



Smart Contract Security Audit

Audit details:

Audited project:	Safe Energy
Deployer address:	0x9bb5b05f66edcfbc9cc0c79df75f34ad4b5c953e
Client contacts:	Safe Energy team
Blockchain:	Binance Smart Chain
Project website:	https://www.safeenergy.club

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 Safe Energy to perform an audit of smart contracts:

- <https://bscscan.com/address/0xbbe899c61198d1826a43e20ea19efc46e50c2b00#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 15.05.2021.

Contract name:	Safe Energy
Contract address:	0xbbe899c61198d1826a43e20ea19efc46e50c2b00
Total supply:	91391874828424587857199
Token ticker:	EnergyX
Decimals:	8
Token holders:	569
Transactions count:	1135
Top 100 holders dominance:	94.83 %
Burn fee rate:	500
Tax fee rate:	500
Total fees:	8608125171575412142801
Total burnt:	8608125171575412142801
Contract deployer address:	0x9bb5b05f66edcfbc9cc0c79df75f34ad4b5c953e
Contract's current owner address:	0x000000000000000000000000000000000000dead

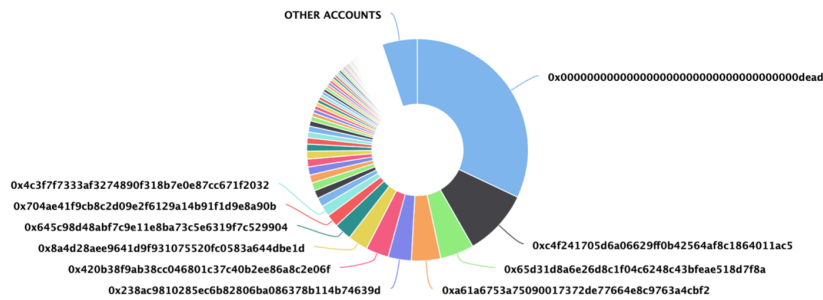
Safe Energy token distribution

💡 The top 100 holders collectively own 94.83% (866,664,049,586,946.00 Tokens) of Safe Energy

💡 Token Total Supply: 913,918,824,633,715.68 Token | Total Token Holders: 569

Safe Energy Top 100 Token Holders

Source: BscScan.com



(A total of 866,664,049,586,946.00 tokens held by the top 100 accounts from the total supply of 913,918,824,633,715.68 token)

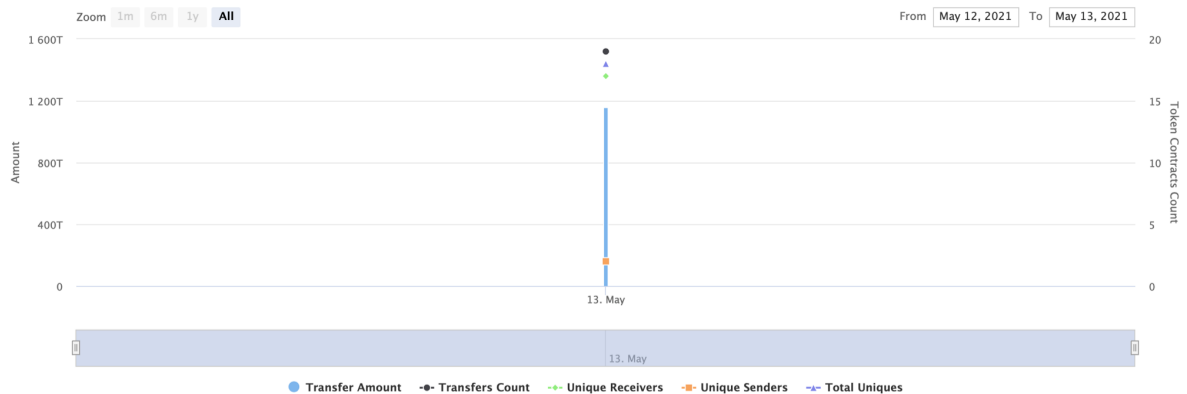
Safe Energy contract interaction details

Time Series: Token Contract Overview


Thu 13, May 2021 - Thu 13, May 2021

Token Contract 0xbbe899c61198d1826a43e20ea19efc46e50c2b00 (Safe Energy)
Source: BscScan.com

Source: BscScan.com



Safe Energy top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x0000000000000000000000000000000000000000dead	292,427,017,915.26370868	31.9970%
2	 0xc4f241705d6a06629ff0b42564af8c1864011ac5	88,645,223,528,009.4826672	9.6995%
3	0x65d31d8a6e26d8c1f04c6248c43bfeae518d7f8a	45,052,682,359,958.02892247	4.9296%
4	0xa61a6753a75090017372de77664e8c9763a4cbf2	38,964,764,659,131.30524926	4.2635%
5	0x238ac9810285ec6b82806ba086378b114b74639d	31,095,699,726,636.54818526	3.4025%
6	0x420b38f9ab38cc046801c37c40b2ee86a8c2e06f	30,301,785,087,684.74783905	3.3156%
7	0x8a4d28aee9641d9f931075520fc0583a644dbe1d	26,762,913,072,589.86098002	2.9284%
8	0x645c98d48abf7c9e11e8ba73c5e6319f7c529904	23,118,852,640,480.52044977	2.5296%
9	0x704ae41f9cb8c2d09e2f6129a14b91f1d9e8a90b	16,844,606,980,079.73689422	1.8431%
10	0x4c3f7f7333af3274890f318b7e0e87cc671f2032	14,657,243,058,817.03845552	1.6038%

Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] _functionCallWithValue #

+ Ownable (Context)

- [Int] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ SafeEnergy (Context, IBEP20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals

- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcluded
- [Pub] totalFees
- [Pub] totalBurn
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
 - modifiers: onlyOwner
- [Ext] includeAccount #
 - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _getTaxFee
- [Ext] _setTaxFee #
 - modifiers: onlyOwner
- [Ext] _setBurnFee #
 - modifiers: onlyOwner
- [Prv] _getMaxTxAmount

(\$) = payable function

= non-constant function

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 `includeAccount` 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 includeAccount(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:

Check that the excluded array list is not too big.

Conclusion

Smart contracts do not contain high severity issues!

Ownership renounced tx -

<https://bscscan.com/tx/0x50522b3fbd97937e6ea732e440a8ca50b8f381479c9d1c715c1261063c9e584f>

Liquidity locking details provided by the team -

<https://dxsale.app/app/pages/dxlockview?id=0&add=0x9bb5B05F66edCFbC9CC0c79Df75F34Ad4B5c953e&type=lplock&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.