



Smart Contract Security Audit

Audit details:

Audited project:	OctaX
Deployer address	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Blockchain:	Binance Smart Chain
Project website:	http://www.octax.finance

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 OctaX to perform an audit of smart contracts:

- <https://bscscan.com/address/0x2518243517C90C7598c4EA51a1321cA7E503cDef#code>
- <https://bscscan.com/address/0x174BE9fBcc00D93A3d447Bc01d0918EbB7F17bA6#code>
- <https://bscscan.com/address/0x4F1498da0f50F94e97F900b7e6E13d8e5220aBE9#code>
- <https://bscscan.com/address/0x39cab1DdaFDa34B9202F5a41f71B15d2F3EbA2aC#code>
- <https://bscscan.com/address/0xEddFB54d3d849A397FD226765775Bc90ce118e3B#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.

Octa Gold contracts details

Token contract details for 10.05.2021.

Contract name:	OctaGold
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x4F1498da0f50F94e97F900b7e6E13d8e5220aBE9
Total supply:	888888000000000000000000
Token ticker:	OCTAG
Decimals:	18
Token holders:	3607
Transactions count:	5566
Top 100 dominance:	100 %
Contract deployer address:	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Contract's current owner address:	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695

OctaX contracts details

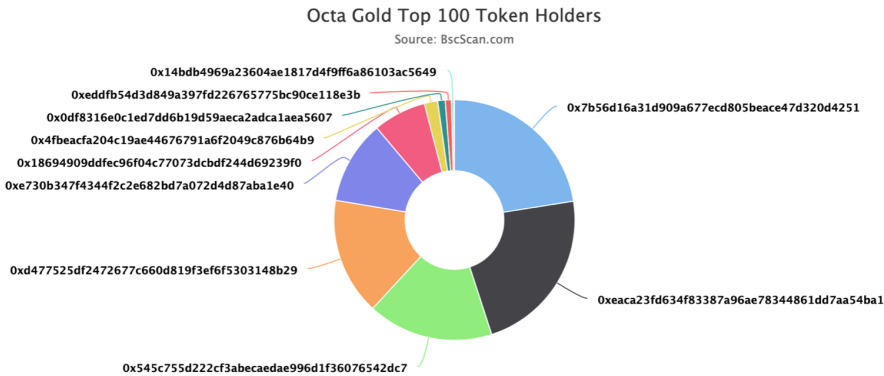
Token contract details for 10.05.2021.

Contract name:	OctaX
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x39cab1DdaFDa34B9202F5a41f71B15d2F3EbA2aC
Total supply:	39808116279513721172180
Token ticker:	OCTAX
Decimals:	18
Token holders:	3353
Transactions count:	33695
Top 100 dominance:	99.83 %
Contract deployer address:	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Contract's current owner address:	0xeddfb54d3d849a397fd226765775bc90ce118e3b

Octa Gold token distribution




The top 100 holders collectively own 100.00% (888,887.22 Tokens) of Octa Gold

Token Total Supply: 888,888.00 Token | Total Token Holders: 3,607



(A total of 888,887.22 tokens held by the top 100 accounts from the total supply of 888,888.00 token)

Octa Gold top 10 token holders

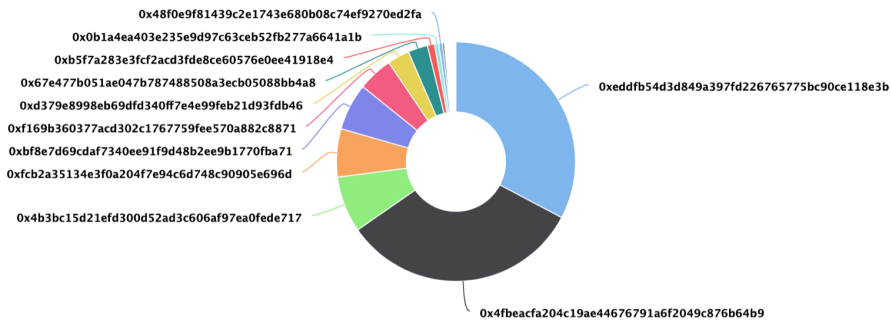
Rank	Address	Quantity (Token)	Percentage
1	0x7b56d16a31d909a677ecd805beace47d320d4251	200,000	22.5000%
2	0xeaca23fd634f83387a96ae78344861dd7aa54ba1	200,000	22.5000%
3	0x545c755d222cf3abecaedae996d1f36076542dc7	150,000	16.8750%
4	0xd477525df2472677c660d819f3ef6f5303148b29	140,000	15.7500%
5	0xe730b347f4344f2c2e682bd7a072d4d87aba1e40	100,000	11.2500%
6	0x18694909ddfec96f04c77073dcbdf244d69239f0	63,203	7.1103%
7	 0x4fbeacfa204c19ae44676791a6f2049c876b64b9	15,824.333271943409800839	1.7802%
8	0x0df8316e0c1ed7dd6b19d59aeca2adca1aea5607	9,000	1.0125%
9	 0xeddfb54d3d849a397fd226765775bc90ce118e3b	7,224.908275990494460617	0.8128%
10	 0x14bdb4969a23604ae1817d4f9ff6a86103ac5649	3,121.976369594481391028	0.3512%

