TECHRIGHT

Security Assessment

# AnkaaToken - Audit

TechRight Verified on 03 May, 2023

---------------------

## Table of contents

## Disclaimer

## Description

Network

Arbitrum

Website

https://www.ankaa.io

Twitter

https://twitter.com/AnkaaExchange

Telegram

https://t.me/ANKAAChat

DApp

https://exchange.ankaa.io

## Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0

| Level | Value | Vulnerability | Risk<br>(Required Action) |
|---|---|---|---|
| Critical | 9 - 10 | A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken. | Immediate action to reduce risk level. |
| High | 7 - 8.9 | A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way. | Implementation of corrective actions as soon as possible. |
| Medium | 4 - 6.9 | A vulnerability that could affect the desired outcome of executing the contract in a specific scenario. | Implementation of corrective actions in a certain period. |
| Low | 2 - 3.9 | A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective. | Implementation of certain corrective actions or accepting the risk. |
| Informational | 0 - 1.9 | A vulnerability that has informational character but is not affecting any of the code. | An observation that does not determine a level of risk |

## Auditing Strategy and Techniques Applied

During the evaluation process, the repository was thoroughly examined to identify any security-related concerns, assess code quality, and ensure adherence to specifications and best practices. Our team of expert pentesters and smart contract developers reviewed the code line-by-line and documented any issues identified.

## Methodology

The auditing process follows a step-by-step routine:

1. Code review that includes:
   i. Review of the specifications, sources and instructions provided to TechRight to ensure a thorough understanding of the size, scope, and functionality of the smart contract's.

   ii. Manual review of code, which involves carefully reading the source code line-by-line to identify potential vulnerabilities.

   iii. Comparison to specification, which is the process of confirming whether the code performs as described in the specifications, sources, and instructions provided.

2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which involves assessing the degree to which test cases cover the code and how much of the code is executed while running those test cases.

   ii. Symbolic execution, which refers to the analysis of a program to identify the inputs that trigger each component of the program to execute.

3. Best practices review, which involves evaluating smart contracts to enhance efficiency, effectiveness, clarity, maintainability, security, and control in accordance with industry and academic practices, recommendations, and research.

4. Specific, itemized, actionable recommendations that enable you to take necessary measures to secure your smart contracts.

## Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review

## Scope

This section lists files that are in scope for the metrics report.

- **Project:** `AnkaaToken`
- **Included Files:**
    - ``
- **Excluded Paths:**
    - ``
- **File Limit:** `undefined`
    - **Exclude File list Limit:** `undefined`
- **Workspace Repository:** `unknown` (`undefined`@`undefined`)

### Source Units in Scope

Source Units Analyzed: `1`
Source Units in Scope: `1` (**100%**)

| Type | File | Logic Contracts | Interfaces | Lines | nLines | nSLOC | Comment Lines | Complex. Score | Capabilities |
|---|---|---|---|---|---|---|---|---|---|
| 📝📚🔍🎨 | AnkaaToken.sol | 8 | 4 | 1492 | 1328 | 584 | 758 | 420 | 🖥🧮🔆Σ |
| 📝📚🔍🎨 | **Totals** | **8** | **4** | **1492** | **1328** | **584** | **758** | **420** | 🖥🧮🔆Σ |

Legend:

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

#### Out of Scope

##### Excluded Source Units

Source Units Excluded: `0`

| File |
|---|
| None |

##### Duplicate Source Units

Duplicate Source Units Excluded: `0`

| File |
|---|
| None |

##### Doppelganger Contracts

Doppelganger Contracts: `3`

| File | Contract | Doppelganger |
|---|---|---|
| AnkaaToken.sol | IERC165 | (exact) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45 |

