



SMART CONTRACT SECURITY AUDIT

SEKUDEX
AUGUST 2021



Sekudex was commissioned by ElonTech to perform an audit of smart contracts:

<https://bscscan.com/address/0xbb58f5c1c7521f6-da845b76c75081505254377d7#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.

AUDIT DETAILS

Audited Project

ElonTech

Contract

0xc66c8b40e9712708d0b4f27c9775dc934b65f0d9

Blockchain

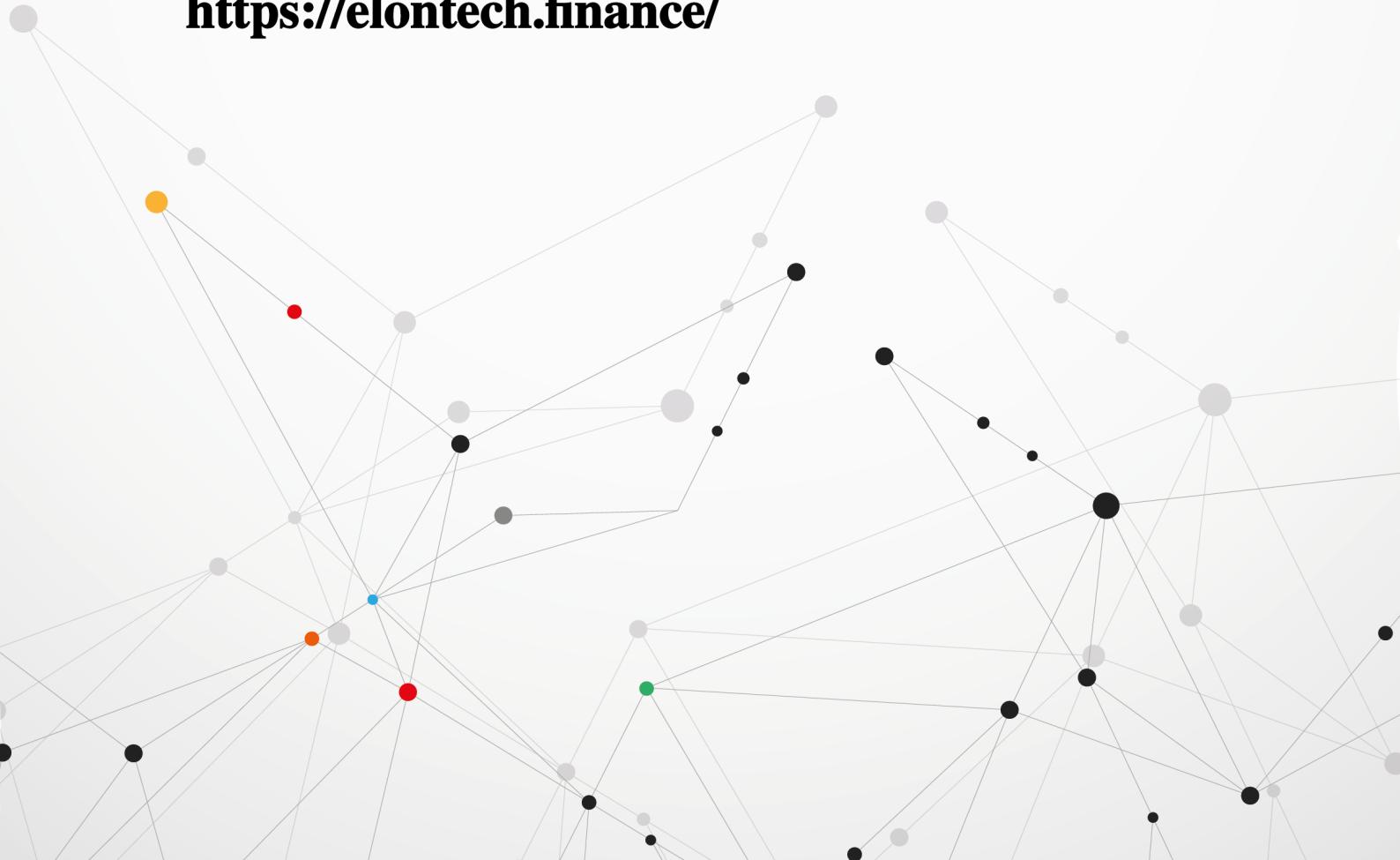
Binance Smart Chain

Deployer Adress

0x82B9F1dCBF5e62d79ae22775A7657568E1403782

Project Website

<https://elontech.finance/>



