Cyberscope

Audit Report

AFRIQ ARBITRAGE SYSTEM

February 2024

Network	BSC TESTNET
Address	0x9E477F49b666124b5Ae0587E7A2A9991C6cA6ED6
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	BLC	Business Logic Concern	Unresolved
●	IDI	Immutable Declaration Improvement	Unresolved
●	RM	Redundant Modifier	Unresolved
●	L19	Stable Compiler Version	Unresolved

Table of Contents

Review

Contract Name	AASToken
Compiler Version	v0.8.23+commit.f704f362
Optimization	200 runs
Testing Deploy	https://testnet.bscscan.com/address/0x295126378652709f8952a80c2e86e51e1dd7a381
Explorer	https://testnet.bscscan.com/address/0x9e477f49b666124b5ae0587e7a2a9991c6ca6ed6
Address	0x9e477f49b666124b5ae0587e7a2a9991c6ca6ed6
Network	BSC_TESTNET
Symbol	AAST
Decimals	18
Total Supply	10,000,000,000
Badge Eligibility	Yes

Audit Updates

Initial Audit	22 Feb 2024

Source Files

Filename	SHA256
contracts/AASToken.sol	8fb5eb8373bde249a5ddd3724eb933994fd786188651c7f6aeb6213783e162a9
@openzeppelin/contracts/utils/Context.sol	847fda5460fee70f56f4200f59b82ae622bb03c79c77e67af010e31b7e2cc5b6
@openzeppelin/contracts/token/ERC20/IERC20.sol	6f2faae462e286e24e091d7718575179644dc60e79936ef0c92e2d1ab3ca3cee
@openzeppelin/contracts/token/ERC20/ERC20.sol	ddff96777a834b51a08fec26c69bb6ca2d01d150a3142b3fdd8942e07921636a
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	1d079c20a192a135308e99fa5515c27acfbb071e6cdb0913b13634e630865939
@openzeppelin/contracts/token/ERC20/extensions/ERC20Capped.sol	cb15f210495f2119cfec53e32738ddb23469d414c45a2d7444c2181a9940bbed
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	2e6108a11184dd0caab3f3ef31bd15fed1bc7e4c781a55bc867ccedd8474565c
@openzeppelin/contracts/interfaces/draft-IERC6093.sol	4aea87243e6de38804bf8737bf86f750443d3b5e63dd0fd0b7ad92f77cdbd3e3

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	4	0	0	0

BLC - Business Logic Concern

Criticality	Minor / Informative
Location	contracts/AASToken.sol#L18
Status	Unresolved

Description

The contract inherits from OpenZeppelin's `ERC20Capped` contract, indicating an intention to utilize a capped token supply. The constructor sets a fixed cap on the token supply and mints a specific number of tokens to the owner's address. Despite the inclusion of `ERC20Capped` , the contract lacks a public or external function that would allow for the minting of additional tokens up to this cap. Additionally, the `ERC20Capped.sol` library implements the same functionality as the overridden implementation.

```
function _update(address from, address to, uint256 value) internal virtual
override (ERC20Capped, ERC20) {

    if (from == address(0)) {
        uint256 maxSupply = cap();
        uint256 supply = totalSupply();

        if (supply + value > maxSupply) {
            revert("ERC20Capped: cap exceeded");
            //revert ERC20ExceededCap(supply, maxSupply);
        }
    }
    super._update(from, to, value);
}
```

Recommendation

It is recommended to revise the business logic of the contract, in order to determine the functionality of minting additional tokens.

IDI - Immutable Declaration Improvement

Criticality	Minor / Informative
Location	contracts/AASToken.sol#L14
Status	Unresolved

Description

The contract declares state variables that their value is initialized once in the constructor and are not modified afterwards. The `immutable` is a special declaration for this kind of state variables that saves gas when it is defined.

```
owner
```

Recommendation

By declaring a variable as immutable, the Solidity compiler is able to make certain optimizations. This can reduce the amount of storage and computation required by the contract, and make it more gas-efficient.