OctaX token distribution

The top 100 holders collectively own 99.83% (39,739.83 Tokens) of OctaX

Token Total Supply: 39,808.12 Token | Total Token Holders: 3,353

OctaX Top 100 Token Holders
Source: BscScan.com



(A total of 39,739.83 tokens held by the top 100 accounts from the total supply of 39,808.12 token)

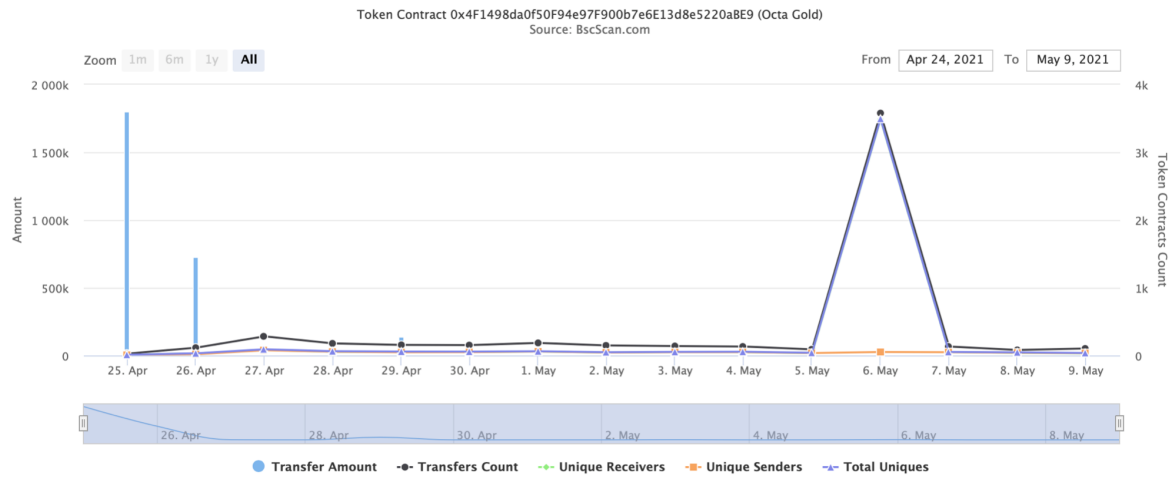
OctaX top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0xeddfb54d3d849a397fd226765775bc90ce118e3b	13,031.908262013808805309	32.7368%
2	0x4fbeacfa204c19ae44676791a6f2049c876b64b9	12,984.905460243469774529	32.6187%
3	0x4b3bc15d21efd300d52ad3c606af97ea0fede717	3,018.517414454275611553	7.5827%
4	0xfcb2a35134e3f0a204f7e94c6d748c90905e696d	2,588.553496091932145563	6.5026%
5	0xbf8e7d69cdf7340ee91f9d48b2ee9b1770fba71	2,523.609064813193963219	6.3394%
6	0xf169b360377acd302c1767759fee570a882c8871	1,879.59458035146484085	4.7216%
7	0xd379e8998eb69dfd340ff7e4e99feb21d93fdb46	1,195.283298137611013614	3.0026%
8	0x67e477b051ae047b787488508a3ecb05088bb4a8	1,053.35458454936853792	2.6461%
9	0xb5f7a283e3fc2acd3fde8ce60576e0ee41918e4	384.824099317868214454	0.9667%
10	0x0b1a4ea403e235e9d97c63ceb52fb277a6641a1b	230.559465770839870549	0.5792%

Octa Gold transactions

Time Series: Token Contract Overview

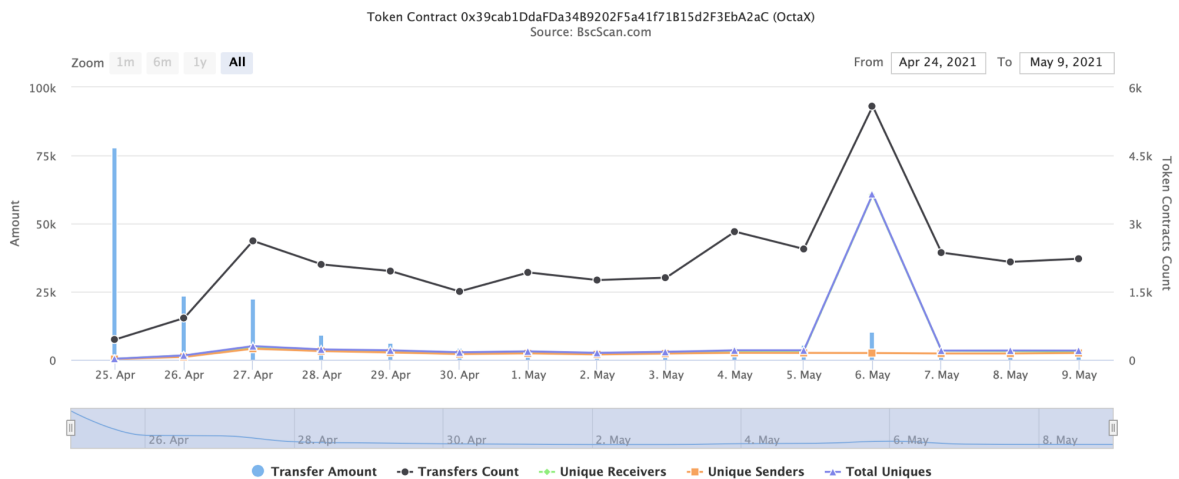
Sun 25, Apr 2021 - Sun 9, May 2021



OctaX transactions

Time Series: Token Contract Overview

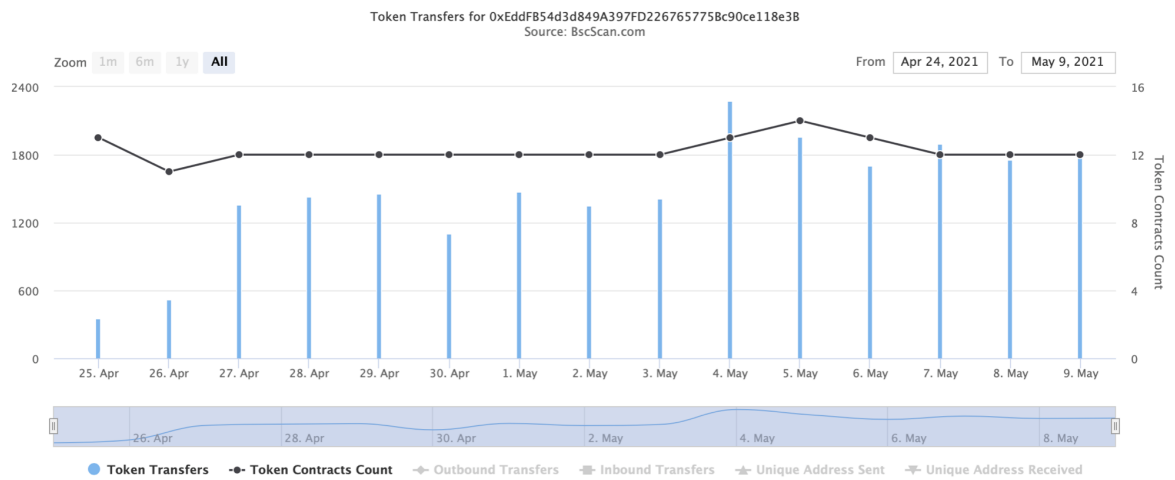
Sun 25, Apr 2021 - Sun 9, May 2021



Masterchef transactions

Time Series: Address Token (BEP-20) Transfers

Sun 25, Apr 2021 - Sun 9, May 2021



Pro-Tip: Click on the chart data points to view more

MasterChef contract details for 10.05.2021.

Contract name:	MasterChef
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xEddFB54d3d849A397FD226765775Bc90ce118e3B
Deployer address:	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Dev address:	0xd379e8998eb69dfd340ff7e4e99feb21d93fdb46
Burn address:	0xb5f7a283e3fcf2acd3fde8ce60576e0ee41918e4
OctaX contract address:	0x39cab1ddafda34b9202f5a41f71b15d2f3eba2ac
OctaX per block:	14000000000000000
Contract owner address:	0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Pool length:	14
Start block:	6861909
Total alloc point:	7910
Bonus multiplier:	1

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. Block gas limit

Issue:

The `updateEmissionRate` function can fail due to block gas limit if the pool size is too big.

Owner privileges

- ❑ Owner can change the burn address.
- ❑ Owner can change the lock day for withdrawals, this could be risky, if the owner will set the big number, then users will not be able to withdraw their funds for a long period of time.

We recommend removing the lock time checking in emergency withdraw function, so users will be able to withdraw their funds without rewards any time they want!

- ❑ Owner can change the owner of the OctaX token through the MasterChef contract, but the owner of the OctaX token should be only the MasterChef contract.

Conclusion

Smart contracts contain low severity issues and owner privileges! Audited only the smart contracts listed above, LP-pair contracts and the other contracts of the project are not audited.

MasterChef contract differs from the GooseDefi fork and has time lock for withdrawals and emergency withdrawals, so users should be notified about the withdrawal time locks and check that carefully.

As mentioned above, we recommend removing the lock time checking in the emergency withdraw function!

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.