



**NOVOS**

## **KYC & AUDIT.**

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.



# CERTIFICATE OF COMPLIANCE

Smart Contract Audit by NOVOS



A Dragons World

Audit Passed

09/30/2022

# Table of Contents

- ❖ **Audit Summary**
- ❖ **Project Overview**
- ❖ **Token Summary**
- ❖ **Main Contract Assessed**
- ❖ **Smart Contract Vulnerability Checks**
- ❖ **Contract Ownership**
- ❖ **Privileged Functions**
- ❖ **Important Notes The Users**
- ❖ **Findings Summary**
- ❖ **Classification of Issues**
- ❖ **Findings Summary**
- ❖ **Classification of Issues**
- ❖ **Findings Table**
- ❖ **Public function that could be declared external**
- ❖ **Missing events arithmetic**
- ❖ **Statistics**
- ❖ **Liquidity**
- ❖ **Token Holders**
- ❖ **Liquidity Holders**
- ❖ **Liquidity Ownership**



# Audit Summary

This report has been prepared for A Dragons World on the BSC network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.



## Project Overview

Parameter	Result
Address	0x1dfb236462707bdA9671656A4C9F232b5F804723
Name	A Dragons World
Token Tracker	ADW
Decimals	10
Supply	1,000,000,000
Platform	BSC
Compiler	v0.8.4+commit.c7e474f2
Optimization	Yes with 1 runs
Other Settings:	default evmVersion
Language	Solidity
Codebase	<a href="https://bscscan.com/address/0x518a6b702b6f65f4845b68adaf09756d54eca251#code">https://bscscan.com/address/0x518a6b702b6f65f4845b68adaf09756d54eca251#code</a>
Url	<a href="https://adragons.world/">https://adragons.world/</a>

## Main Contract Assessed

Name	Contract	Live
<b>A Dragons World</b>	0x1dfb236462707bdA9671656A4C9F232b5F804723	Yes



# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Unencrypted Private Data On-Chain	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Code With No Effects	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Message call with hardcoded gas amount	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Hash Collisions With Multiple Variable Length Arguments	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Unexpected Ether balance	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Presence of unused variables	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Right-To-Left-Override control character (U+202E)	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Typographical Error	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ DoS With Block Gas Limit	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Arbitrary Jump with Function Type Variable	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Insufficient Gas Griefing	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Incorrect Inheritance Order	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Write to Arbitrary Storage Location	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Requirement Violation	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Missing Protection against Signature Replay Attacks	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Weak Sources of Randomness from Chain Attributes	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>





# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Authorization through tx.origin	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Delegatecall to Untrusted Callee	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Use of Deprecated Solidity Functions	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Assert Violation	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Reentrancy	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Unprotected SELFDESTRUCT Instruction	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Unprotected Ether Withdrawal	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Unchecked Call Return Value	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Outdated Compiler Version	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Integer Overflow and Underflow	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Function Default Visibility	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>





# Contract Ownership

The contract ownership of A Dragons World is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

01

The current owner is the address `0x53e0FB31aea623D472ccD834746E490cfB356E8c` which can be viewed from: [HERE](#)

02

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

03

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.



# Important Notes To The Users:



01

If ``amount`` is the maximum ``uint256``, the allowance is not updated on ``transferFrom``. This is semantically equivalent to an infinite approval. Requirements: - ``spender`` cannot be the zero address.

02

**NOTE:** Does not update the allowance if the current allowance is the maximum ``uint256``. Requirements: - ``from`` and ``to`` cannot be the zero address. - ``from`` must have a balance of at least ``amount``. - the caller must have allowance for ``from``'s tokens of at least ``amount``.

03

Atomically increases the allowance granted to ``spender`` by the caller. This is an alternative to `{approve}` that can be used as a mitigation for \* problems described in `{IERC20-approve}`. Emits an `{Approval}` event indicating the updated allowance.

04

Atomically decreases the allowance granted to ``spender`` by the caller. This is an alternative to `{approve}` that can be used as a mitigation for problems described in `{IERC20-approve}`. \* Emits an `{Approval}` event indicating the updated allowance.

# Technical Findings Summary

## Classification of Issues

### Total

What you should pay attention to



# Findings

Public function that could be declared external



ID	Severity	Contract	Function
01	Informational	ADragonsWorld	Functions: size, getKeyAtIndex, getIndexOfKey

## Description

Gas Optimization. Public function that could be declared external

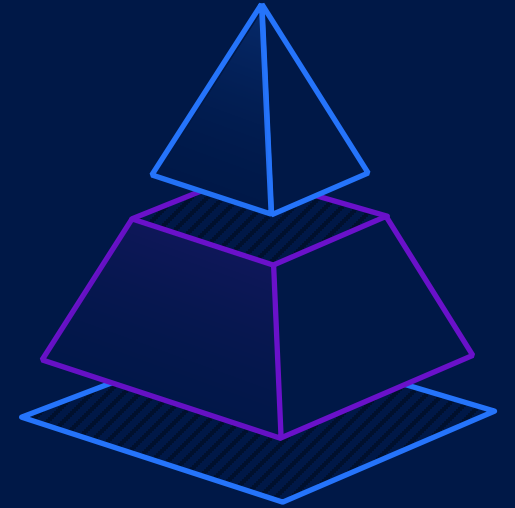
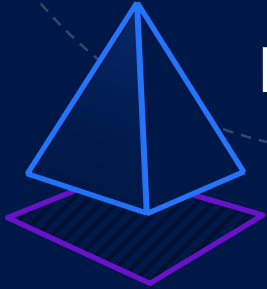
## Recommendation

Public functions that are never called by the contract should be declared external to save gas.



