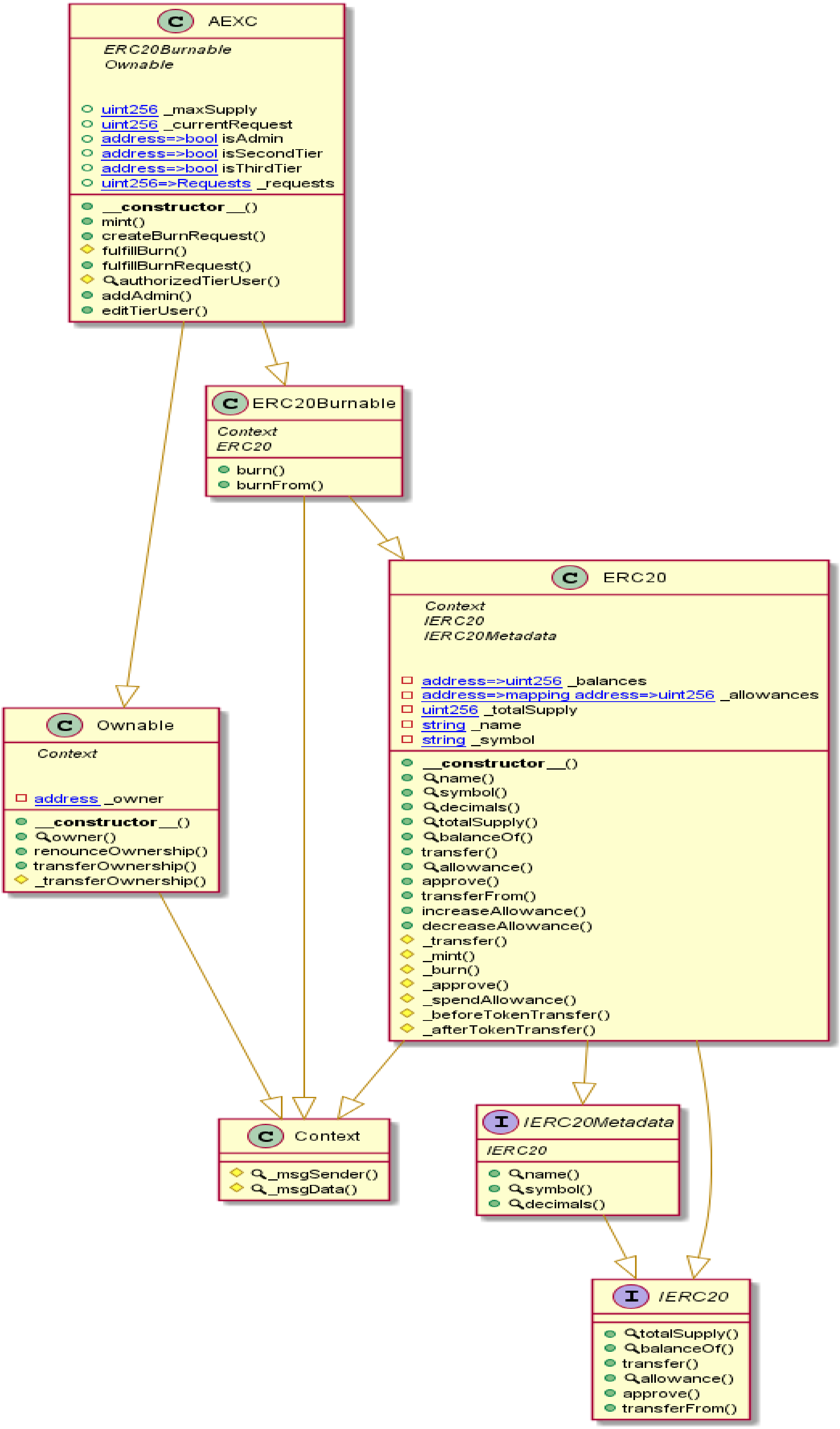
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - AEXC Token