RM - Redundant Modifier

Criticality	Minor / Informative
Location	contracts/AASToken.sol#L32
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations. Specifically, the contract declares the `onlyOwner` modifier, which is not being used by the contract.

```
modifier onlyOwner {
    require(msg.sender == owner, "Only the owner can call this function");
    _;
}
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it. The team is advised to remove these segments from the contract.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	contracts/AASToken.sol#L4
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.23;
```

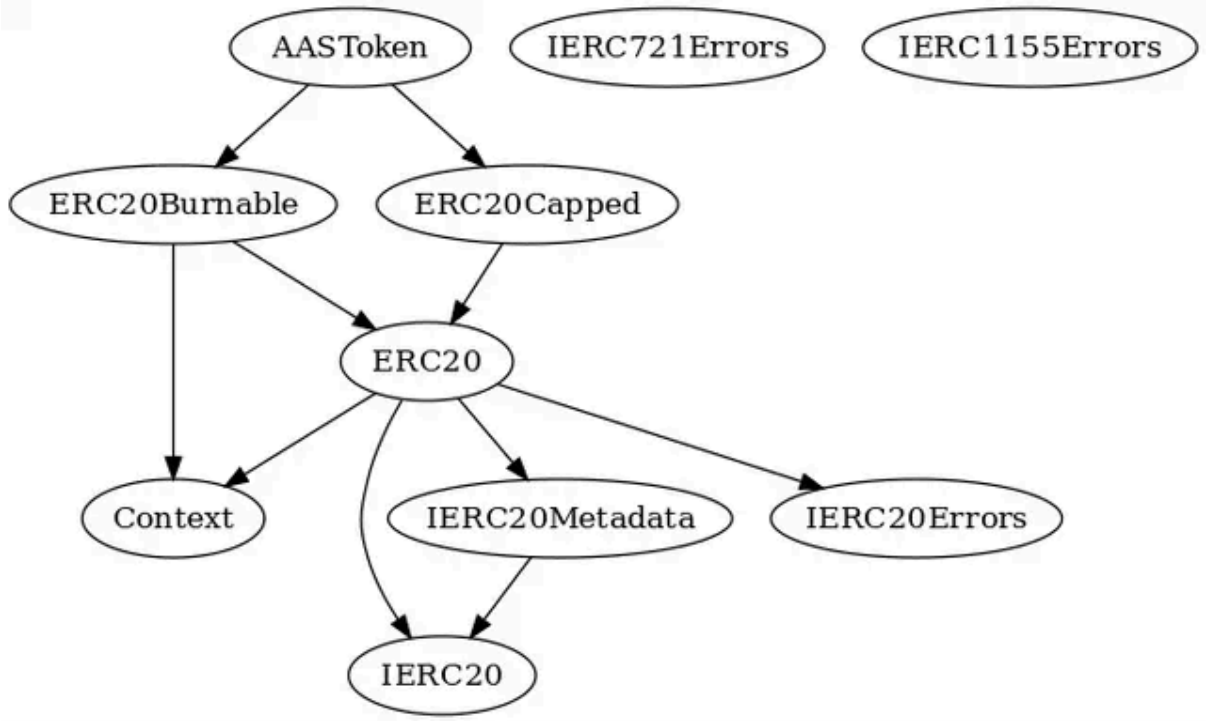
Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

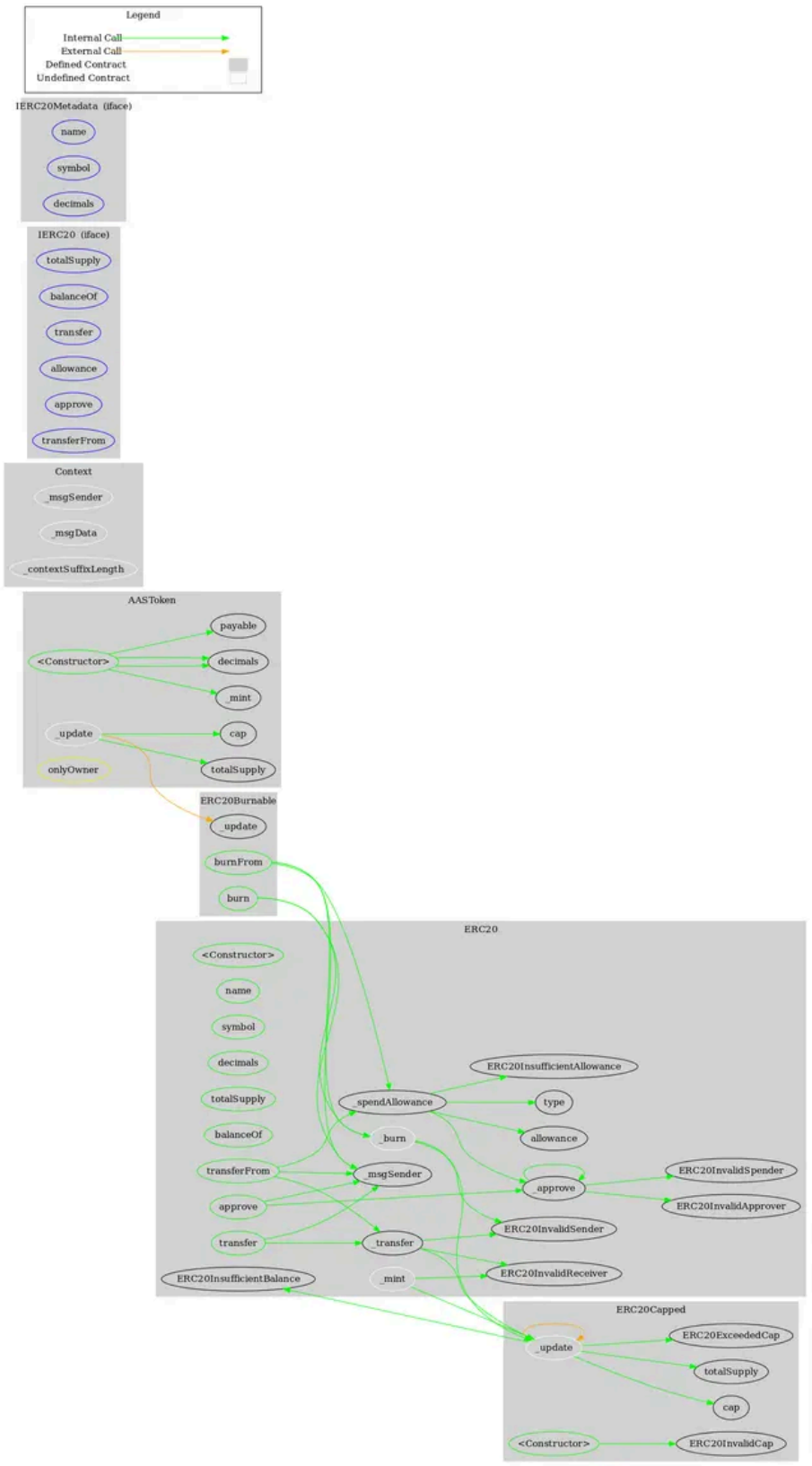
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AASToken	Implementation	ERC20Capped, ERC20Burnable		
		Public	✓	ERC20 ERC20Capped
	_update	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IERC20Metadata (iface)
name
symbol
decimals
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Context
_msgSender
_msgData
_contextSuffixLength
AASToken
payable
<Constructor>
decimals
_mint
_update
cap
onlyOwner
totalSupply
ERC20Burnable
_update
burnFrom
burn
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
approve
transfer
ERC20InsufficientBalance
ERC20InsufficientAllowance
spendAllowance
type
allowance
_burn
_msgSender
approve
ERC20InvalidSpender
ERC20InvalidApprover
ERC20InvalidSender
transfer
_mint
ERC20InvalidReceiver
ERC20Capped
_update
ERC20ExceededCap
totalSupply
cap
<Constructor>
ERC20InvalidCap

Summary

AFRIQ ARBITRAGE SYSTEM contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. AFRIQ ARBITRAGE SYSTEM is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope'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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io