checkdot

AUDIT COMPANY

GATECH

Agata

SMART CONTRACT SECURITY AUDIT

September

2023

CheckDot

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 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 CheckDot and its affiliates (including CheckDot verifiers, shareholders, employees, directors, officers and other representatives) owe no duty of care towards you or any other person, nor does CheckDot 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 CheckDot 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, CheckDot hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against CheckDot, 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.

Background

CheckDot was commissioned by Agatech to perform an audit of smart contracts:

Mainnet Deployed Contract:
https://bscscan.com/token/0xb427e47e8fdd678278d2a91eeac014ffcddaf029

Github Repository: https://github.com/AgaTechSystems/Agata

Github Repository Commit Hash: b6800a37bfa7cbac0133300e156a765ea9a1860d

Website: https://agatech.io

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.

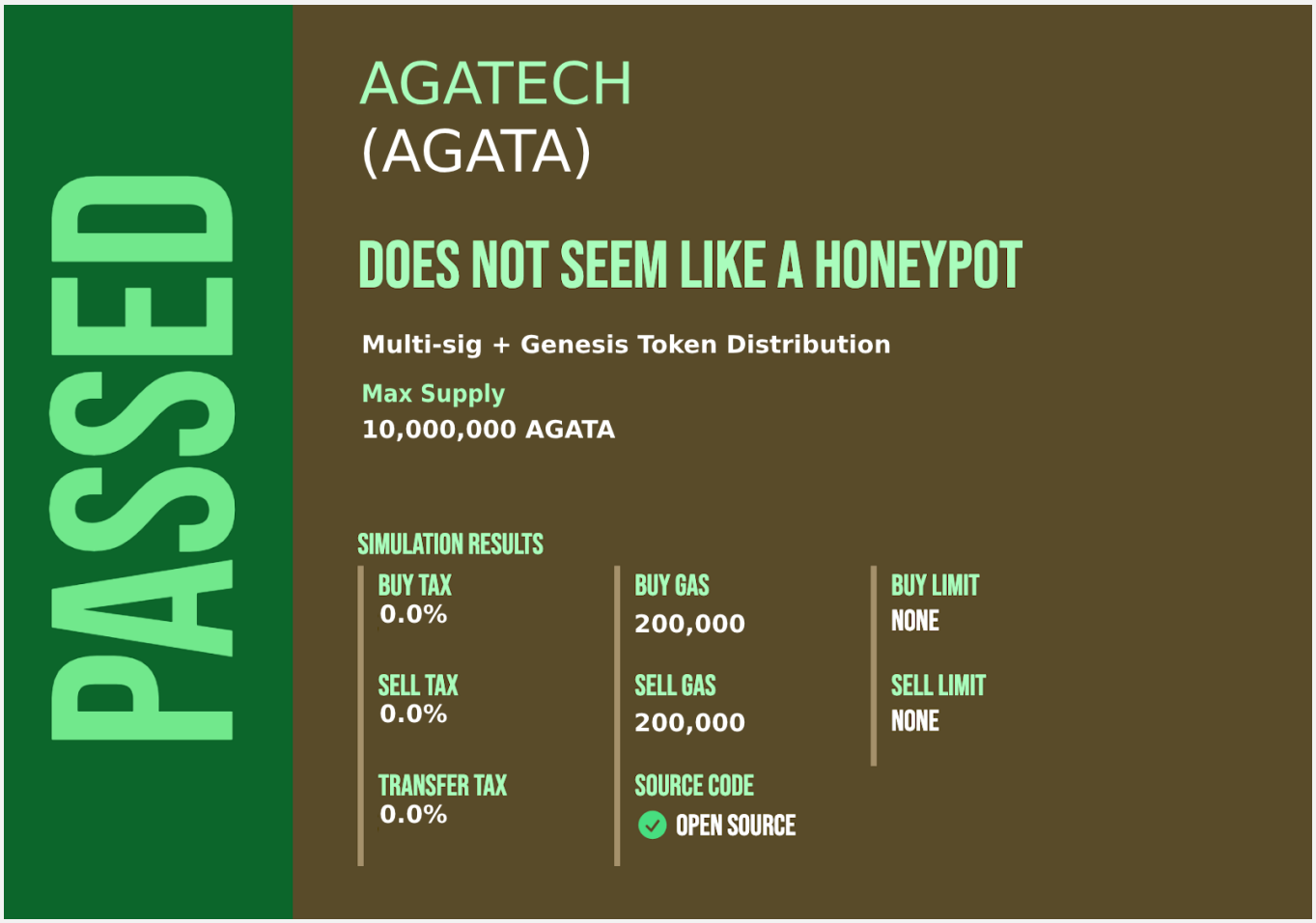
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed
22	Fees detection	Passed

SMART CONTRACT AUDIT

Contract Overview



Source code Verified on BSCscan.
0% Buy Internal Tax.
0% Sell Internal Tax.
No Buy Limit.
No Sell Limit.

Issues Categories

Total: [0 High, 0 Medium, 0 Low]

High Severity Issues

1. No issues.

Medium Severity Issues

1. No issues.

Low Severity Issues

1. No issues.

Token Distribution

The token distribution process in this ERC-20 token smart contract is a crucial component that allocates the initial supply of 10,000,000 AGATA tokens to various wallets in accordance with predefined tokenomics. This distribution is a recommended practice applied by the project to fulfill various purposes, including liquidity provision, team incentives, development, platform enhancements, strategic partnerships, reserves, and initiatives.