Email: audit@EtherAuthority.io

Slither Results Log

Slither Log >> AEXC.sol

```
INFO:Detectors:
AEXC.constructor(string,string).name (AEXC.sol#575) shadows:
        - ERC20.name() (AEXC.sol#140-142) (function)
        - IERC20Metadata.name() (AEXC.sol#91) (function)
AEXC.constructor(string,string).symbol (AEXC.sol#576) shadows:
        - ERC20.symbol() (AEXC.sol#148-150) (function)
        - IERC20Metadata.symbol() (AEXC.sol#96) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Context._msgData() (AEXC.sol#108-110) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.4 (AEXC.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter AEXC.createBurnRequest(address,uint256)._burnAddress (AEXC.sol#608) is not in mixedCase
Parameter AEXC.createBurnRequest(address,uint256)._burnAmount (AEXC.sol#608) is not in mixedCase
Parameter AEXC.fulfillBurn(address,uint256,uint256)._from (AEXC.sol#623) is not in mixedCase
Parameter AEXC.fulfillBurn(address,uint256,uint256)._burnAmount (AEXC.sol#624) is not in mixedCase
Parameter AEXC.fulfillBurnRequest(uint256,uint256)._tier (AEXC.sol#637) is not in mixedCase
Parameter AEXC.addAdmin(address[],bool)._users (AEXC.sol#671) is not in mixedCase
Parameter AEXC.editTierUser(address[],uint256,bool)._users (AEXC.sol#684) is not in mixedCase
Parameter AEXC.editTierUser(address[],uint256,bool)._tier (AEXC.sol#685) is not in mixedCase
Parameter AEXC.editTierUser(address[],uint256,bool)._status (AEXC.sol#686) is not in mixedCase
Variable AEXC._maxSupply (AEXC.sol#551) is not in mixedCase
Variable AEXC._currentRequest (AEXC.sol#552) is not in mixedCase
Variable AEXC._requests (AEXC.sol#564) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
AEXC.slitherConstructorVariables() (AEXC.sol#550-697) uses literals with too many digits:
        - _maxSupply = 25000000000000000000000000 (AEXC.sol#551)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
AEXC._maxSupply (AEXC.sol#551) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
```

```
INFO:Detectors:
name() should be declared external:
        - ERC20.name() (AEXC.sol#140-142)
symbol() should be declared external:
        - ERC20.symbol() (AEXC.sol#148-150)
decimals() should be declared external:
        - ERC20.decimals() (AEXC.sol#165-167)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (AEXC.sol#179-181)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (AEXC.sol#191-195)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (AEXC.sol#214-218)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (AEXC.sol#236-245)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (AEXC.sol#259-263)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (AEXC.sol#279-288)
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (AEXC.sol#469-471)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (AEXC.sol#484-487)
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (AEXC.sol#524-526)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (AEXC.sol#532-535)
mint(address,uint256) should be declared external:
        - AEXC.mint(address,uint256) (AEXC.sol#596-599)
createBurnRequest(address,uint256) should be declared external:
        - AEXC.createBurnRequest(address,uint256) (AEXC.sol#608-620)
fulfillBurnRequest(uint256,uint256) should be declared external:
        - AEXC.fulfillBurnRequest(uint256,uint256) (AEXC.sol#637-654)
addAdmin(address[],bool) should be declared external:
        - AEXC.addAdmin(address[],bool) (AEXC.sol#671-675)
```

```
addAdmin(address[],bool) should be declared external:
        - AEXC.addAdmin(address[],bool) (AEXC.sol#671-675)
editTierUser(address[],uint256,bool) should be declared external:
        - AEXC.editTierUser(address[],uint256,bool) (AEXC.sol#683-696)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:AEXC.sol analyzed (7 contracts with 75 detectors), 37 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

AEXC.sol

Gas & Economy

Gas costs:

Gas requirement of function AEXC.name is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 140:4:

Gas costs:

Gas requirement of function AEXC.mint is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 596:4:

Gas costs:

Gas requirement of function AEXC.createBurnRequest is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 608:4:

Gas costs:

Gas requirement of function AEXC.fulfillBurnRequest is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 637:4:

Gas costs:

Gas requirement of function AEXC.editTierUser is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 683:4:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.
more
Pos: 689:8:

Miscellaneous

Constant/View/Pure functions:

ERC20._afterTokenTransfer(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 456:4:

Similar variable names:

AEXC.authorizedTierUser(address,uint256) : Variables have very similar names "user" and "tier". Note: Modifiers are currently not considered by this static analysis.
Pos: 663:19:

Similar variable names:

AEXC.authorizedTierUser(address,uint256) : Variables have very similar names "user" and "tier". Note: Modifiers are currently not considered by this static analysis.
Pos: 664:31:

No return:

IERC20Metadata.decimals(): Defines a return type but never explicitly returns a value.
Pos: 101:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 638:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 639:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 641:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 688:8:

Solhint Linter

AEXC.sol

```
AEXC.sol:3:1: Error: Compiler version ^0.8.9 does not satisfy the r
semver requirement
AEXC.sol:39:5: Error: Explicitly mark visibility in function (Set
ignoreConstructors to true if using solidity >=0.7.0)
AEXC.sol:42:27: Error: Code contains empty blocks
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Email: audit@EtherAuthority.io