



# MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

2021

# BITCOIN SB TOKEN AUDIT REPORT

4 JAN 2022

## SECURITY ASSESMENT

# TABLE OF CONTENTS

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



# SECURITY ASSESMENT

## SUMMARY

This report has been prepared for Bitcoin SB to discover issues and vulnerabilities in the source code of the Bitcoin SB 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.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# SECURITY ASSESSMENT

# BACKGROUND

MotechAudit was commissioned by Bitcoin SB to perform an audit of smart contracts:

<https://etherscan.io/address/0xcf8829ae9384540c886a151fac3a865794cb9a01>

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

Bitcoin SB



### DEPLOYER ADDRESS

0x274eD495AD1be97282cF6a4271B92e50B1c398C1



### CLIENT CONTACTS:

Bitcoin SB team



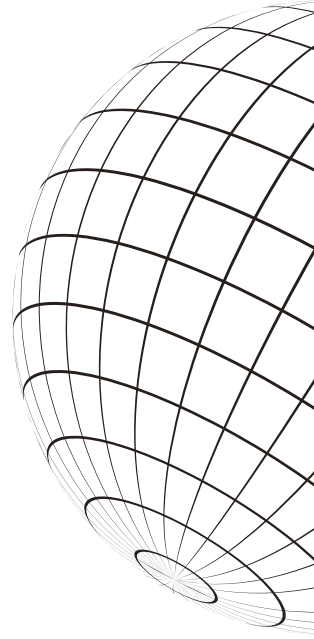
### BLOCKCHAIN

Ethereum Project



### WEBSITE:

<https://bitcoinsb.org>

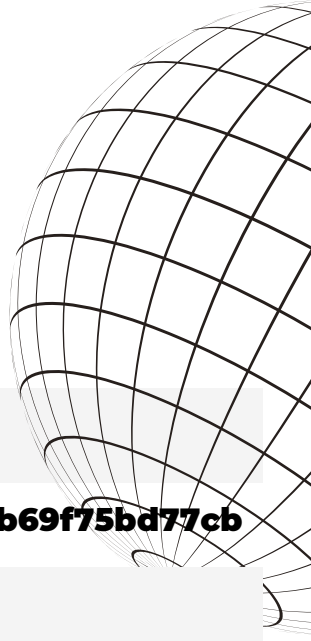


**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

# CONTRACT DETAILS

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



<b>Contract name</b>	<b>Bitcoin SB</b>
<b>Contract address</b>	<b>0xa478a13242b64629bff309125770b69f75bd77cb</b>
<b>Total supply</b>	<b>1,000,000 BSB</b>
<b>Token ticker</b>	<b>Bitcoin SB (BSB)</b>
<b>Decimals</b>	<b>18</b>
<b>Token holders</b>	<b>287</b>
<b>Transactions count</b>	<b>2,448</b>
<b>Top 100 holders dominance</b>	<b>99.89%</b>
<b>Contract deployer address</b>	<b>0x274eD495AD1be97282cF6a4271B92e50B1c398C1</b>
<b>Contract's current owner address</b>	<b>0x274eD495AD1be97282cF6a4271B92e50B1c398C1</b>

## SECURITY ASSESSMENT

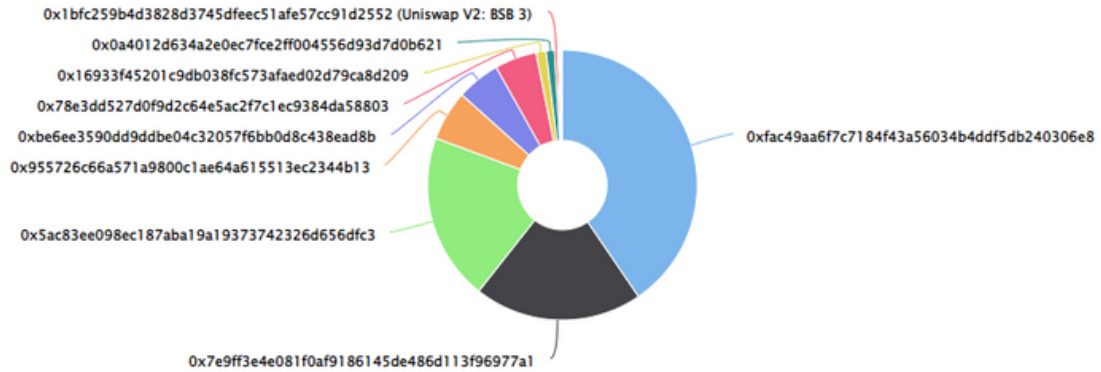
# BITCOIN SB TOKEN DISTRIBUTION

The top 100 holders collectively own 99.97% (999,686.41 Tokens) of Bitcoin SB

Token Total Supply: 1,000,000.00 Token | Total Token Holders: 287

### Bitcoin SB Top 100 Token Holders

Source: Etherscan.io



(A total of 999,686.41 tokens held by the top 100 accounts from the total supply of 1,000,000.00 token)

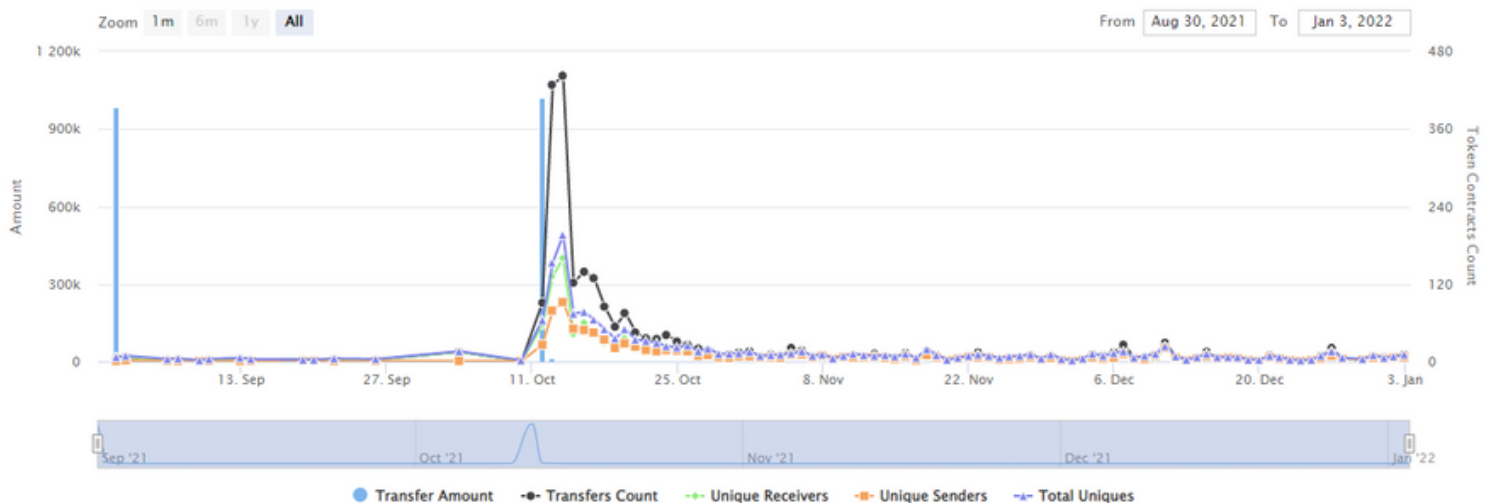
## BITCOIN SB TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Wed 1, Sept 2021 - Mon 3, Jan 2022

Token Contract 0xa478a13242b64629bff309125770b69f75bd77cb (Bitcoin SB)