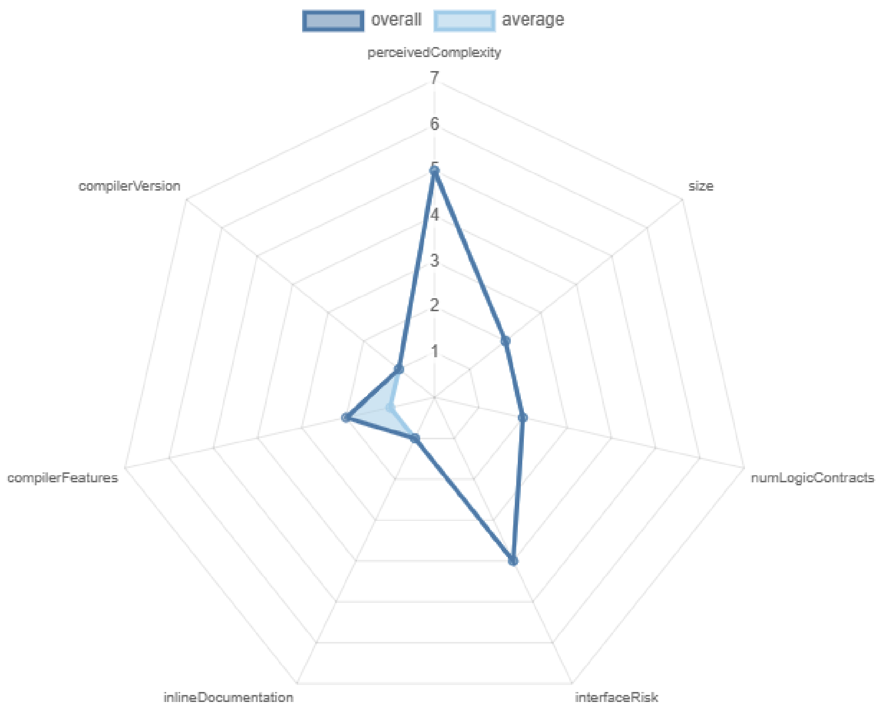
| File | Contract | Doppelganger |
|---|---|---|
| AnkaaToken.sol | IERC20 | (fuzzy) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57 |
| AnkaaToken.sol | IERC20Metadata | (fuzzy) 0, 1, 2 |

## Report

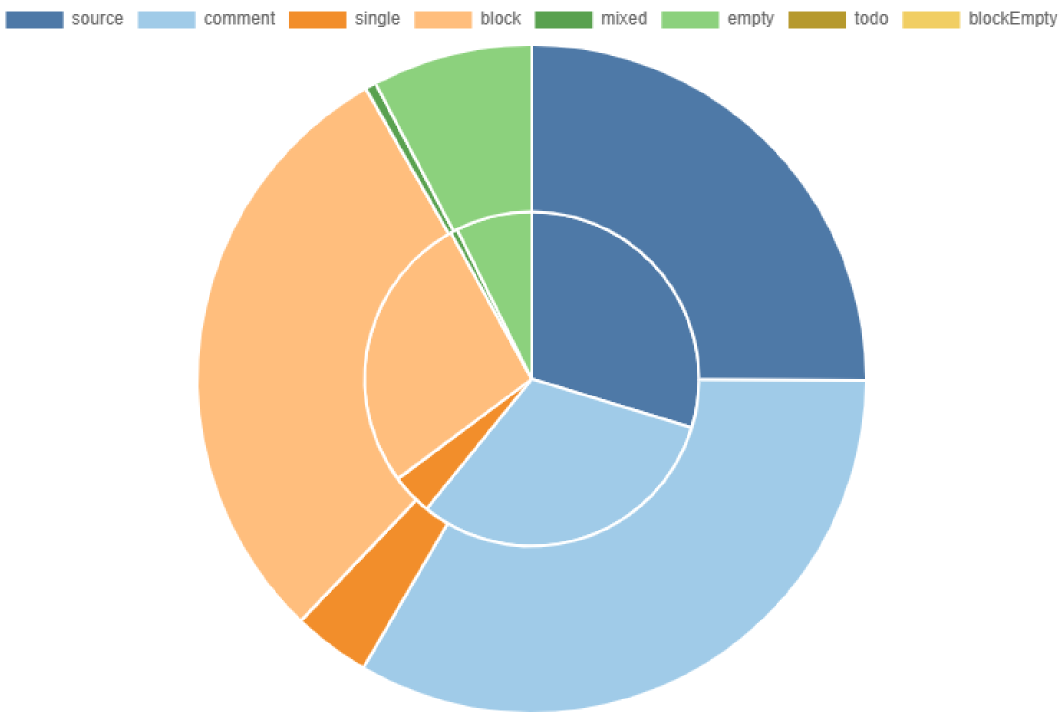
### Overview

The analysis finished with `0` errors and `0` duplicate files.

