



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

CRYPTO STAKE TOKEN AUDIT REPORT

2021

24 NOV 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
Crypto Stake Token Distribution	8
Crypto Stake 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 Crypto Stake to discover issues and vulnerabilities in the source code of the Crypto Stake 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 Test net 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.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

BACKGROUND

MotechAudit was commissioned by Crypto Stake to perform an audit of smart contracts:

<https://bscscan.com/address/0xc182bda20ae32ddae3ad5cd94b191380114d2f72>

The purpose of the audit was to achieve the following:

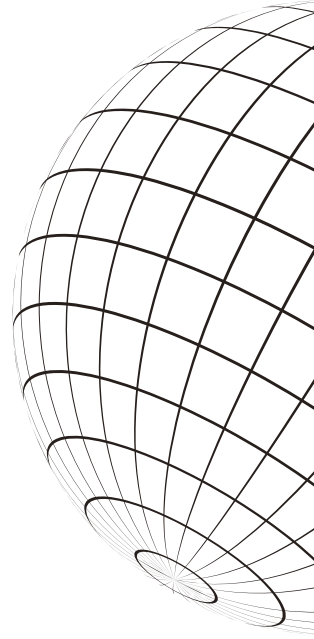
- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

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

AUDIT DETAILS



AUDITED PROJECT

Crypto Stake



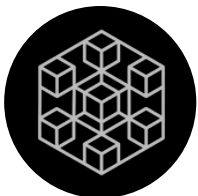
DEPLOYER ADDRESS

0x97aA45D0C87CC81D8d6c045D400Ce602A3879504



CLIENT CONTACTS:

Crypto Stake Team



BLOCKCHAIN

Binance Smart Chain Project



WEBSITE:

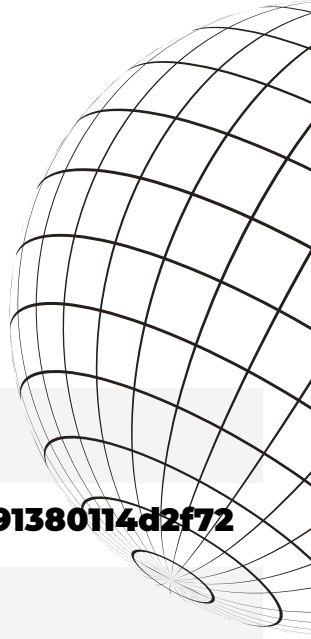
<https://crypto-stake.org/>



SECURITY ASSESSMENT

CONTRACT DETAILS

Token contract details for Aug-09-2021



Contract name	Crypto Stake
Contract address	0xc182bda20ae32ddae3ad5cd94b191380114d2f72
Total supply	200,000,000 CST
Token ticker	Crypto Stake Token (CST)
Decimals	18
Token holders	200
Transactions count	260
Top 100 holders dominance	99.9416%
Contract deployer address	0x97aA45D0C87CC81D8d6c045D400Ce602A3879504
Contract's current owner address	0x97aA45D0C87CC81D8d6c045D400Ce602A3879504



SECURITY ASSESSMENT

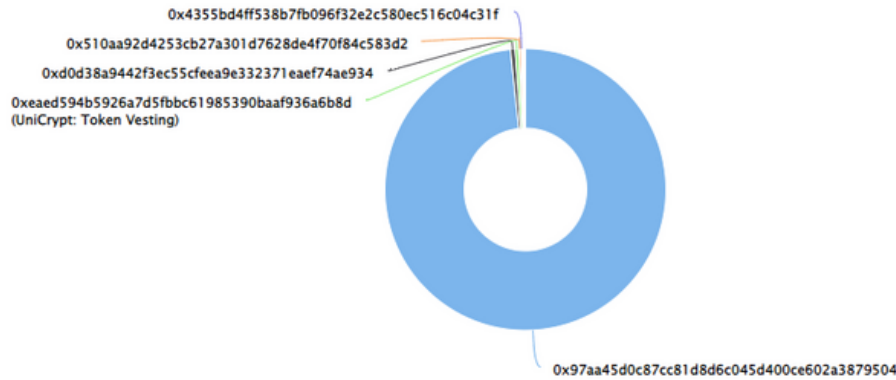
CRYPTO STAKE TOKEN DISTRIBUTION

The top 100 holders collectively own 99.98% (199,964,767.54 Tokens) of Crypto Stake Token