# Findings

## Missing events arithmetic



ID	Severity	Contract	Function
02	Informational	ADragonsWorld	Missing events for setWalletBalance, setMaxBuyTransaction, setMaxSellTransaction, setSwapTokensAtAmount, setSellTransactionMultiplier

### Description

Functions that change critical arithmetic parameters should emit an event.

### Recommendation

Emit corresponding events for critical parameter changes.

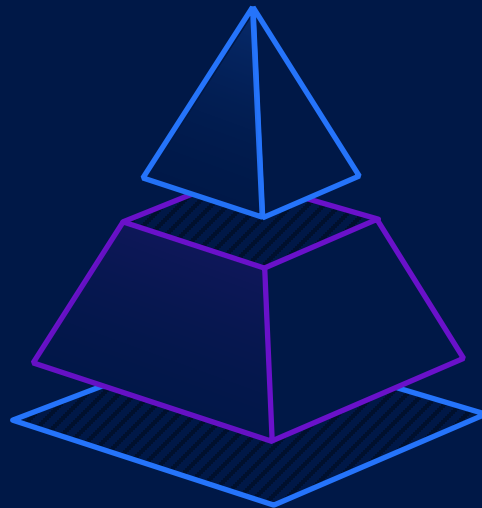


# Privileged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
✓ renounceOwnership	<ul style="list-style-type: none"><li>▪ none</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ transferOwnership	<ul style="list-style-type: none"><li>▪ address newOwner</li></ul>	<ul style="list-style-type: none"><li>▪ <b>public</b></li></ul>
✓ prepareForPartnerOrExchangeListing	<ul style="list-style-type: none"><li>▪ address_partnerOrExchangeAddress</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setWalletBalance	<ul style="list-style-type: none"><li>▪ uint256 _maxWalletBalance</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setMaxBuyTransaction	<ul style="list-style-type: none"><li>▪ uint256 _maxTxn</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setMaxSellTransaction	<ul style="list-style-type: none"><li>▪ uint256 _maxTxn</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ updateBusdDividendToken	<ul style="list-style-type: none"><li>▪ address _newContract</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ updateMarketingWallet	<ul style="list-style-type: none"><li>▪ address _newWallet</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setSwapTokensAtAmount	<ul style="list-style-type: none"><li>▪ uint256 _swapAmount</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setSellTransactionMultiplier	<ul style="list-style-type: none"><li>▪ uint256 _multiplier</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setTradingIsEnabled	<ul style="list-style-type: none"><li>▪ none</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setBusdDividendEnabled	<ul style="list-style-type: none"><li>▪ bool _enabled</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setMarketingEnabled	<ul style="list-style-type: none"><li>▪ bool _enabled</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ setSwapAndLiquifyEnabled	<ul style="list-style-type: none"><li>▪ bool _enabled</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ updatebusdDividendTracker	<ul style="list-style-type: none"><li>▪ address newAddress</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>
✓ updateUniswapV2Router	<ul style="list-style-type: none"><li>▪ address newAddress</li></ul>	<ul style="list-style-type: none"><li>▪ <b>external</b></li></ul>

# Privileged Functions (onlyOwner & Others)

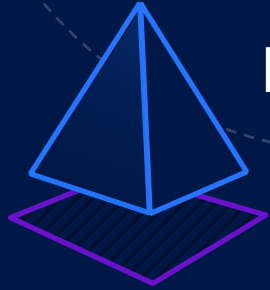
Function Name	Parameters	Visibility
✓ <code>excludeFromFees</code>	▪ <code>address account, bool excluded</code>	▪ <b>public</b>
✓ <code>excludeFromDividend</code>	▪ <code>address account</code>	▪ <b>public</b>
✓ <code>setAutomatedMarketMakerPair</code>	▪ <code>address pair, bool value</code>	▪ <b>external</b>
✓ <code>updateGasForProcessing</code>	▪ <code>uint256 newValue</code>	▪ <b>external</b>
✓ <code>updateMinimumBalanceForDividends</code>	▪ <code>uint256 newMinimumBalance</code>	▪ <b>external</b>
✓ <code>updateClaimWait</code>	▪ <code>uint256 claimWait</code>	▪ <b>external</b>
✓ <code>processDividendTracker</code>	▪ <code>uint256 gas</code>	▪ <b>external</b>





# Statistics

## Liquidity Info



Parameter	Result
Pair Address	-
ADW Reserves	0 ADW
Reserves, -	0 -
Liquidity Value	\$0



# Statistics

## Token (ADW) Holders Info

Parameter	Result
ADW Percentage Burnt	0 %
ADW Amount Burnt	0 ADW
Top 10 Percentage Own	100 %
Top 10 Amount Owned	1,000,000,000 ADW

Rank	Address	Quantity	Percentage	Analytics
1	<a href="#">Pinksale: PinkLock V2</a>	850,000,000	<u>85.0000%</u>	<a href="#">Analytics</a>
2	<a href="#">0x0f701caf391d2c4b5462143052c88718010b7bac</a>	149,150,000	<u>14.9150%</u>	<a href="#">Analytics</a>
3	<a href="#">0x53e0fb31aea623d472ccd834746e490cfb356e8c</a>	600,000	<u>0.0600%</u>	<a href="#">Analytics</a>
4	<a href="#">0x552ed31aabf6a60f5f71fa6a34aac8094913cf3c</a>	250,000	<u>0.0250%</u>	<a href="#">Analytics</a>





## Disclaimer

Novos has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Novos is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Novos or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by Novos 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.