Source: Etherscan.io






















**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT



## SECURITY ASSESSMENT

# TOP 10 TOKEN HOLDERS

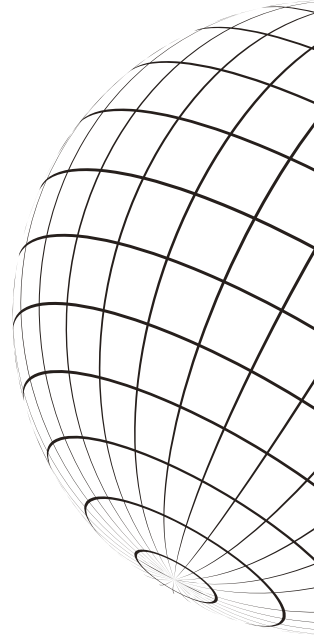
Rank	Address	Quantity	Percentage	Value	Analytics
1	 0xfac49aa6f7c7184f43a56034b4ddf5db240306e8	404,771.857255696917344253	<u>40.4772%</u>	\$7,821,119.20	
2	 0x7e9ff3e4e081f0af9186145de486d113f96977a1	201,687.703289800253035608	<u>20.1688%</u>	\$3,897,068.29	
3	 0x5ac83ee098ec187aba19a19373742326d656dfc3	200,000	<u>20.0000%</u>	\$3,864,458.00	
4	 0x955726c66a571a9800c1ae64a615513ec2344b13	60,000	<u>6.0000%</u>	\$1,159,337.40	
5	 0xbe6ee3590dd9ddbe04c32057f6bb0d8c438ead8b	52,000	<u>5.2000%</u>	\$1,004,759.08	
6	 0x78e3dd527d0f9d2c64e5ac2f7c1ec9384da58803	50,285.2636814162	<u>5.0285%</u>	\$971,626.45	
7	 0x16933f45201c9db038fc573afaed02d79ca8d209	12,000	<u>1.2000%</u>	\$231,867.48	
8	 0x0a4012d634a2e0ec7fce2ff004556d93d7d0b621	10,000	<u>1.0000%</u>	\$193,222.90	
9	 Uniswap V2: BSB 3	3,664.835334614951289426	<u>0.3665%</u>	\$70,813.01	
10	0x1aba3a2a109b999fabe1a0b16f0620b73efbd84b	593	<u>0.0593%</u>	\$11,458.12	

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  
Too many digits Literals with many digits are difficult to read and review.  
Recommendation: Please use scientific notation and/or ether units: ie. 1e6 ether; 50e3 ether; etc.

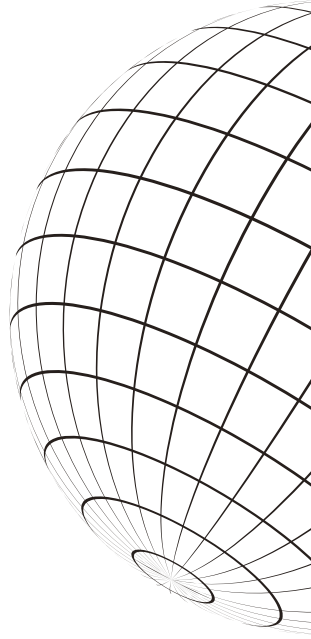
**Lines:** BitcoinSB#133

```
_totalSupply = 1000000 * 10 ** _decimal;
```



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

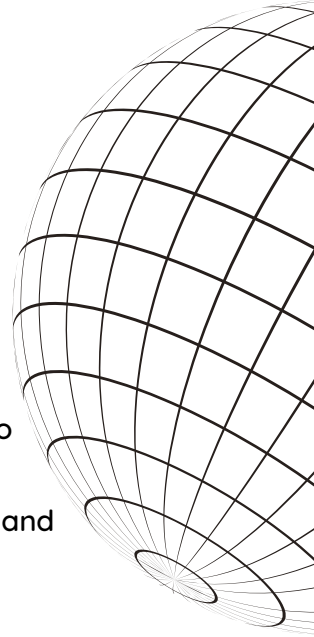
**SECURITY ASSESMENT**  
**TOKEN LOGO**



# 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