#### Risk



#### Source Lines (sloc vs. nsloc)



#### Inline Documentation

- **Comment-to-Source Ratio:** On average there are `0.75` code lines per comment (lower=better).
- **ToDo's:** `0`

#### Components

| 📝Contracts | 📚Libraries | 🔍Interfaces | 🎨Abstract |
|---|---|---|---|
| 2 | 2 | 4 | 4 |

#### Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

| 🌐Public | 💰Payable |
|---|---|
| 38 | 0 |

| External | Internal | Private | Pure | View |
|---|---|---|---|---|
| 15 | 72 | 0 | 18 | 27 |

#### StateVariables

| Total | 🌐Public |
|---|---|
| 13 | 3 |

#### Capabilities

| Solidity Versions observed | 🧪 Experimental Features | 💰 Can Receive Funds | 🖥 Uses Assembly | 💣 Has Destroyable Contracts |
|---|---|---|---|---|
| `^0.8.9` | | | `yes` (5 asm blocks) | |

| 📤 Transfers ETH | ⚡ Low-Level Calls | 👥 DelegateCall | 🧮 Uses Hash Functions | 🔖 ECRecover | 🌀 New/Create/Create2 |
|---|---|---|---|---|---|
| | | | `yes` | | |

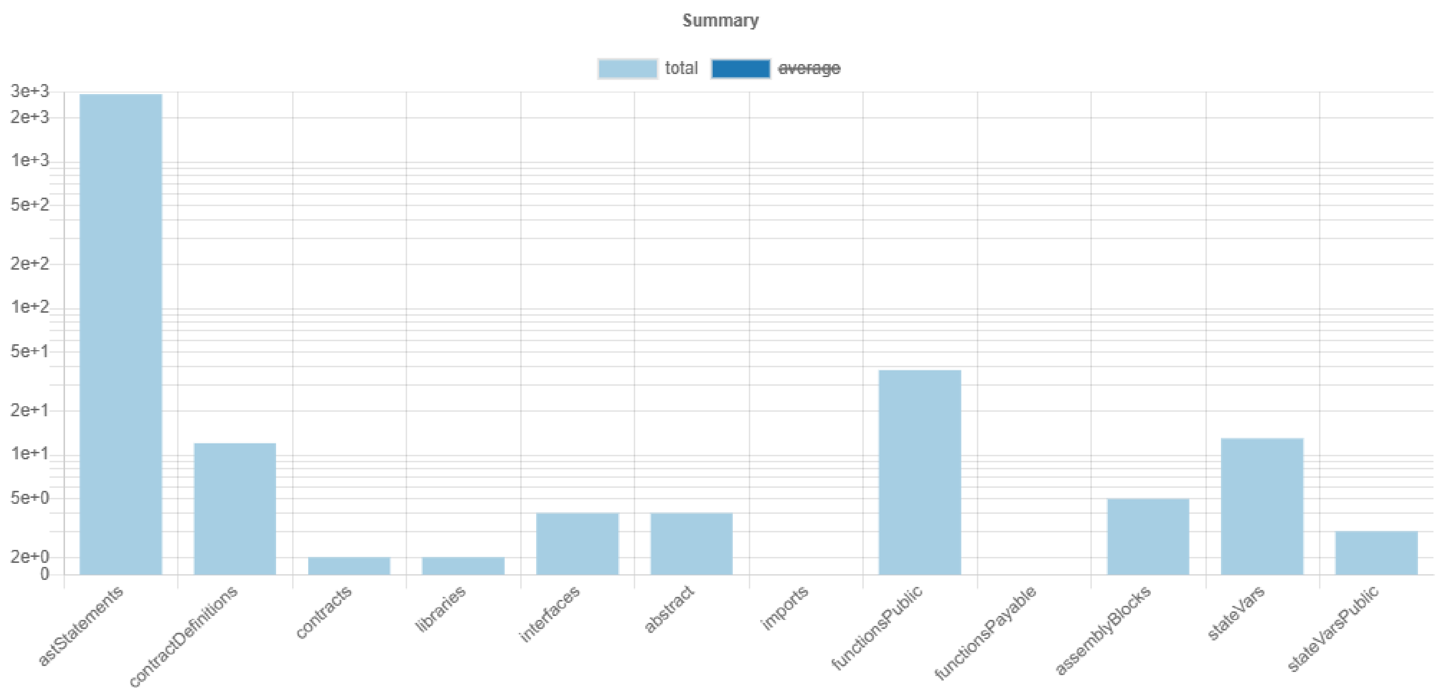
| ♻️ TryCatch | Σ Unchecked |
|---|---|
| | `yes` |