Token Total Supply: 200,000,000.00 Token | Total Token Holders: 200

Crypto Stake Token Top 100 Token Holders

Source: BscScan.com



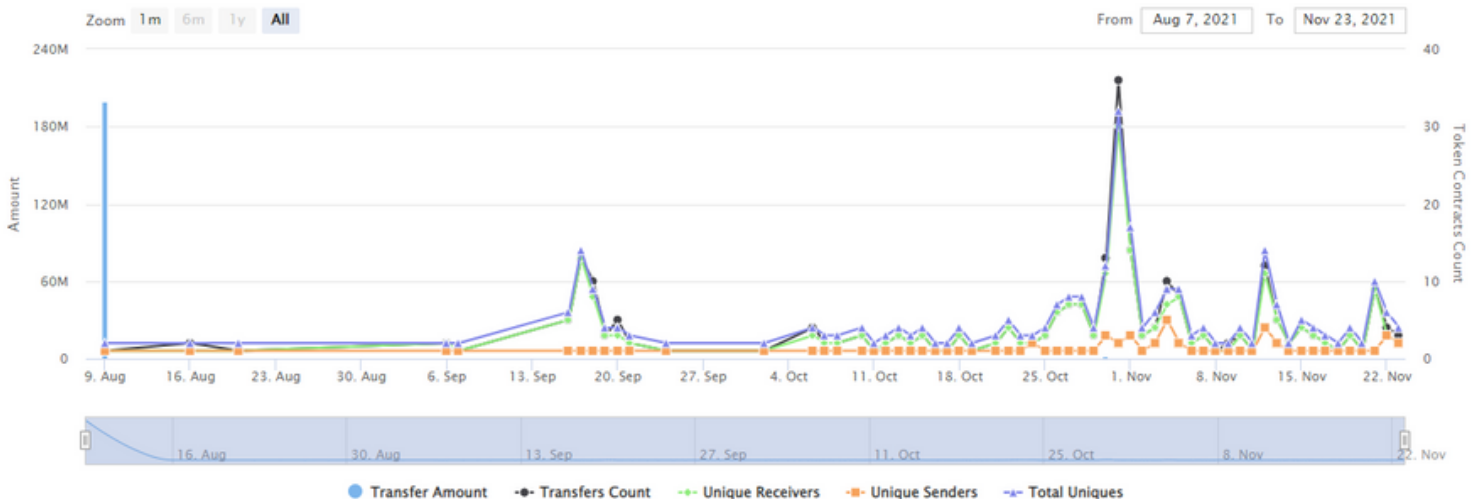
(A total of 199,964,767.54 tokens held by the top 100 accounts from the total supply of 200,000,000.00 token)

CRYPTO STAKE TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Mon 9, Aug 2021 - Tue 23, Nov 2021



Token Contract 0xc182bda20ae32ddae3ad5cd94b191380114d2f72 (Crypto Stake Token)
Source: BscScan.com



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Analytics
1	0x97aa45d0c87cc81d8d6c045d400ce602a3879504	196,620,063.188447537	98.3100%	📈
2	0xd0d38a9442f3ec55cfeca9e332371eae74ae934	1,024,823.2304044	0.5124%	📈
3	 UniCrypt: Token Vesting	797,354.208375	0.3987%	📈
4	 0x510aa92d4253cb27a301d7628de4f70f84c583d2	546,652.711	0.2733%	📈
5	0x4355bd4ff538b7fb096f32e2c580ec516c04c31f	200,000	0.1000%	📈
6	0xd6a96319f0dbc70ffd439af4a99480ae726393bd	135,338.33333333	0.0677%	📈
7	0x74f492536700309823871701301d34b5a87911c8	101,431.26637	0.0507%	📈
8	0x518d4bb9b4d15f18cf284588e3ecce9e91e38cbf	50,653.5	0.0253%	📈
9	0x9d75e55b7f30a100fe7c5ab95d6cbe85ed5971aa	40,720	0.0204%	📈
10	0xf9f4b5092482518644966d7fd0ca82012e32ee8d	33,714	0.0169%	📈

source:<https://bscscan.com/>

SECURITY ASSESSMENT

SECURITY ISSUES

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No high severity issues found.

Low Severity Issues

1. Using contracts with empty functions

In the code, we've found several contracts (ERC20Basic, ERC20) which have all functions unimplemented. Those look like interfaces but are declared as contracts.

Contracts: ERC20Basic, ERC20

Recommendation: We'd recommend doing the following:

- move "totalSupply" variable declaration from ERC20Basic to StandardToken;
- declare functions of ERC20Basic, ERC20 external instead of public;
- remove the inheritance from the ERC20 and put two inheritances into the StandardToken (contract StandardToken is ERC20, ERC20Basic);
- declare both ERC20Basic and ERC20 as interfaces instead of contracts

2. Unlimited minting token

The owner of the contract is able to mint an unlimited amount of the token at any time. If it is correct behavior, please make sure this is stated in the whitelist and the community is acknowledged.

Contracts: CoinToken

Function: mint

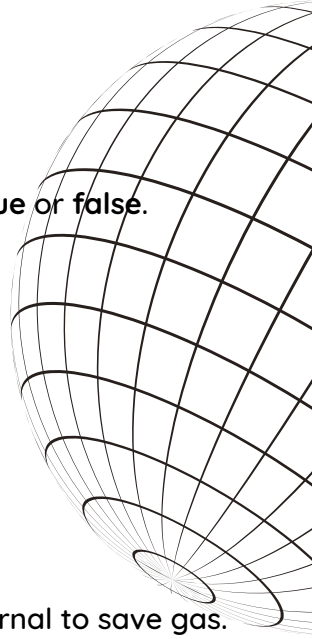
Recommendation: Please either restrict minting by some hard cap, or add vesting time, or inform the community that the minting is unlimited and unrestricted for the owner.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

SECURITY ISSUES



3. Boolean equality

Boolean constants can be used directly and do not need to be compared to **true** or **false**.

Contracts: StandardToken

Function: transfer, transferFrom

Recommendation: Remove the equality to the boolean constant.

4. A public function that could be declared external

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

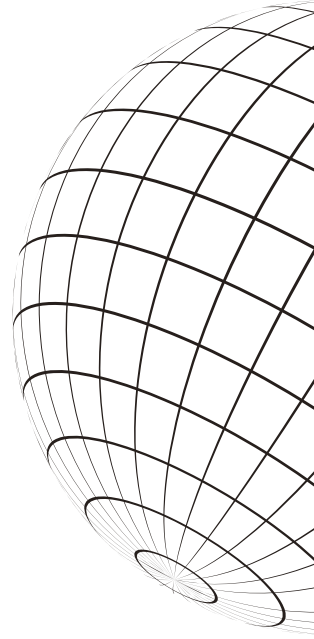
Contracts: Ownabletoken, Pausable, ERC20Basic, StandardToken, ERC20, CoinToken

Function: Ownabletoken.transferOwnership, Pausable.pause, Pausable.unpause, ERC20Basic.balanceOf, StandardToken.balanceOf, ERC20.allowance, StandardToken.allowance, PausableToken.blackListAddress, CoinToken.burn, CoinToken.mint

Recommendation: Use the external attribute for functions never called from the contract.



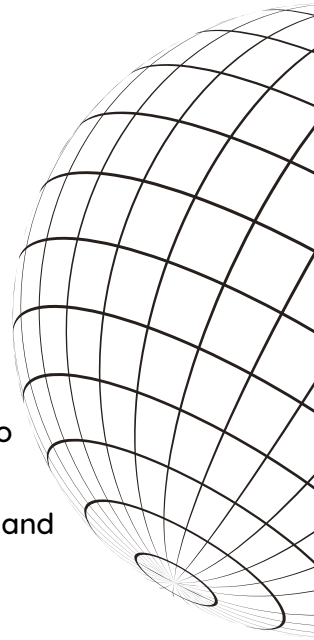
SECURITY ASSESMENT
TOKEN LOGO



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