



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

ARATA TOKEN AUDIT REPORT

2021

09 DEC 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
Arata Token Distribution	8
Arata Token Contract Interaction Details	8
Top 10 Token Holders	9
Security Issue	10
Token Logo	11
Conclusion	12



SECURITY ASSESMENT

SUMMARY

This report has been prepared for Arata to discover issues and vulnerabilities in the source code of the Arata project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Testnet Deployment techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and MotechAudit hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

BACKGROUND

MotechAudit was commissioned by Arata to perform an audit of smart contracts:

<https://bscscan.com/address/0xd4a06f9d51a992a3a1f07bd5cdff1c465b23a723>

The purpose of the audit was to achieve the following:

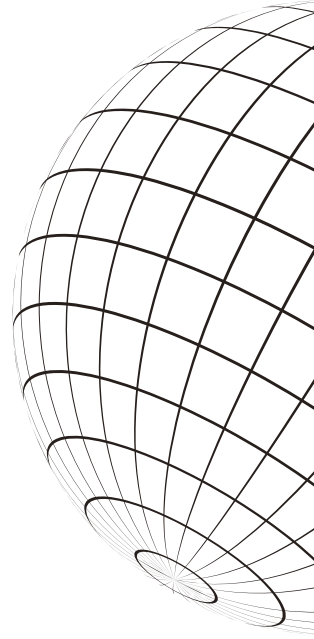
- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

AUDIT DETAILS



AUDITED PROJECT

Arata



DEPLOYER ADDRESS

0x6d0bbd8f6B032195B65e1F471A060B7341d25c2F



CLIENT CONTACTS:

Arata Team



BLOCKCHAIN

Binance smart chain Project



WEBSITE:

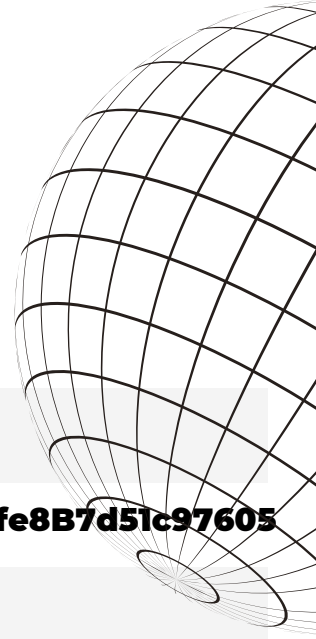
<https://arata.io>



SECURITY ASSESSMENT

CONTRACT DETAILS

Token contract details for Sep-25-2021



Contract name	Arata
Contract address	0x49092aB0b87f6C7B4449a6031dfe8B7d51c97605
Total supply	5,000,000 ARATA
Token ticker	Arata Studio (ARATA)
Decimals	18
Token holders	1,595
Transactions count	42,495
Top 100 holders dominance	97.95%
Contract deployer address	0x6d0bbd8f6B032195B65e1F471A060B7341d25c2F
Contract's current owner address	0x6d0bbd8f6B032195B65e1F471A060B7341d25c2F

SECURITY ASSESSMENT

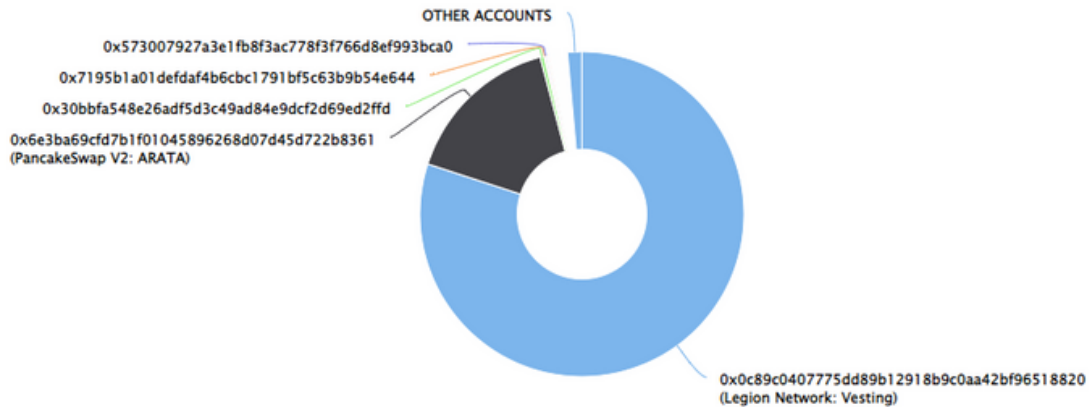
ARATA TOKEN DISTRIBUTION

The top 100 holders collectively own 98.58% (4,929,186.77 Tokens) of Arata Studio