#### Dependencies / External Imports

| Dependency / Import Path | Count |
|---|---|

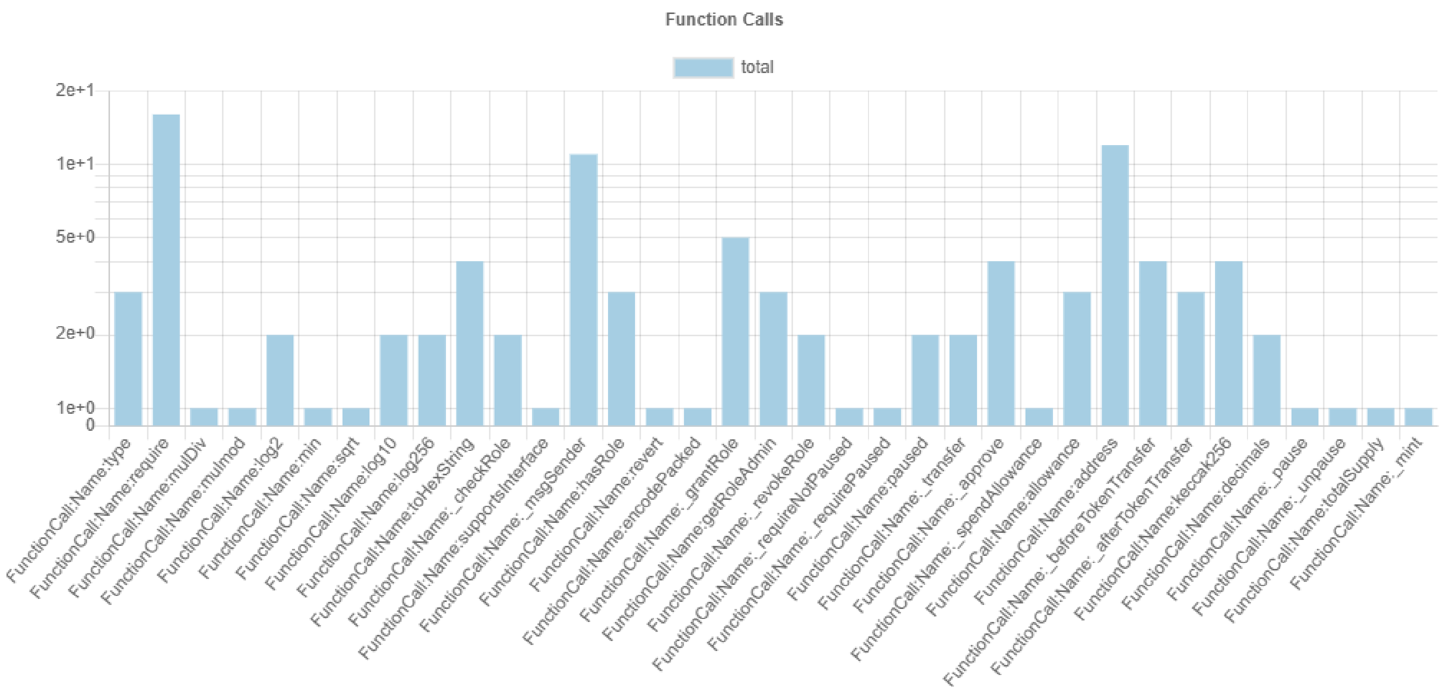
#### Totals

##### Summary

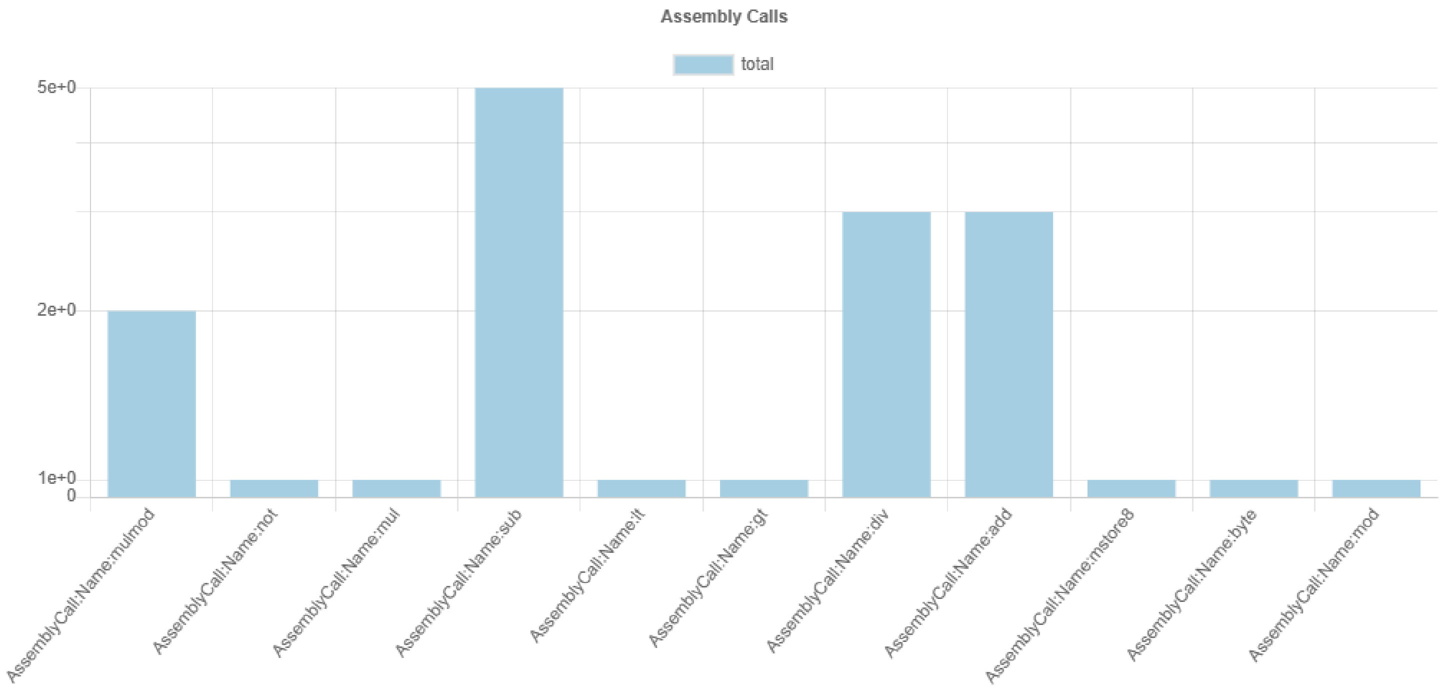


##### AST Node Statistics

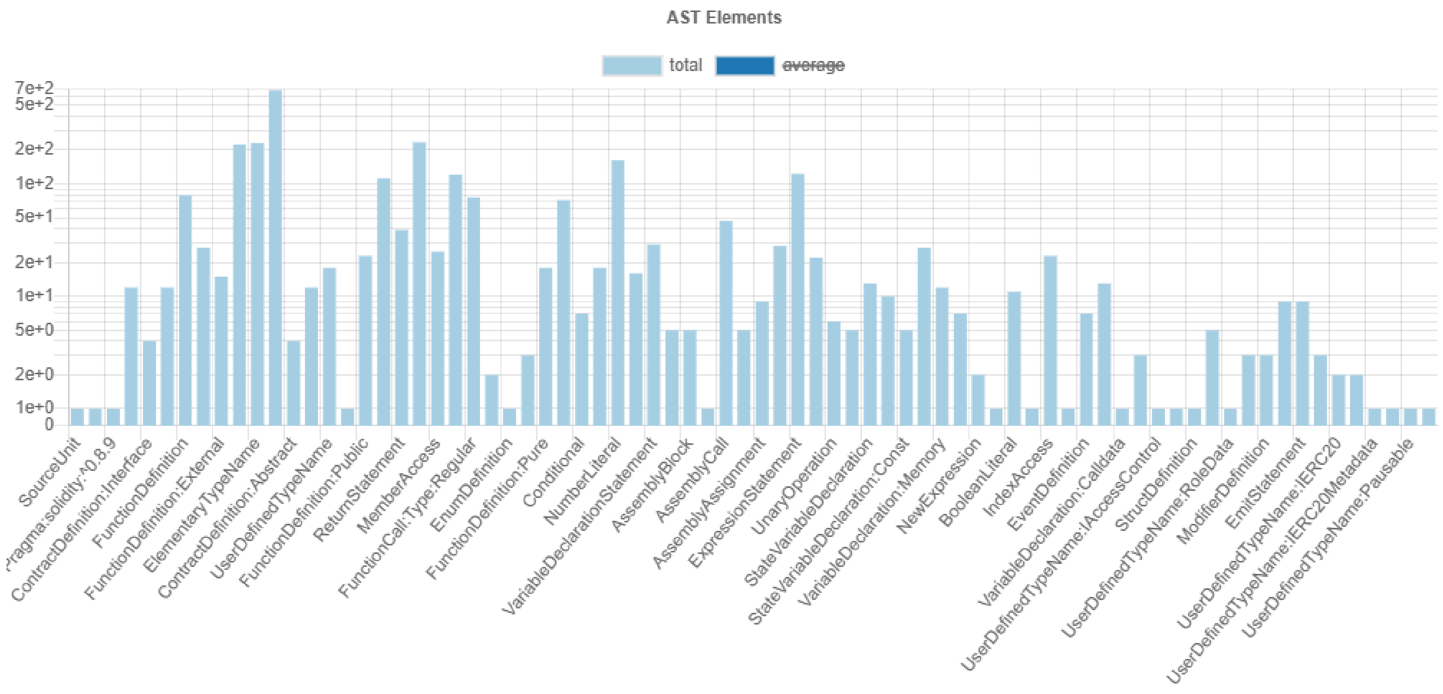
#### Function Calls



## Assembly Calls



## AST Total



**Inheritance Graph**

**Contract Summary**

Sūrya's Description Report Files Description Table

| File Name | SHA-1 Hash |
|---|---|
| AnkaaToken.sol | ab0ca70b128d228a14e2bcbaeff79fdfa0afd1dd |

Contracts Description Table

| Contract | Type | Bases | | |
