



# MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

2021

# THE TRUTH TOKEN AUDIT REPORT

10 NOV 2021

## SECURITY ASSESMENT

# TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
The Truth Token Distribution	8
The Truth Token Contract Interaction Details	8
Top 10 Token Holders	9
Security Issue	10 -11
Token Logo	12
Conclusion	13



# SECURITY ASSESMENT

## SUMMARY

This report has been prepared for The Truth to discover issues and vulnerabilities in the source code of the The Truth project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Testnet Deployment techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# SECURITY ASSESSMENT

# 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 MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit 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 MotechAudit 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, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, 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.



# SECURITY ASSESSMENT

# BACKGROUND

MotechAudit was commissioned by The Truth to perform an audit of smart contracts:

<https://etherscan.io/address/0x249e38ea4102d0cf8264d3701f1a0e39c4f2dc3b>

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.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# SECURITY ASSESSMENT

## AUDIT DETAILS



### AUDITED PROJECT

The Truth



### DEPLOYER ADDRESS

0x378Ddb6914e32c4D9c0E08881d460eE9c6C73b82



### CLIENT CONTACTS:

The Truth team



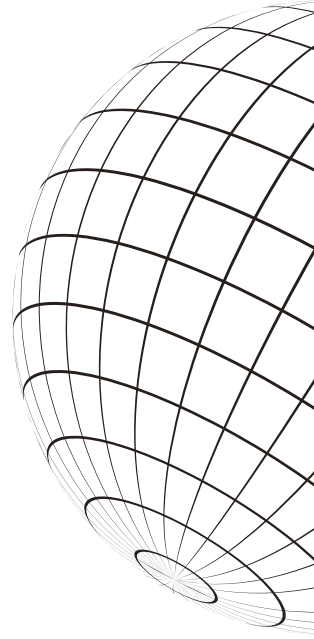
### BLOCKCHAIN

Ethereum Project



### WEBSITE:

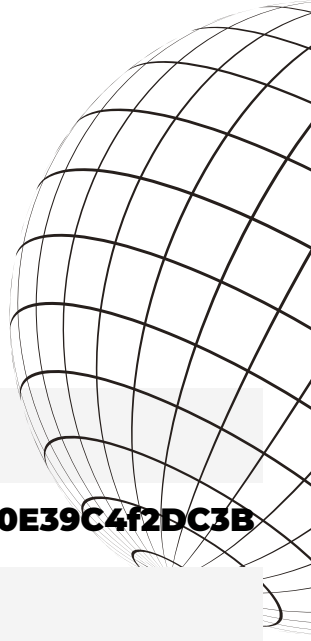
<https://www.ufogaming.io/>



## SECURITY ASSESSMENT

# CONTRACT DETAILS

### Token contract details for May-21-2021



<b>Contract name</b>	<b>The Truth</b>
<b>Contract address</b>	<b>0x249e38Ea4102D0cf8264d3701f1a0E39C4f2DC3B</b>
<b>Total supply</b>	<b>51,515,151,515,151 UFO</b>
<b>Token ticker</b>	<b>THE TRUTH (UFO)</b>
<b>Decimals</b>	<b>18</b>
<b>Token holders</b>	<b>30,518</b>
<b>Transactions count</b>	<b>133,978</b>
<b>Top 100 holders dominance</b>	<b>75.2282%</b>
<b>Contract deployer address</b>	<b>0x378Ddb6914e32c4D9c0E08881d460eE9c6C73b82</b>
<b>Contract's current owner address</b>	<b>0x378Ddb6914e32c4D9c0E08881d460eE9c6C73b82</b>

## SECURITY ASSESSMENT

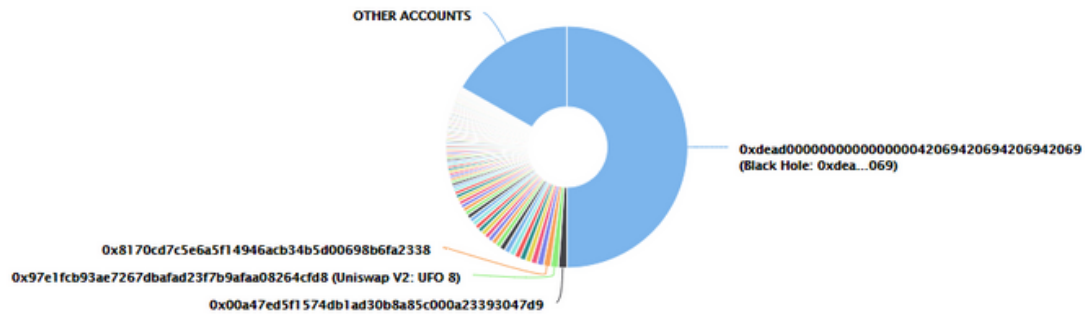
# THE TRUTH TOKEN DISTRIBUTION

The top 100 holders collectively own 83.20% (42,860,572,807,448.90 Tokens) of THE TRUTH

Token Total Supply: 51,515,151,515.00 Token | Total Token Holders: 30,545

### THE TRUTH Top 100 Token Holders

Source: Etherscan.io



(A total of 42,860,572,807,448.90 tokens held by the top 100 accounts from the total supply of 51,515,151,515.00 token)

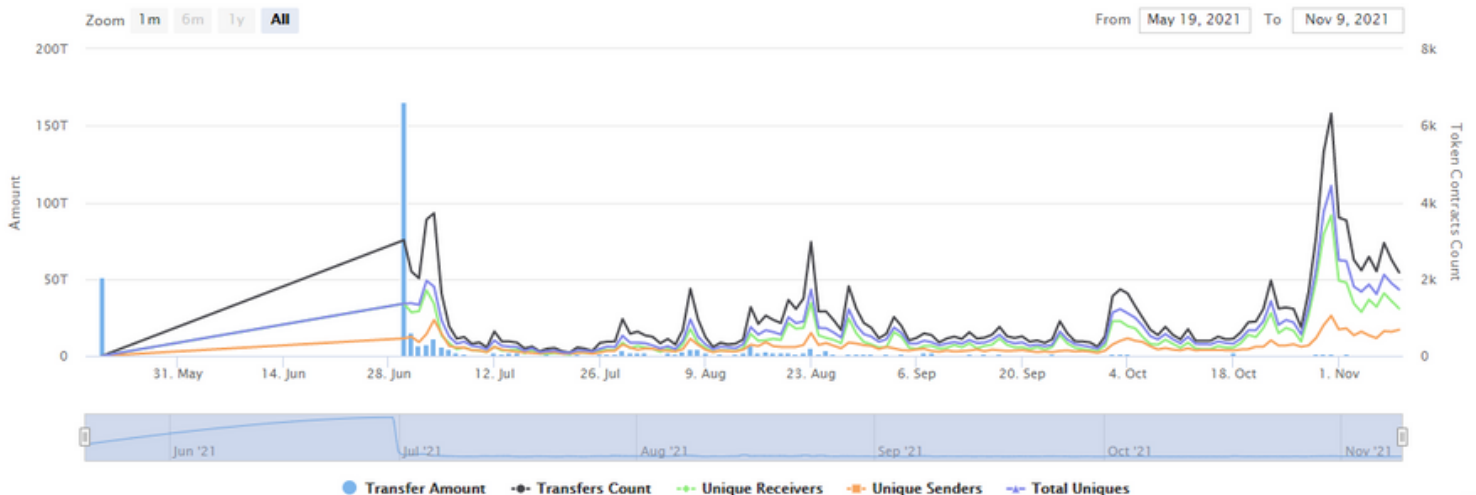
## THE TRUTH TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Fri 21, May 2021 - Tue 9, Nov 2021

Token Contract 0x249e38ea4102d0cf8264d3701f1a0e39c4f2dc3b (THE TRUTH)


Source: Etherscan.io





## SECURITY ASSESSMENT

# TOP 10 TOKEN HOLDERS

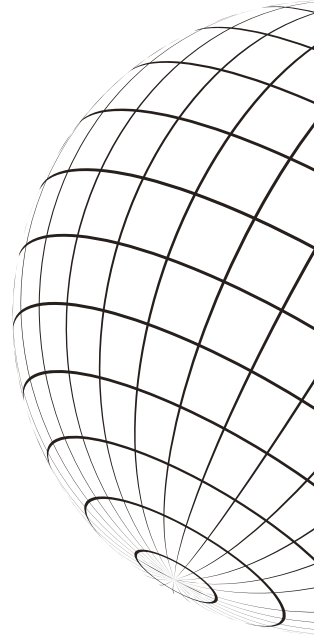
Rank	Address	Quantity	Percentage	Value	Analytics
1	Black Hole: 0xdea...069	25,757,575,757,575.5	50.0000%	\$103,287,878.79	<a href="#">📈</a>
2	0x00a47ed5f1574db1ad30b8a85c000a23393047d9	589,970,031,051.12	1.1452%	\$2,365,779.82	<a href="#">📈</a>
3	 Uniswap V2: UFO 8	532,228,650,794.445523190663544501	1.0331%	\$2,134,236.89	<a href="#">📈</a>
4	0x8170cd7c5e6a5f14946acb34b5d00698b6fa2338	500,000,000,000	0.9706%	\$2,005,000.00	<a href="#">📈</a>
5	0xa8729109d3a03901aa89da4c51f785f08cf974d1	455,482,011,729	0.8842%	\$1,826,482.87	<a href="#">📈</a>
6	0x8bdb69f351da6d484f1afec3274ab33fa70a16ce	421,080,001,000	0.8174%	\$1,688,530.80	<a href="#">📈</a>
7	0x9fc2799ffe4d723480efb5413c26ae7c3cf5e7f	408,000,000,000	0.7920%	\$1,636,080.00	<a href="#">📈</a>
8	0xb21f6964d32b3aad08d2c9e3f8d965e7941cc4f	395,999,999,999.9999999999999999999999	0.7687%	\$1,587,960.00	<a href="#">📈</a>
9	0xa59104cfe3f859a008be2c5a5297b29b84eef5eb	392,484,925,413.3534	0.7619%	\$1,573,864.55	<a href="#">📈</a>
10	0x2e2a64555bd20161c679370f3bba6c47d10d6cd5	392,216,331,727.37	0.7614%	\$1,572,787.49	<a href="#">📈</a>

source:<https://etherscan.io/>



# SECURITY ASSESSMENT

## SECURITY ISSUES



✓ Critical Severity Issues  
No high severity issues found.

✓ High Severity Issues  
No high severity issues found.

✓ Medium Severity Issues  
No high severity issues found.

✓ Low Severity Issues  
No high severity issues found.

Lowest / Code style / Best Practice

1. Issue: Public function that could be declared external.

public functions that are never called by the contract should be declared external to save gas.

Lines: #203

```
function name() public view virtual override returns (string memory) {
```

Lines: #211

```
function symbol() public view virtual override returns (string memory)  
{
```

# SECURITY ASSESSMENT

## SECURITY ISSUES

Lines: #235

```
function totalSupply() public view virtual override returns (uint256) {
```

Lines: #242

```
function balanceOf(address account) public view virtual override  
returns (uint256) {
```

Lines: #254

```
function transfer(address recipient, uint256 amount) public virtual  
override returns (bool) {
```

Lines: #273

```
function approve(address spender, uint256 amount) public virtual  
override returns (bool) {
```

Lines: #291

```
function transferFrom(address sender, address recipient, uint256  
amount) public virtual override returns (bool) {
```

Lines: #313

```
function increaseAllowance(address spender, uint256 addedValue) public  
virtual returns (bool) {
```

Lines: #332

```
function decreaseAllowance(address spender, uint256 subtractedValue)  
public virtual returns (bool) {
```

### 2. Issue: Maximum line length.

Solidity declares recommended maximum line length.

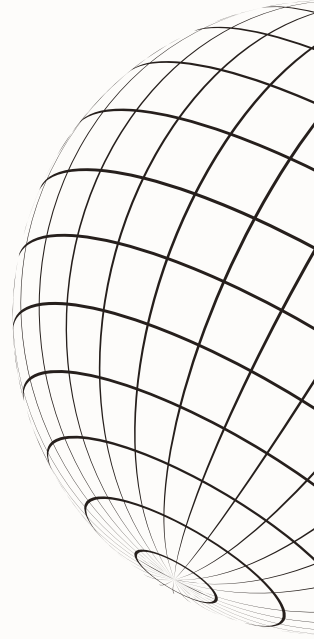
Recommendation: Please follow the solidity style guide

Lines: #70, 262, 291 and 332



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

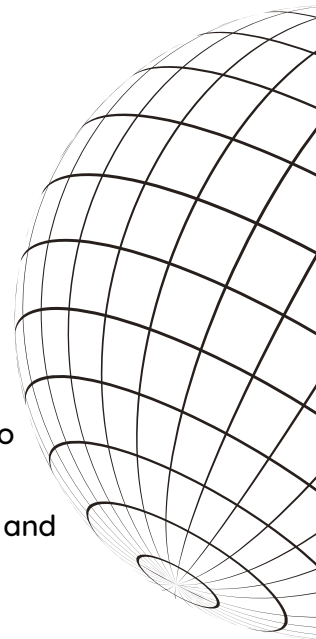
# SECURITY ASSESMENT TOKEN LOGO



# SECURITY ASSESMENT CONCLUSION

Smart contracts contain owner privileges!

Motech Audit 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.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT