Smart Contract Security Audit

Audit details:

Audited project:	Vangold
Deployer address	0x0a2aa1610e4295d1ee7b1da2f08ba210fa6e56bf
Client contacts:	@vgd_admin
Blockchain:	Binance Smart Chain
Project website:	https://www.vangold.finance

April, 2021
TechRate

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 Vangold to perform an audit of smart contracts:

- *https://bscscan.com/address/0xfd91fa8fab5ca11569e256fa8844bc2abecc331d#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 08.04.2021.

Contract name:	Vangold
Compiler version:	v0.8.2+commit.661d1103
Contract address:	0xfd91fa8fab5ca11569e256fa8844bc2abecc331d
Total supply:	100_000_000
Token ticker:	VGD
Decimals:	18
Token holders:	4865
Transactions count:	9489
Top 100 holders dominance:	93.39 %
Contract deployer address:	0x0a2aa1610e4295d1ee7b1da2f08ba210fa6e56bf
Contract's current owner address:	0x39b5c42d32ad6bfebcb221cbb06f08aa28b63048
Contract's new owner address, which does not accepted ownership	Zero address, but it will not accept the ownership, so current owner will left as owner of the contract

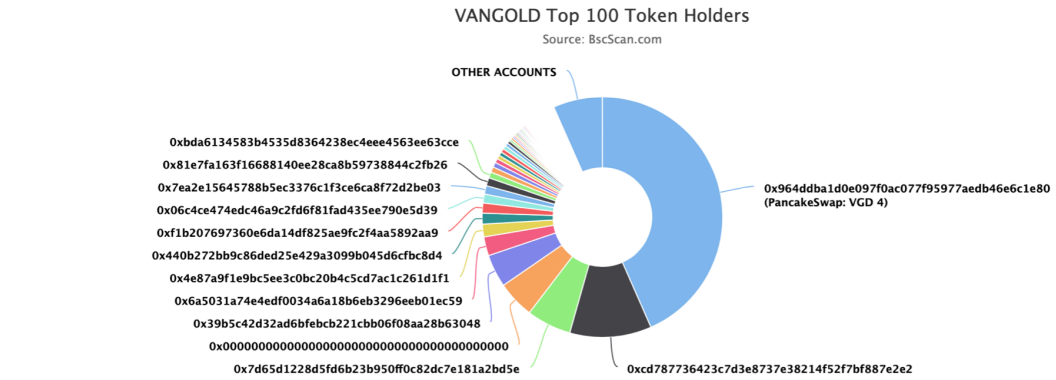
Vangold top 5 token holders

Rank	Address	Quantity	Percentage
1	PancakeSwap: VGD 4	43,402,081.1998857	43.4021%
2	0xcd787736423c7d3e8737e38214f52f7bf887e2e2	11,000,000	11.0000%
3	0x7d65d1228d5fd6b23b950ff0c82dc7e181a2bd5e	6,000,000	6.0000%
4	0x0000000000000000000000000000000000000000	5,000,000	5.0000%
5	0x39b5c42d32ad6bfebcb221cbb06f08aa28b63048	4,410,100	4.4101%

Vangold top 100 token distribution

The top 100 holders collectively own 93.38% (93,378,492.30 Tokens) of VANGOLD

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 4,865

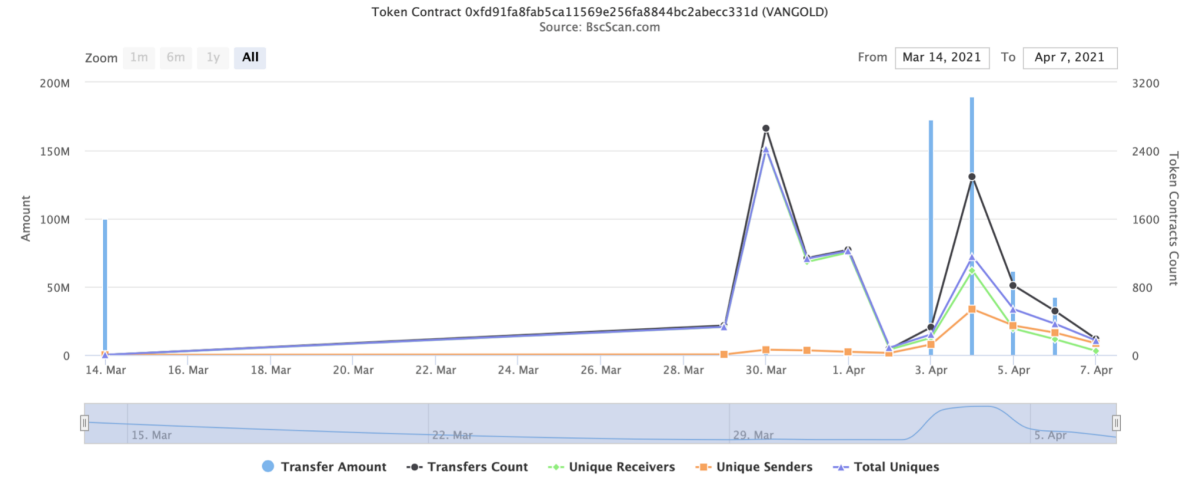


(A total of 93,378,492.30 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

Vangold contract interaction details

Time Series: Token Contract Overview

Sun 14, Mar 2021 - Wed 7, Apr 2021



Contract functions details

Function	Return value	Who can call
transferOwnership(address)	void	owner
acceptOwnership()	void	only new owner, set in function transferOwnership
totalSupply()	uint	public
balanceOf(address)	uint	public
transfer(address, uint)	bool	public
approve(address, uint)	bool	public
transferFrom(address, address, uint)	bool	public
allowance(address, address)	uint	public
approveAndCall(address, uint, bytes)	bool	public
transferAnyERC20Token(address, uint)	bool	owner

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

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Zero address checking

Issue:

There is no zero address checking in the following functions.
transfer:

```
function transfer(address to, uint tokens) public override returns (bool success) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    Transfer(msg.sender, to, tokens);
    return true;
}
```

transferFrom:

```
function transferFrom(address from, address to, uint tokens) public virtual override returns (bool success) {
    balances[from] = safeSub(balances[from], tokens);
    allowed[from][msg.sender] = safeSub(allowed[from][msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    Transfer(from, to, tokens);
    return true;
}
```

Recommendation:

Please add the zero address checking to prevent users from sending their tokens by mistake to the zero address

Conclusion

Smart contract does not contain any high severity issues!

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.