TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project: Env Finance

Deployer address   0x3290458d69788302c7dca753896f3c0a10952368

Client contacts: @Zeppe79

Blockchain: Binance Smart Chain

Project website: https://www.env.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 Env Finance to perform an audit of smart contracts:

- *https://bscscan.com/address/0x4D2b1966F347E48B2d247F684d7677854083 E4AB#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:	Env Finance
Compiler version:	v0.4.24+commit.e67f0147
Contract address:	0x4D2b1966F347E48B2d247F684d7677854083E4AB
Total supply:	12_300_000_000_000_000
Token ticker:	ENV
Decimals:	8
Token holders:	41
Transactions count:	44
Top 100 holders dominance:	100 %
Contract deployer address:	0x3290458d69788302c7dca753896f3c0a10952368
Paused status:	False
Minting finished status:	True
Contract owner address:	0xe0f1dedde3650e8d7a46e413228e25ab21b789c6
Deployed at transaction:	0x50909fc61ef05e8c08abb0a489141922c837d6318424b2046fa8b61448e4a4ea

Env Finance top 5 holders

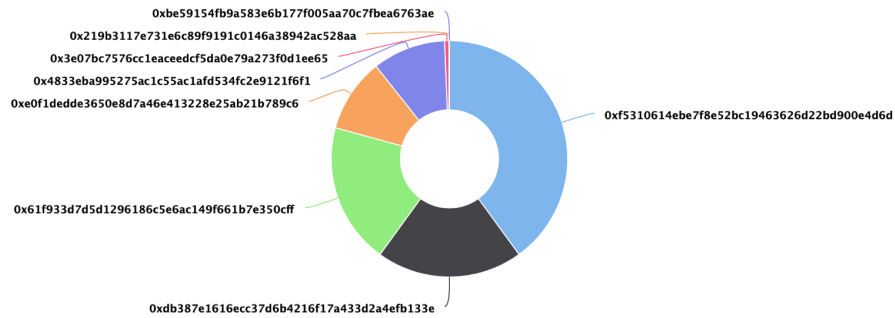| Rank	Address	Quantity	Percentage
1	0xf5310614ebe7f8e52bc19463626d22bd900e4d6d	49,200,000	40.0000%
2	0xdb387e1616ecc37d6b4216f17a433d2a4efb133e	24,600,000	20.0000%
3	0x61f933d7d5d1296186c5e6ac149f661b7e350cff	23,693,000	19.2626%
4	0xe0f1dedde3650e8d7a46e413228e25ab21b789c6	12,404,000	10.0846%
5	0x4833eba995275ac1c55ac1afd534fc2e9121f6f1	12,300,000	10.0000%

Env Finance top 100 token distribution

💡 Token Total Supply: 123,000,000.00 Token | Total Token Holders: 41

ENVFinanceToken Top 100 Token Holders
Source: BscScan.com

- 0xbe59154fb9a583e6b177f005aa70c7fbea6763ae
- 0x219b3117e731e6c89f9191c0146a38942ac528aa
- 0x3e07bc7576cc1eaceedcf5da0e79a273f0d1ee65
- 0x4833eba995275ac1c55ac1afd534fc2e9121f6f1
- 0xe0f1dedde3650e8d7a46e413228e25ab21b789c6
- 0xf5310614ebe7f8e52bc19463626d22bd900e4d6d
- 0x61f933d7d5d1296186c5e6ac149f661b7e350cff
- 0xdb387e1616ecc37d6b4216f17a433d2a4efb133e