CONTRACT DETAILS

Contract Name	ElonTech
Contract Adress	0xC66c8b40E9712708d0b4F27c9775Dc934B65F0d9
Total Supply	34,979,803,438,049.375
Decimals	18
Token Ticker	ETCH
Holders	9516
Transactions	57450
Top 100 holders dominance	99,91
Minting finished	TRUE
Contract's current Owner address	0x3b73405bfaa9eda4d3971590c475148d2551a443
Contract deployer adress	0x82B9F1dCBF5e62d79ae22775A7657568E1403782

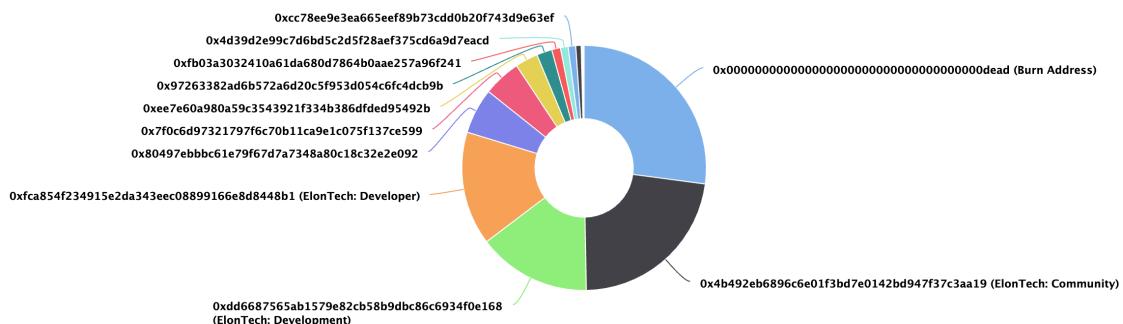
TOKEN DISTRIBUTION

The top 100 holders collectively own 99.91% (34,946,969,039,286.40 Tokens) of ElonTech