|---|---|---|---|---|
| └ | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| | | | | |
| **IERC165** | Interface | | | |
| └ | supportsInterface | External ❗ | | NO❗ |
| | | | | |
| **ERC165** | Implementation | IERC165 | | |
| └ | supportsInterface | Public ❗ | | NO❗ |
| | | | | |
| **Math** | Library | | | |
| └ | max | Internal 🔒 | | |
| └ | min | Internal 🔒 | | |
| └ | average | Internal 🔒 | | |
| └ | ceilDiv | Internal 🔒 | | |
| └ | mulDiv | Internal 🔒 | | |
| └ | mulDiv | Internal 🔒 | | |
| └ | sqrt | Internal 🔒 | | |
| └ | sqrt | Internal 🔒 | | |
| └ | log2 | Internal 🔒 | | |
| └ | log2 | Internal 🔒 | | |
| └ | log10 | Internal 🔒 | | |
| └ | log10 | Internal 🔒 | | |
| └ | log256 | Internal 🔒 | | |
| └ | log256 | Internal 🔒 | | |
| | | | | |
| **Strings** | Library | | | |
| └ | toString | Internal 🔒 | | |
| └ | toHexString | Internal 🔒 | | |
| └ | toHexString | Internal 🔒 | | |
| └ | toHexString | Internal 🔒 | | |
| | | | | |
| **IAccessControl** | Interface | | | |
| └ | hasRole | External ❗ | | NO❗ |
| └ | getRoleAdmin | External ❗ | | NO❗ |
| └ | grantRole | External ❗ | 🛑 | NO❗ |
| └ | revokeRole | External ❗ | 🛑 | NO❗ |
| └ | renounceRole | External ❗ | 🛑 | NO❗ |

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | | | | |
| **Context** | Implementation | | | |
| └ | _msgSender | Internal 🔒 | | |
| └ | _msgData | Internal 🔒 | | |
| | | | | |
| **AccessControl** | Implementation | Context, IAccessControl, ERC165 | | |
| └ | supportsInterface | Public ❗ | | NO❗ |
| └ | hasRole | Public ❗ | | NO❗ |
| └ | _checkRole | Internal 🔒 | | |
| └ | _checkRole | Internal 🔒 | | |
| └ | getRoleAdmin | Public ❗ | | NO❗ |
| └ | grantRole | Public ❗ | 🛑 | onlyRole |
| └ | revokeRole | Public ❗ | 🛑 | onlyRole |
| └ | renounceRole | Public ❗ | 🛑 | NO❗ |
| └ | _setupRole | Internal 🔒 | 🛑 | |
| └ | _setRoleAdmin | Internal 🔒 | 🛑 | |
| └ | _grantRole | Internal 🔒 | 🛑 | |
| └ | _revokeRole | Internal 🔒 | 🛑 | |
| | | | | |
| **Pausable** | Implementation | Context | | |
| └ | | Public ❗ | 🛑 | NO❗ |
| └ | paused | Public ❗ | | NO❗ |
| └ | _requireNotPaused | Internal 🔒 | | |
| └ | _requirePaused | Internal 🔒 | | |
| └ | _pause | Internal 🔒 | 🛑 | whenNotPaused |
| └ | _unpause | Internal 🔒 | 🛑 | whenPaused |
| | | | | |
| **IERC20** | Interface | | | |
| └ | totalSupply | External ❗ | | NO❗ |
| └ | balanceOf | External ❗ | | NO❗ |
| └ | transfer | External ❗ | 🛑 | NO❗ |
| └ | allowance | External ❗ | | NO❗ |
| └ | approve | External ❗ | 🛑 | NO❗ |
| └ | transferFrom | External ❗ | 🛑 | NO❗ |
| | | | | |
| **IERC20Metadata** | Interface | IERC20 | | |
| └ | name | External ❗ | | NO❗ |
| └ | symbol | External ❗ | | NO❗ |
| └ | decimals | External ❗ | | NO❗ |
| | | | | |
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata | | |
| └ | | Public ❗ | 🛑 | NO❗ |

| Contract | Type | Bases | | |
|---|---|---|---|---|
| └ | name | Public ❗ | | NO❗ |
| └ | symbol | Public ❗ | | NO❗ |
| └ | decimals | Public ❗ | | NO❗ |
| └ | totalSupply | Public ❗ | | NO❗ |
| └ | balanceOf | Public ❗ | | NO❗ |
| └ | transfer | Public ❗ | 🛑 | NO❗ |
| └ | allowance | Public ❗ | | NO❗ |
| └ | approve | Public ❗ | 🛑 | NO❗ |
| └ | transferFrom | Public ❗ | 🛑 | NO❗ |
| └ | increaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | decreaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | _transfer | Internal 🔒 | 🛑 | |
| └ | _mint | Internal 🔒 | 🛑 | |
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _approve | Internal 🔒 | 🛑 | |
| └ | _spendAllowance | Internal 🔒 | 🛑 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfer | Internal 🔒 | 🛑 | |
| | | | | |
| **AnkaaToken** | Implementation | ERC20, Pausable, AccessControl | | |
| └ | | Public ❗ | 🛑 | ERC20 |
| └ | maxSupply | Public ❗ | | NO❗ |
| └ | pause | Public ❗ | 🛑 | onlyRole |
| └ | unpause | Public ❗ | 🛑 | onlyRole |
| └ | mint | Public ❗ | 🛑 | onlyRole |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑 | whenNotPaused |

Legend

| Symbol | Meaning |
|---|---|
| 🛑 | Function can modify state |
| 💵 | Function is payable |

## Detectors Issue

| Description | Check | Impact | Confidence |
|---|---|---|---|
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#185) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#182) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- prod0 = prod0 / twos (AnkaaToken.sol#166)<br>- result = prod0 * inverse (AnkaaToken.sol#193) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#186) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#187) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse = (3 * denominator) ^ 2 (AnkaaToken.sol#178) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#183) | divide-before-multiply | Medium | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) performs a multiplication on the result of a division:<br>- denominator = denominator / twos (AnkaaToken.sol#163)<br>- inverse *= 2 - denominator * inverse (AnkaaToken.sol#184) | divide-before-multiply | Medium | Medium |
| Strings.toString(uint256) (AnkaaToken.sol#425-445) uses assembly<br>- INLINE ASM (AnkaaToken.sol#431-433)<br>- INLINE ASM (AnkaaToken.sol#437-439) | assembly | Informational | High |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) uses assembly<br>- INLINE ASM (AnkaaToken.sol#127-131)<br>- INLINE ASM (AnkaaToken.sol#147-154)<br>- INLINE ASM (AnkaaToken.sol#161-170) | assembly | Informational | High |
| AccessControl._setRoleAdmin(bytes32,bytes32) (AnkaaToken.sol#808-812) is never used and should be removed | dead-code | Informational | Medium |
| Math.ceilDiv(uint256,uint256) (AnkaaToken.sol#106-109) is never used and should be removed | dead-code | Informational | Medium |
| Math.log10(uint256,Math.Rounding) (AnkaaToken.sol#357-362) is never used and should be removed | dead-code | Informational | Medium |
| Math.mulDiv(uint256,uint256,uint256) (AnkaaToken.sol#116-196) is never used and should be removed | dead-code | Informational | Medium |
| Strings.toHexString(uint256) (AnkaaToken.sol#450-454) is never used and should be removed | dead-code | Informational | Medium |
| Math.sqrt(uint256,Math.Rounding) (AnkaaToken.sol#255-260) is never used and should be removed | dead-code | Informational | Medium |
| Math.max(uint256,uint256) (AnkaaToken.sol#80-82) is never used and should be removed | dead-code | Informational | Medium |
| Math.log2(uint256) (AnkaaToken.sol#266-302) is never used and should be removed | dead-code | Informational | Medium |
| Math.average(uint256,uint256) (AnkaaToken.sol#95-98) is never used and should be removed | dead-code | Informational | Medium |

