



Smart Contract Security Audit

Audit details:

Audited project:	GaiaDAO
Deployer address:	0x4ca942531b2b34b5e898c3395c3144434fb6fe3a
Client contacts:	GaiaDAO team
Blockchain:	Binance Smart Chain
Project website:	https://gaiadao.org

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

TechRate was commissioned by GaiaDAO to perform an audit of smart contracts:

- <https://www.bscscan.com/address/0x25Be9E26Db60B1A3d1f7fa21679385dF076Af7FB#code>

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.

Contracts details

Token contract details for 05.05.2021.

Contract name:	GaiaDAO
Contract address:	0x25Be9E26Db60B1A3d1f7fa21679385dF076Af7FB
Total supply:	98_262_300_552_756_587
Token ticker:	GAIA
Decimals:	9
Token holders:	1556
Transactions count:	14263
Top 100 holders dominance:	91.88 %
Liquidity fee:	1
Burn fee:	1
Reflection fee:	1
Donation fee:	2
Tax fee:	4
Total fees:	1_737_699_447_243_413
Uniswap V2 pair:	0x93d4539af567ead92f0bc8223bbfce0cd5bf57a9
Contract deployer address:	0x4ca942531b2b34b5e898c3395c3144434fb6fe3a
Contract's current owner address:	0x4ca942531b2b34b5e898c3395c3144434fb6fe3a

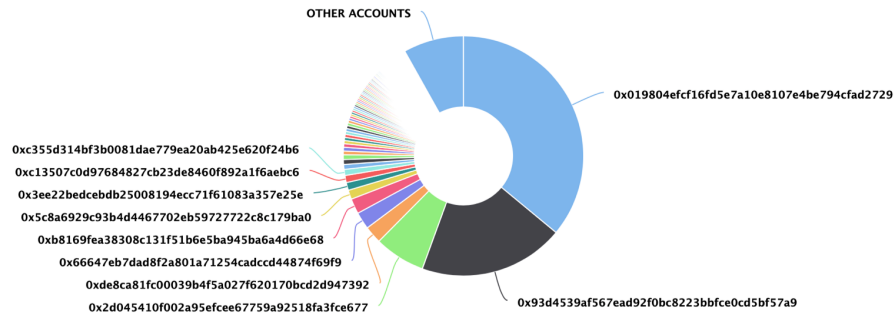
GaiaDAO token distribution

The top 100 holders collectively own 91.88% (90,281,073.98 Tokens) of Gaia

Token Total Supply: 98,262,300.55 Token | Total Token Holders: 1,556

Gaia Top 100 Token Holders

Source: BscScan.com

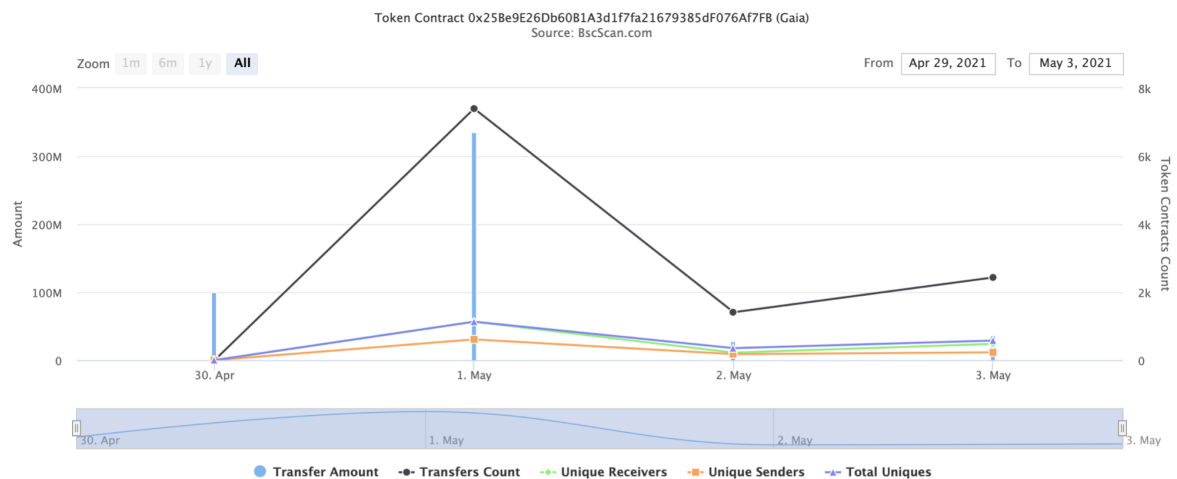


(A total of 90,281,073.98 tokens held by the top 100 accounts from the total supply of 98,262,300.55 token)





GaiaDAO contract interaction details

Time Series: Token Contract Overview



Fri 30, Apr 2021 - Mon 3, May 2021



GaiaDAO top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	 0x019804efcf16fd5e7a10e8107e4be794cfad2729	35,389,649.611772538	36.0155%
2	 0x93d4539af567ead92f0bc8223bbfce0cd5bf57a9	19,213,487.268042722	19.5533%
3	 0x2d045410f002a95efcee67759a92518fa3fce677	6,752,889.606667937	6.8723%
4	0xde8ca81fc00039b4f5a027f620170bcd2d947392	2,300,896.521871147	2.3416%
5	 0x66647eb7dad8f2a801a71254cadccd44874f69f9	2,267,549.684993002	2.3076%
6	0xb8169fea38308c131f51b6e5ba945ba6a4d66e68	2,028,411.622134975	2.0643%
7	0x5c8a6929c93b4d4467702eb59727722c8c179ba0	1,221,279.963677601	1.2429%
8	0x3ee22bedcebdb25008194ecc71f61083a357e25e	1,022,991.777538182	1.0411%
9	0xc13507c0d97684827cb23de8460f892a1f6aebc6	943,419.749024794	0.9601%
10	0xc355d314bf3b0081dae779ea20ab425e620f24b6	801,626.38267213	0.8158%

GaiaDAO LP token holders

Rank	Address	Quantity	Percentage
1	 0xf488afd05d150317de66e62db0597244cfbfe6f1	2.300276266981459207	94.5677%
2	0x4ca942531b2b34b5e898c3395c3144434fb6fe3a	0.11102187775566668	4.5643%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	0.021113427724495952	0.8680%
4	0x7180aa7488ee9b15bf8596bb25447eb45f64bb02	0.000000130815783278	0.0000%
5	 0x00	0.0000000000000001	0.0000%

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.	Low issues
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

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Out of gas

Issue:

- ❑ The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeInReward(address account↑) external onlyOwner() {
    require(!_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- ❑ The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Use `EnumerableSet` instead of array or do not use long arrays.

Owner privileges

- ☐ Owner can change the liquidity, tax, reflection, burn and donation fee.
- ☐ Owner can change the maximum transaction amount.
- ☐ Owner can exclude from the fee.
- ☐ Owner can change the charity address.

Conclusion

Smart contracts contain low severity issues and owner privileges! Liquidity pair contract is not checked.

DXSale locking details provided by the team can be found by this link - <https://dxsale.app/app/pages/dxlockview?id=2&add=0x7180aa7488eE9B15bf8596Bb25447Eb45f64BB02&type=tokenlock&chain=BSC>

Presale info details provided by the team can be found by this link - <https://dxsale.app/app/pages/defipresale?saleID=173&chain=BSC>

Techrate 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.