The distribution is executed within the contract's constructor function and is designed to ensure transparency, security, and adherence to the specified allocation percentages. Below, we provide an overview of the key wallets involved in the token distribution and the corresponding percentage allocations:

1. 40% (4,000,000) **Agatech Multisig Wallet** (AgatechMultisig): This wallet is designated as the main multisig wallet for Agatech and receives 40% of the total supply, ensuring a significant portion of tokens for governance and operational needs.
2. 10% (1,000,000) **Team Vesting Wallet** (teamVestingWallet): A wallet dedicated to team members, receiving 10% of the total supply to incentivize long-term commitment and align interests with project success.
3. 10% (1,000,000) **Development Fund Wallet** (developmentFundWallet): This wallet, allocated 10% of the total supply, is intended to support project development and growth.
4. 20% (2,000,000) **Platform and Features Development Wallet** (platformsFeaturesWallet): With 20% of the total supply, this wallet focuses on financing platform enhancements and feature development.
5. 5% (500,000) **Strategic Alliances Wallet** (strategicAlliancesWallet): Reserved for strategic partnerships, this wallet receives 5% of the total supply to foster collaborative initiatives.
6. 5% (500,000) **Treasury Reserves Wallet** (treasuryReservesWallet): A wallet holding 5% of the total supply, serving as a reserve for financial stability and future endeavors.
7. 5% (500,000) **AgaPaid Initiative Wallet** (agaPaidInitiativeWallet): Dedicated to the AgaPaid initiative, this wallet receives 5% of the total supply to support specific project initiatives.
8. 5% (500,000) **Deployer Wallet** (deployerWallet): Dedicated to the Deployer, this wallet receives 5% of the total supply to support specific project launch initiatives like creating pools of liquidity.

Owner's possibilities

executeTransaction

Within the context of this ERC-20 token smart contract, the executeTransaction function serves as a powerful tool exclusively accessible to the contract owner. This function empowers the contract owner to execute a range of operations on the Ethereum blockchain, thereby facilitating essential governance and operational tasks.

Key Capabilities:

1. **Execution of Transactions to Other Contracts**: The ***executeTransaction*** function enables the contract owner to interact with external smart contracts on the Ethereum blockchain. By specifying the target contract's address, the amount of Ether to be transferred alongside the transaction, and the relevant data corresponding to the target contract's function, the owner can trigger the execution of transactions to the specified contract.
2. **Funds Transfer**: Through the ***executeTransaction*** function, the owner can seamlessly transfer Ether to other contracts or Ethereum addresses. This functionality is invaluable for making payments, token distributions, and conducting financial operations securely.
3. **Interaction with External Smart Contracts**: The function allows for the inclusion of specific data tailored to the function being called in external smart contracts. This empowers the owner to initiate precise actions in other contracts, such as token transfers, parameter adjustments, or any other functions exposed by those contracts.

4. **Governance Control**: The ***executeTransaction*** function plays a pivotal role in a multisig governance framework, ensuring that the contract owner(s) can propose and execute transactions only after obtaining consensus from other authorized parties, as required.
5. **Transaction Logging**: Upon successful execution of a transaction using this function, an ExecutedTransaction event is generated. This event maintains a comprehensive record of executed transactions, ensuring transparency and providing an immutable historical record of actions taken by the contract owner.

Security Considerations:

The ***executeTransaction*** function is rigorously secured by a robust access control mechanism that restricts interaction exclusively to the contract owner. This stringent restriction ensures that only authorized individuals, typically the contract's creator or designated owner, can initiate transactions through this function. As such, the security and integrity of the ERC-20 token smart contract are effectively safeguarded against unauthorized access and malicious actions. Also this function cannot be used to modify the contract.

Conclusion

After a comprehensive review of the smart contract's code and its various components, it is reassuring to note that the contract exhibits several key security attributes. The codebase is well-structured, well-commented, and boasts a high degree of clarity, making it easily understandable and maintainable.

Robust Access Control and Authorization

One notable security feature is the robust access control mechanism, which ensures that only the contract owner has the privilege to interact with critical functions, such as the token distribution. This stringent authorization layer serves as a crucial defense against potential unauthorized access and malicious actions, effectively safeguarding the contract's integrity and the tokens it manages.

Transparent Token Distribution

The token distribution process is transparent and meticulously documented within the constructor function. The allocation percentages and the associated wallet addresses are clearly visible, providing transparency and accountability regarding how the initial supply of 10,000,000 AGATA tokens is distributed among various purposes. Additionally, the emission of Transfer events during distribution further enhances transparency by creating an immutable ledger of token transfers.

Fee-Free Model

It is noteworthy that the smart contract operates on a fee-free model, as no fees or charges are associated with its functions. This simplicity aligns with the project's objective of ensuring a straightforward and cost-effective user experience.

In summary, the security level of this smart contract appears solid, with well-defined access controls, transparent token distribution and a clear, no-fee model. No vulnerabilities or issues were identified during our review. However, it is important to emphasize that code audits and security assessments should be an ongoing practice to adapt to evolving threats and maintain the long-term security of the contract. In addition, we had already discussed with this team to advise them on the best practices that were applied here, which led to a better finding.

Overall, the smart contract demonstrates a commendable commitment to security, transparency and usability, providing a solid foundation for the intended use in the deployment and management of AGATA tokens.

CheckDot 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.