(A total of 123,000,000.00 tokens held by the top 100 accounts from the total supply of 123,000,000.00 token)
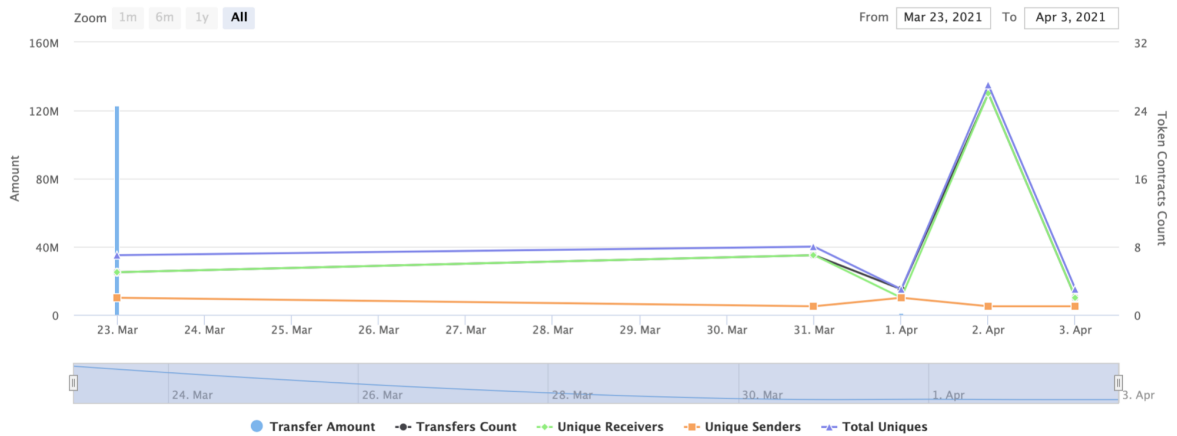
Env Finance contract interaction details

Time Series: Token Contract Overview   Tue 23, Mar 2021 - Sat 3, Apr 2021

Token Contract 0x4D2b1966F347E48B2d247F684d7677854083E4AB (ENVFinanceToken)
Source: BscScan.com

Zoom 1m 6m 1y **All**   From Mar 23, 2021 To Apr 3, 2021

● Transfer Amount   -●- Transfers Count   -+- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

Contract functions details

Function	Return value	Who can call
name()	string	public
symbol()	string	public
decimals()	uint8	public
totalSupply()	uint256	public
balanceOf(address)	uint256	public
transfer(address, uint256)	bool	public
allowance(address, address)	uint256	public
approve(address, uint256)	bool	public
transferfrom(address, address, uint256)	bool	public
increaseAllowance(address, uint256)	bool	public
decreaseAllowance(address, uint256)	bool	public
renounceOwnership()	void	owner
transferOwnership(address)	void	owner
mint(address, uint256)	bool	owner
finishMinting()	bool	owner
actualBalanceOf(address)	uint256	public
freezingBalanceOf(address)	uint256	public
freezingCount(address)	uint	public
freezeTo(address, uint, uin64)	void	public
getFreezing(address, uint)	uint64, uint	public
releaseOnce()	void	public
releaseAll()	uint	public
burn(uint256)	void	public
pause()	void	public
unpause()	void	public
mintAndFreeze(address, uint, uint64)	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. Wrong event

Issue:

There is a wrong Transfer event in function mintAndFreeze.

```solidity
function mintAndFreeze(address _to, uint _amount, uint64 _until) public onlyOwner canMint returns (bool) {
    totalSupply_ = totalSupply_.add(_amount);

    bytes32 currentKey = toKey(_to, _until);
    freezings[currentKey] = freezings[currentKey].add(_amount);
    freezingBalance[_to] = freezingBalance[_to].add(_amount);

    freeze(_to, _until);
    emit Mint(_to, _amount);
    emit Freezed(_to, _until, _amount);
    emit Transfer(msg.sender, _to, _amount);
    return true;
}
```

Recommendation:

There should be a Transfer event from zero address to _to address, because this is minting of tokens, so it should be from zero address.

Owner privileges

1. Owner privileges

❏ Owner can pause the transfers of contract tokens.

```solidity
function pause() onlyOwner whenNotPaused public {
    paused = true;
    emit Pause();
}
```

Conclusion

Smart contracts do not contain any high severity issues! However, smart contracts contain owner privileges.

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.