Token Total Supply: 34,979,803,438,049.38 Token | Total Token Holders: 9,516

ElonTech Top 100 Token Holders

Source: BscScan.com

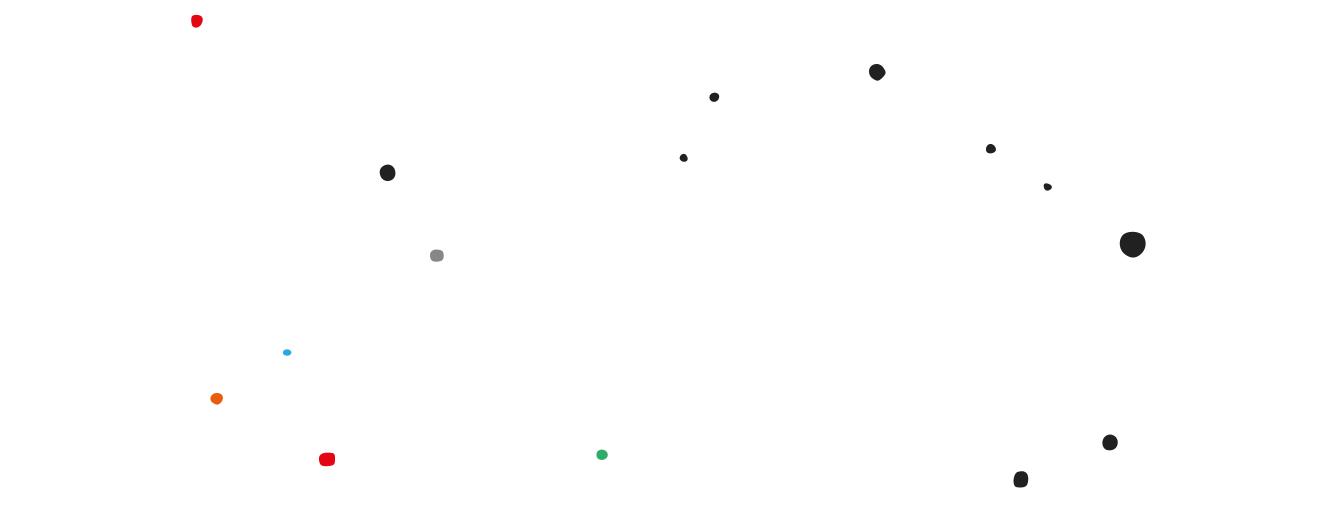
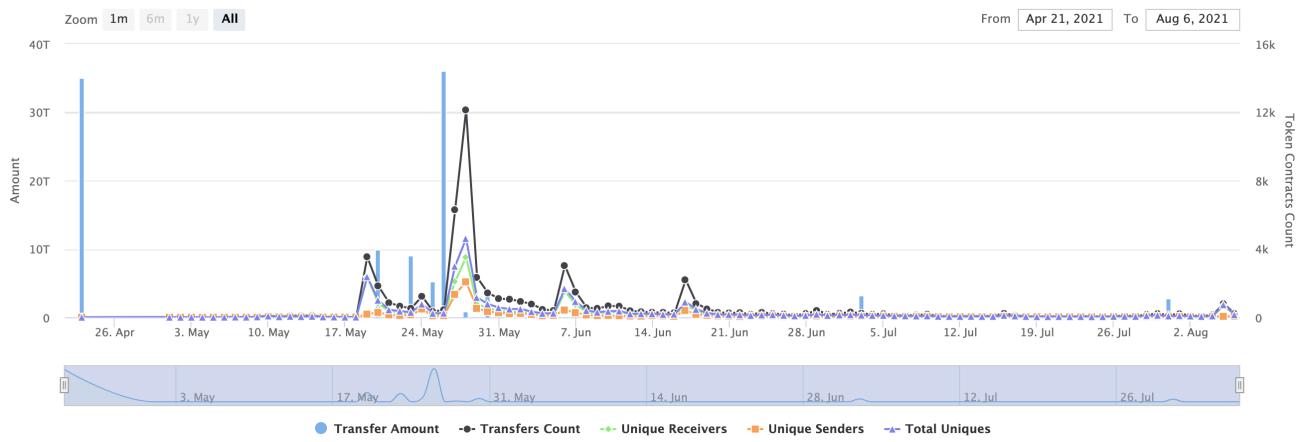


(A total of 34,946,969,039,286.40 tokens held by the top 100 accounts from the total supply of 34,979,803,438,049.38 token)

CONTRACT INTERACTIONS DETAILS

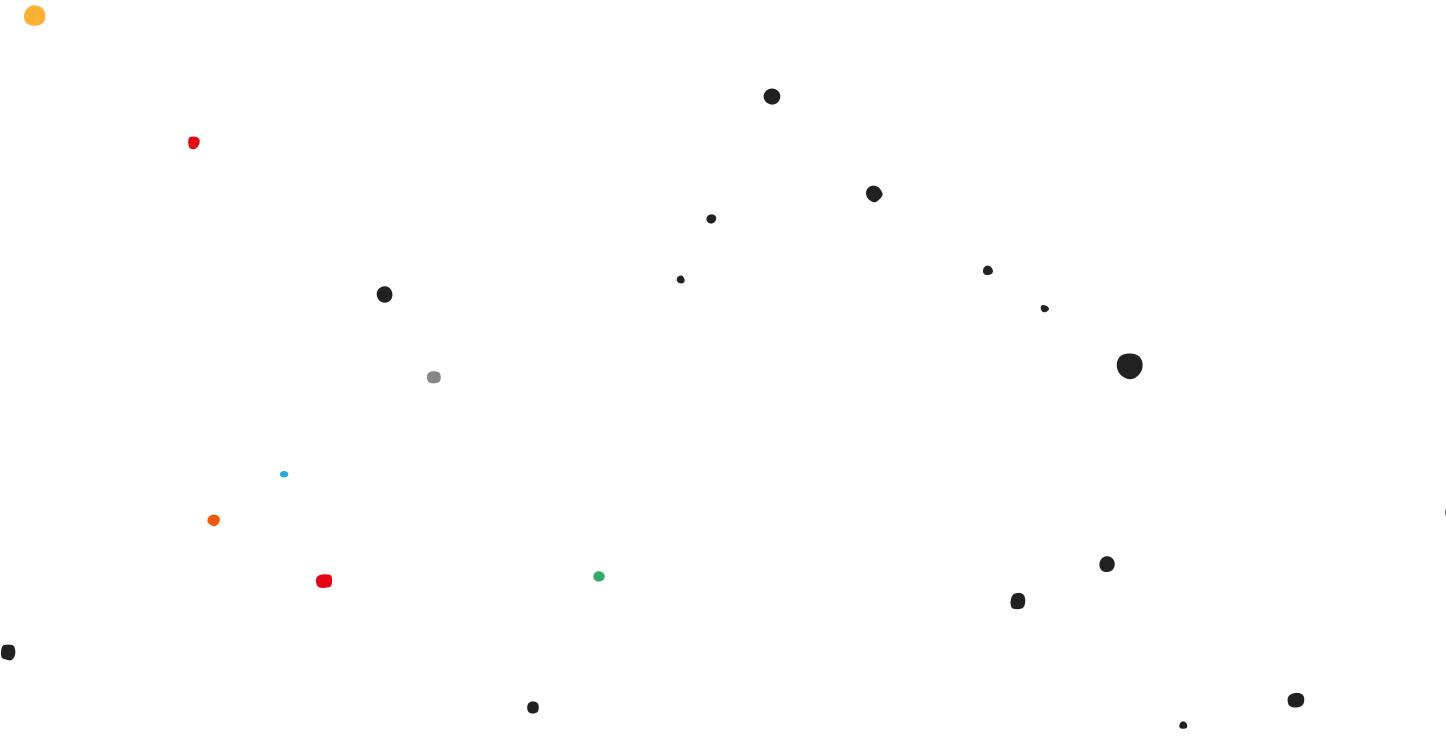
Token Contract 0xc66c8b40e9712708d0b4f27c9775dc934b65f0d9 (ElonTech)

Source: BscScan.com

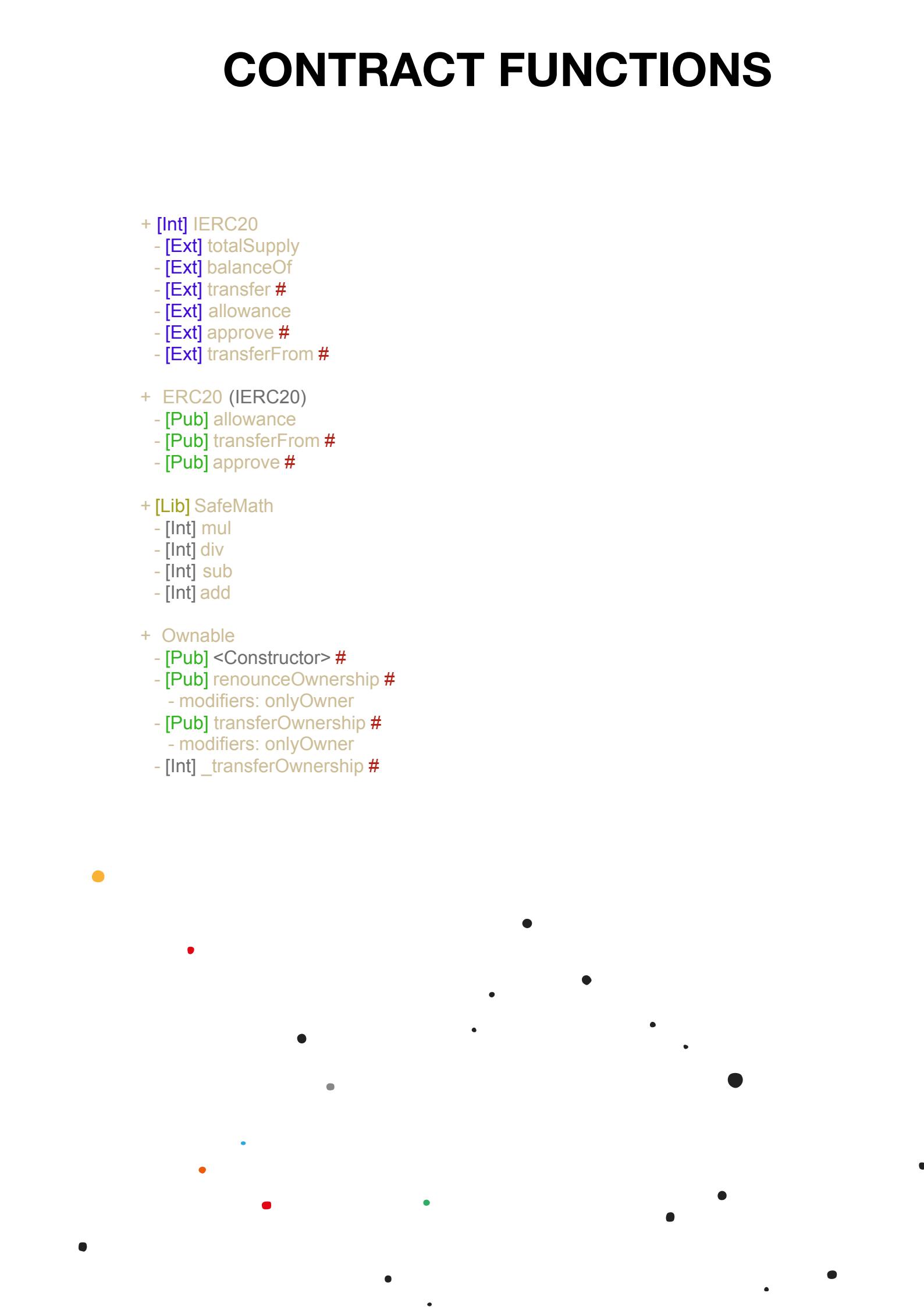


TOP 15 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	Burn Address	9,479,527,631,711.3375	27.1000%	\$62,653,041.98	
2	ElonTech: Community	7,908,854,616,839.566251766655706185	22.6098%	\$52,271,992.82	
3	ElonTech: Development	5,246,970,515,707.406	15.0000%	\$34,678,802.23	
4	ElonTech: Developer	5,246,970,515,707.406	15.0000%	\$34,678,802.23	
5	0x80497ebbbc61e79f67d7a7348a80c18c32e2e092	2,098,788,206,282.9625	6.0000%	\$13,871,520.89	
6	0x7f0c6d97321797f6c70b11ca9e1c075f137ce599	1,746,836,424,132.675848892184782736	4.9938%	\$11,545,365.98	
7	0xee7e60a980a59c3543921f334b386dfded95492b	1,049,394,103,141.48125	3.0000%	\$6,935,760.45	
8	0x97263382ad6b572a6d20c5f953d054c6fc4dc9b	716,109,915,863.89850387494850433	2.0472%	\$4,732,985.27	
9	0xfb03a3032410a61da680d7864b0aae257a96f241	400,000,000,000	1.1435%	\$2,643,720.00	
10	0x4d39d2e99c7d6bd5c2d5f28aef375cd6a9d7eadc	355,170,637,135.864216303119143965	1.0154%	\$2,347,429.29	
11	0xcc78ee9e3ea665eef89b73cdd0b20f743d9e63ef	349,798,034,380.49375	1.0000%	\$2,311,920.15	
12	0x3b73405bfaa9eda4d3971590c475148d2551a443	248,855,646,528.125389063439638699	0.7114%	\$1,644,761.62	
13	0xb215a1e8be096c99d6bbdbdec2260eed7a67a16a	58,999,257,528.23336034	0.1687%	\$389,943.79	
14	0x7660c696b8e3db40ed973aa3aab8928c9776b9	5,000,000,000	0.0143%	\$33,046.50	
15	0x5782af893473e5b9bc8bdb6af3e6fe12ae95b405	3,001,761,278.410352282176959929	0.0086%	\$19,839.54	



CONTRACT FUNCTIONS

- + [Int] IERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
 - + ERC20 (IERC20)
 - [Pub] allowance
 - [Pub] transferFrom #
 - [Pub] approve #
 - + [Lib] SafeMath
 - [Int] mul
 - [Int] div
 - [Int] sub
 - [Int] add
 - + Ownable
 - [Pub] <Constructor> #
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- 
- The background of the slide features a minimalist abstract design consisting of numerous small, semi-transparent colored dots scattered across the white space. These dots are in various colors including yellow, red, green, blue, and black, creating a subtle, organic pattern.

CONTRACT FUNCTIONS

- + BasicToken (IERC20, Ownable)
 - [Pub] __AllowTokenTransfer #
 - modifiers:
 - onlyOwner
 - [Pub] totalSupply
 - [Pub] totalSupplyCheck #
 - [Pub] transfer #
 - [Pub] balanceOf
- + StandardToken (ERC20, BasicToken)
 - [Pub] transferFrom #
 - [Pub] approve #
 - [Pub] allowance
 - [Pub] increaseApproval #
 - [Pub] decreaseApproval #
- + MintableToken (StandardToken)
 - [Pub] __basicTokenTransferable #
 - modifiers: onlyOwner
 - [Pub] stop_mint #
 - modifiers: onlyOwner
 - [Pub] mint #
 - modifiers: hasMintPermission,canMint
 - [Pub] finishMinting #
 - modifiers: onlyOwner,canMint

CONTRACT FUNCTIONS

- + FreezableToken (StandardToken)
 - [Int] toKey
 - [Pub] freezingCount
 - [Pub] getFreezing
 - [Pub] releaseOnce #
 - [Pub] releaseAll #
 - [Int] freeze #
- + FreezableMintableToken (FreezableToken, MintableToken)
 - [Pub] mintAndFreeze #
 - modifiers: onlyOwner,canMint
- + Consts
- + MainToken (Consts, FreezableMintableToken)
 - [Pub] <Constructor> #
 - [Pub] __name
 - [Pub] __symbol
 - [Pub] __decimals
 - [Pub] transferFrom #
 - [Pub] transfer #

(\$) = payable function

= non-constant function

ISSUES CHECKING

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

No low severity issues found.

0 SECURITY ISSUES FOUND

Owner privileges (In the period when the owner is not renounced)

- Owner can mint and freeze if mintingFinished is set to false.

```
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;
}
```

OUR CONCLUSION

Smart contracts do not contain high severity issues.*

*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.

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. 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 Sekudex, no duty of care towards you or any other person, nor does Sekudex 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.



<https://Sekudex.finance>