Token Total Supply: 5,000,000.00 Token | Total Token Holders: 1,595

Arata Studio Top 100 Token Holders

Source: BscScan.com



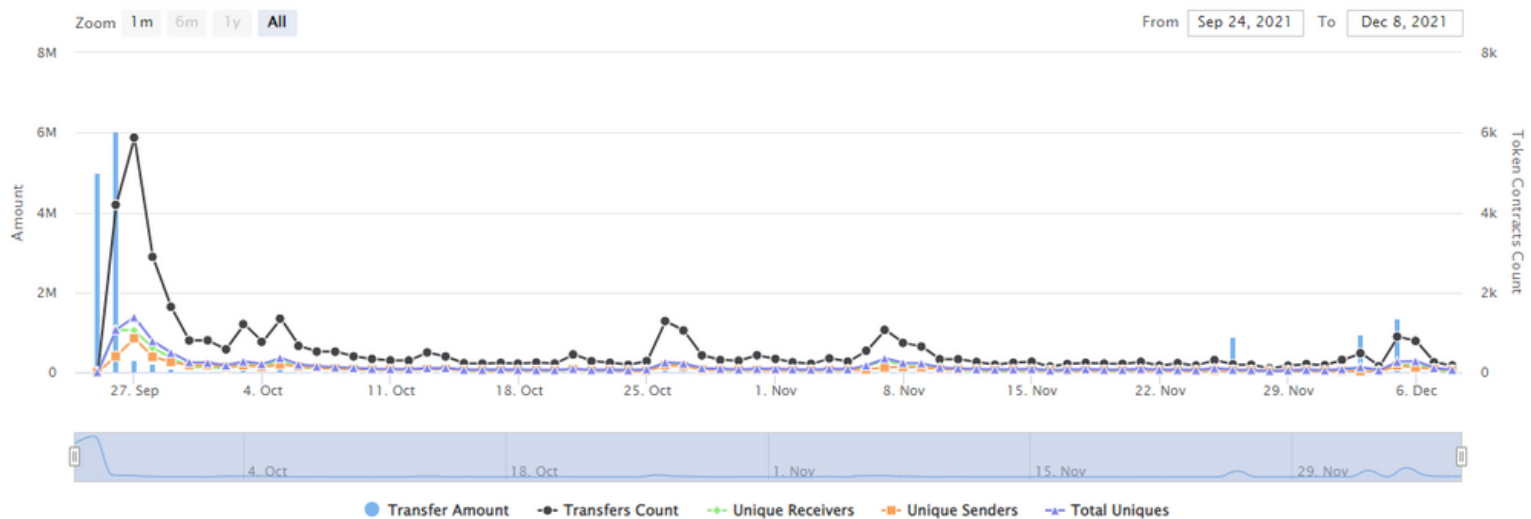
(A total of 4,929,186.77 tokens held by the top 100 accounts from the total supply of 5,000,000.00 token)

ARATA TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Sat 25, Sept 2021 - Wed 8, Dec 2021















Token Contract 0xd4a06f9d51a992a3a1f07bd5cdf1c465b23a723 (Arata Studio)
Source: BscScan.com



