Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Adamia (EURA) Token
Website: https://adamia.de
Platform: Ethereum
Language: Solidity
Date: July 27th, 2023

Table of contents

`

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 Adamia team to perform the Security audit of the Adamia (EURA) 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 July 27th, 2023.

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

- Adamia is an ERC20 standard token contract on the ethereum blockchain.

- The smart contracts have functions like minting, burning, etc.

Audit scope

Name	Code Review and Security Analysis Report for Adamia (EURA) Token Smart Contract
Platform	**Ethereum / Solidity**
File	Adamia.sol
Online Code	0xC47842E5B24DA5810Ceedafe086286bD43B92875
Audit Date	July 27th, 2023

This is a private and confidential document. No part of this document should
be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Name: Adamia ● Symbol: EURA ● Decimals: 6 ● Total Supply: 1 billion ● Initial Supply: 1 billion	**YES, This is valid.**
Ownership Control: ● Owner can mint unlimited tokens as this is a stable token. ● Owner can add/remove any wallet from the blacklist. ● Owner can renounce ownership. ● Current owner can transfer the ownership.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **"Secured"**. This token contract does contain owner control, which does not make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here →
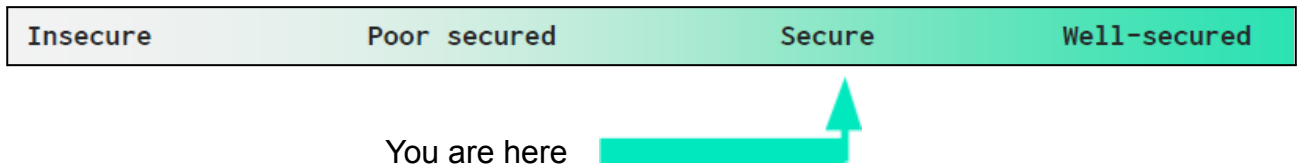
We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

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 0 low and 4 very low level issues.

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	Moderated
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	Moderated
	"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 EURA 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 EURA Token.

The EURA Token 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 **well** commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given an Adamia Token smart contract code in the form of a https://etherscan.io web link. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented.And 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.

Another source of information was its official project URL: https://adamia.de which provided rich information about the project architecture and tokenomics.

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 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	name	read	Passed	No Issue
8	symbol	read	Passed	No Issue
9	decimals	read	Passed	No Issue
10	totalSupply	read	Passed	No Issue
11	balanceOf	read	Passed	No Issue
12	transfer	write	Passed	No Issue
13	allowance	read	Passed	No Issue
14	approve	write	Passed	No Issue
15	transferFrom	write	Passed	No Issue
16	increaseAllowance	write	Passed	No Issue
17	decreaseAllowance	write	Passed	No Issue
18	_transfer	internal	Passed	No Issue
19	_mint	internal	Passed	No Issue
20	_burn	internal	Passed	No Issue
21	_approve	internal	Passed	No Issue
22	_spendAllowance	internal	Passed	No Issue
23	_beforeTokenTransfer	internal	Passed	No Issue
24	_afterTokenTransfer	internal	Passed	No Issue
25	decimals	write	Passed	No Issue
26	mint	write	Unlimited token minting by the Owner	Refer Audit Findings
27	burn	write	Passed	No Issue
28	addToBlacklist	write	Owner can freeze any wallet	Refer Audit Findings
29	removeFromBlacklist	write	access only Owner	No Issue
30	isBlacklisted	read	Passed	No Issue
31	transfer	write	Passed	No Issue
32	transferFrom	write	Passed	No Issue
33	approve	write	Passed	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:

(1) Make variables constant:

```
uint256 public initialSupply = 1000000000 * 10**_decimals;
```

These variables will be unchanged. So, please make it constant. It will save some gas.

Resolution: Declare those variables as constant. Just put a constant keyword.

(2) Missing antiwhale feature:

There is no limit for transferring tokens. Hence after adding liquidity users can buy lots of tokens at a lower price, and can manipulate the token supply.

Resolution: We suggest adding a transfer limit for some time period to restrict the users from buying large amounts of tokens at lower price.

This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io

(3) Unlimited token minting by the Owner:

The token owner can mint unlimited tokens. Token minting without any maximum limit is considered inappropriate for tokenomics.

Resolution: We recommend placing some limit on token minting to mitigate this issue.

Status: Acknowledged as a business requirement.

(4) Owner can freeze any wallet:

The owner can blacklist any wallet at any time. By this users will freeze and cannot transfer or use his tokens.

Resolution: We suggest confirming this feature and the owner has to secure his private key so that nobody misuse this feature.

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:

Adamia.sol

- mint: Owner can mint unlimited tokens.
- addToBlacklist: Owner can add any wallet to blacklist.
- removeFromBlacklist: Owner can remove any wallet from blacklist.

Ownable.sol

- renounceOwnership: Deleting ownership will leave the contract without an owner, removing any owner-only functionality.
- transferOwnership: Current owner can transfer ownership of the contract to a new account.

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 https://etherscan.io web link. And we have used all possible tests based on given objects as files. We had observed 4 informational issues in the smart contracts. But those are not critical ones. So, **it's good to go for the production**.

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.

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

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.
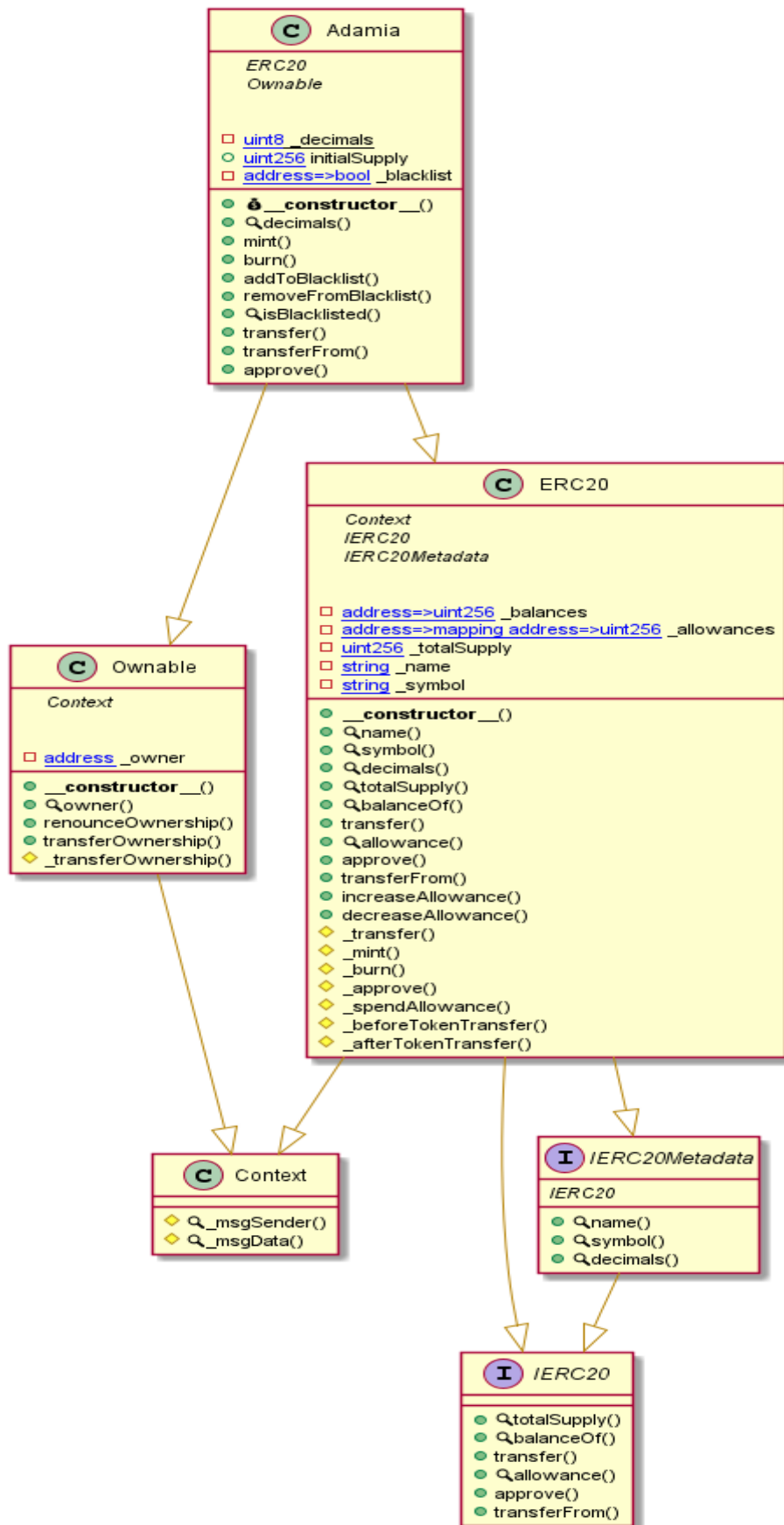
Technical Disclaimer

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 - Adamia (EURA) Token

Adamia

C

ERC20
Ownable

- □ uint8 _decimals
- ○ uint256 initialSupply
- □ address=>bool _blacklist

- ● __constructor__()
- ● decimals()
- ● mint()
- ● burn()
- ● addToBlacklist()
- ● removeFromBlacklist()
- ● isBlacklisted()
- ● transfer()
- ● transferFrom()
- ● approve()

ERC20

C

Context
IERC20
IERC20Metadata

- □ address=>uint256 _balances
- □ address=>mapping address=>uint256 _allowances
- □ uint256 _totalSupply
- □ string _name
- □ string _symbol

- ● __constructor__()
- ● name()
- ● symbol()
- ● decimals()
- ● totalSupply()
- ● balanceOf()
- ● transfer()
- ● allowance()
- ● approve()
- ● transferFrom()
- ● increaseAllowance()
- ● decreaseAllowance()
- ◇ _transfer()
- ◇ _mint()
- ◇ _burn()
- ◇ _approve()
- ◇ _spendAllowance()
- ◇ _beforeTokenTransfer()
- ◇ _afterTokenTransfer()

Ownable

C

Context

- □ address _owner

- ● __constructor__()
- ● owner()
- ● renounceOwnership()
- ● transferOwnership()
- ◇ _transferOwnership()

Context

C

- ◇ _msgSender()
- ◇ _msgData()

IERC20Metadata

I

IERC20

- ● name()
- ● symbol()
- ● decimals()

IERC20

I

- ● totalSupply()
- ● balanceOf()
- ● transfer()
- ● allowance()
- ● approve()
- ● transferFrom()

Slither Results Log

Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

Slither Log >> Adamia.sol

```
Contract locking ether found:
        Contract Adamia (Adamia.sol#595-672) has payable functions:
        - Adamia.constructor() (Adamia.sol#606-608)
        But does not have a function to withdraw the ether
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#contracts-that-lock-ether

Context._msgData() (Adamia.sol#24-26) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version0.8.19 (Adamia.sol#7) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.
16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Constant Adamia._decimals (Adamia.sol#598) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Adamia.slitherConstructorVariables() (Adamia.sol#595-672) uses literals with too many digits:
        - initialSupply = 1000000000 * 10 ** _decimals (Adamia.sol#599)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

Adamia.initialSupply (Adamia.sol#599) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
Adamia.sol analyzed (6 contracts with 84 detectors), 7 result(s) found
```

Solidity Static Analysis

Adamia.sol

Gas costs:

Gas requirement of function Adamia.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: 616:4:

Gas costs:

Gas requirement of function Adamia.burn 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: 623:4:

Constant/View/Pure functions:

Adamia.approve(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 666:4:

No return:

IERC20.transferFrom(address,address,uint256): Defines a return type but never explicitly returns a value.
Pos: 106:4:

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: 624:8:

Solhint Linter

Adamia.sol

```
Compiler version 0.8.19 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:6
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:191
Error message for require is too long
Pos: 9:341
Error message for require is too long
Pos: 9:368
Error message for require is too long
Pos: 9:369
Error message for require is too long
Pos: 9:374
Error message for require is too long
Pos: 9:423
Error message for require is too long
Pos: 9:428
Error message for require is too long
Pos: 9:458
Error message for require is too long
Pos: 9:459
Code contains empty blocks
Pos: 24:505
Code contains empty blocks
Pos: 24:525
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:540
Error message for require is too long
Pos: 9:575
Constant name must be in capitalized SNAKE_CASE
Pos: 5:597
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:605
Error message for require is too long
Pos: 9:639
```

Software analysis result:

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