| Description | Check | Impact | Confidence |
|---|---|---|---|
| Math.log2(uint256,Math.Rounding) (AnkaaToken.sol#308-313) is never used and should be removed | dead-code | Informational | Medium |
| Math.log256(uint256) (AnkaaToken.sol#370-394) is never used and should be removed | dead-code | Informational | Medium |
| Strings.toString(uint256) (AnkaaToken.sol#425-445) is never used and should be removed | dead-code | Informational | Medium |
| ERC20._burn(address,uint256) (AnkaaToken.sol#1343-1359) is never used and should be removed | dead-code | Informational | Medium |
| Math.log256(uint256,Math.Rounding) (AnkaaToken.sol#400-405) is never used and should be removed | dead-code | Informational | Medium |
| Math.sqrt(uint256) (AnkaaToken.sol#219-250) is never used and should be removed | dead-code | Informational | Medium |
| Context._msgData() (AnkaaToken.sol#591-593) is never used and should be removed | dead-code | Informational | Medium |
| Math.mulDiv(uint256,uint256,uint256,Math.Rounding) (AnkaaToken.sol#201-212) is never used and should be removed | dead-code | Informational | Medium |
| Math.log10(uint256) (AnkaaToken.sol#319-351) is never used and should be removed | dead-code | Informational | Medium |
| AccessControl._setupRole(bytes32,address) (AnkaaToken.sol#799-801) is never used and should be removed | dead-code | Informational | Medium |
| Math.min(uint256,uint256) (AnkaaToken.sol#87-89) is never used and should be removed | dead-code | Informational | Medium |
| AnkaaToken._maxSupply (AnkaaToken.sol#1457) is set pre-construction with a non-constant function or state variable:<br>- 10000000 * 10 ** decimals() | function-init-state | Informational | High |
| solc-0.8.19 is not recommended for deployment | solc-version | Informational | High |
| Pragma version^0.8.9 (AnkaaToken.sol#8) allows old versions | solc-version | Informational | High |
| AnkaaToken.slitherConstructorVariables() (AnkaaToken.sol#1453-1493) uses literals with too many digits:<br>- _maxSupply = 10000000 * 10 ** decimals() (AnkaaToken.sol#1457) | too-many-digits | Informational | Medium |

## Summary

| CRITICAL | HIGH | MEDIUM | LOW | INFORMATIONAL | OPTIMIZATION |
|---|---|---|---|---|---|
| Passed | Passed | 8 Issues | Passed | 26 Issues | Passed |

## Owner privileges

| No. | Issue | Description | Status |
|---|---|---|---|
| 1 | **No critical issues found** | The contract does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the source code. | **Passed** |
| 2 | **Contract owner cannot mint** | It is no possible to mint new tokens. | **Passed** |
| 3 | **Contract owner cannot blacklist addresses** | It is not possible to lock user funds by blacklisting addresses. | **Passed** |
| 4 | **Contract owner cannot set high fees** | The fees, if applicable, can be a maximum of 25% or lower. The contract can therefore not be locked. Please take a look in the comment section for more details. | **Passed** |
| 5 | **Contract owner cannot blacklist addresses** | It is not possible to lock user funds by blacklisting addresses | **Passed** |

| No. | Issue | Description | Status |
|---|---|---|---|
| 6 | **Contract cannot be locked** | Owner cannot lock any user funds. | **Passed** |