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

TOP 10 TOKEN HOLDERS

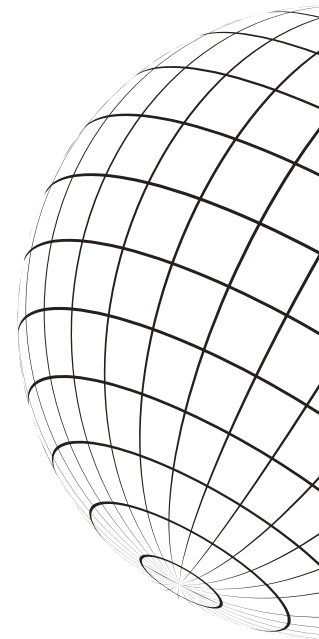
Rank	Address	Quantity	Percentage	Value	Analytics
1	 Legion Network: Vesting	4,000,000.000000000000000008	80.0000%	\$6,040,000.00	
2	 PancakeSwap V2: ARATA	792,881.148667287249363262	15.8576%	\$1,197,250.53	
3	 0x30bbfa548e26adf5d3c49ad84e9dcf2d69ed2ffd	18,249.135267799163946222	0.3650%	\$27,556.19	
4	0x7195b1a01defdaf4b6cbc1791bf5c63b9b54e644	6,585.061823565172344119	0.1317%	\$9,943.44	
5	0x573007927a3e1fb8f3ac778f3f766d8ef993bca0	6,528.0350650160914616	0.1306%	\$9,857.33	
6	0xbcd69ce8027b930c7712290f4f0c1e8864382123	4,000	0.0800%	\$6,040.00	
7	0x629f0cb1f77cbd39509febab56a56a120aa2020b	3,953.858964445296877071	0.0791%	\$5,970.33	
8	0x326a8b9f07d13f241546ba3e26f21dea63bca02b	3,801.6	0.0760%	\$5,740.42	
9	 0xbc80cbce3560ca1c88baf802e29be71552cb3038	3,631.393926025531411047	0.0726%	\$5,483.40	
10	0xe2191c8672df678770a1572c10a35dc6c87e177b	2,671.61918776370425446	0.0534%	\$4,034.14	

source:<https://bscscan.com/>



SECURITY ASSESSMENT

SECURITY ISSUES



✓ Critical Severity Issues
No high severity issues found.

✓ High Severity Issues
No high severity issues found.

✓ Medium Severity Issues
No high severity issues found.

⚠ Low Severity Issues
1. Using SafeMath in Solidity \geq 0.8.0 Starting solidity version 0.8.0 arithmetic operations revert on underflow and overflow. There's no more need to assert the result of operations.

Contracts: Arata.sol

Recommendation: Please avoid using assert for arithmetic operations.

2. A public function that could be declared external. public functions that are never called by the contract should be declared external to save gas.

Contracts: Arata.sol

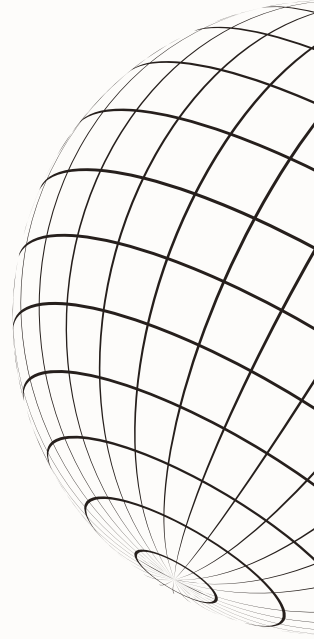
Functions: EnableAllFees, SetSellTax, SetBuyTax, SetMiningAddress, setAutomatedMarketMakerPair, BlackListAddress, IsBlackListed

Recommendation: Use the external attribute for functions never called from the contract.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

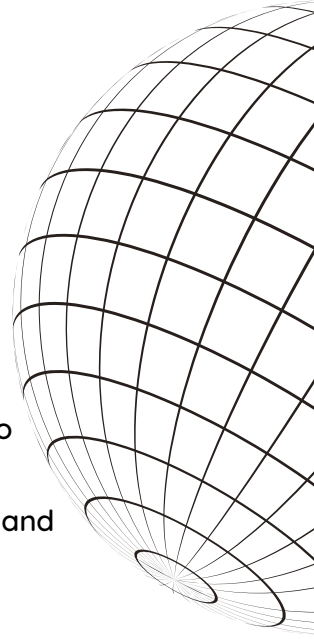
SECURITY ASSESMENT TOKEN LOGO



SECURITY ASSESMENT CONCLUSION

Smart contracts contain owner privileges!

Motech Audit note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT