



**BSCEX**

## **SMART CONTRACT SECURITY ANALYSIS**

**MARCH 2nd, 2021**

## Project Summary

Project Name	BSCEX
Scope	A decentralized exchange-centered ecosystem that aims making Binance's off-chain services available on the blockchain, developing applications on BSC and offering users yield farming opportunities.
Platform	Binance, Solidity

## Executive Summary

- Three smart contracts were analyzed to check the availability of code vulnerabilities associated with the process of funds staking: [BSCX](#), [BSCXMasterFarmer](#), [BSCXNTS](#).
- No significant security issues were revealed in the aforementioned contracts.

Smart Contract Ownership	Team Reward	Total Supply	Minting Function	Migration Function	Funds Lock Period	Contract Pause	Suspicious Functions
EOA	30% of user rewards	Fixed	Not available	Not available	None	Possible	Not found

### External Smart Contract Audits:

- The project's smart contracts were audited by [Verichains](#), but the audit features the BSCXNTX contract that is currently missing on <https://github.com/Bscex>. Thus, validity of the audit is doubtful.

# Manual Check Results

## Ownership structure:

Smart contract	Owner	Description
<a href="#"><b>BSCX</b></a>	<a href="#"><b>BSCXMasterFarmer</b></a>	<p>The owner can call:</p> <ul style="list-style-type: none"> <li>• the mint function</li> <li>• addTransferBurnExceptAddress</li> <li>• removeTransferBurnExceptAddress</li> <li>• setTransferBurnRate (The maximum rate is 100%. The current is set to 0%)</li> </ul> <p>The contract:</p> <ul style="list-style-type: none"> <li>• defines total supply;</li> <li>• burns transferBurnRate with each transfer, besides the ones initiated by whitelisted addresses. The current transferBurnRate is 0%, the maximum rate is 100%)</li> </ul> <p>The token deployer is the <a href="#">Bscex: Deployer</a>, which is the top <b>BSCX</b> EOA holder (The share is 6%). The second largest holder is an <a href="#">EOA address</a>, closely related to the deployer (The share is 4.4%).</p>
<a href="#"><b>BSCXMasterFarmer</b></a>	<a href="#"><b>Bscex: Deployer</b></a>	<p>5 156 028 <b>BSCX</b> are locked in the contract for 660 days.</p> <p>The owner can call:</p> <ul style="list-style-type: none"> <li>• transferOwnership/ renounceOwnership</li> <li>• addTransferBurnExceptAddress (in the <b>BSCX</b> token smart contract)</li> <li>• removeTransferBurnExceptAddress (in the <b>BSCX</b> token smart contract)</li> <li>• setTransferBurnRate (in the <b>BSCX</b> token smart contract)</li> <li>• setBurnPercent</li> <li>• setMigrator</li> <li>• set - the function updates a pool's BSCX allocation point</li> <li>• add -the function adds new liquidity providers to pools</li> </ul> <p>The EOA owner could instantly migrate LP tokens from one pair address to another without restrictions.</p> <p>Currently, the contract is used to lock users' tokens and can't mint new tokens.</p>
<a href="#"><b>BSCXNTS</b></a>	<a href="#"><b>Bscex: Deployer</b></a>	<p>The owner can call the following functions:</p> <ul style="list-style-type: none"> <li>• add</li> <li>• _setAllocPoints defines allocation points in a pool</li> <li>• _setHalvingAtBlocks</li> <li>• setStatus</li> <li>• setReferrallPToken</li> <li>• setAmountLPStakeLevelRefer</li> <li>• setPercentLPLevelRefer</li> <li>• set updates a given pool's BSCX allocation point</li> </ul>

 **Total supply:**

- Fixed: 9 983 396 tokens

 **Team reward:**

- 30% of user rewards

 **Minting function:**

- Not available

 **Migration function:**

- Not available

 **Funds lock period:**

- None

 **Possibility to pause the Smart Contracts:**

- Available for funds withdrawal and claiming rewards. Emergency withdrawals are not affected

 **Suspicious functions:**

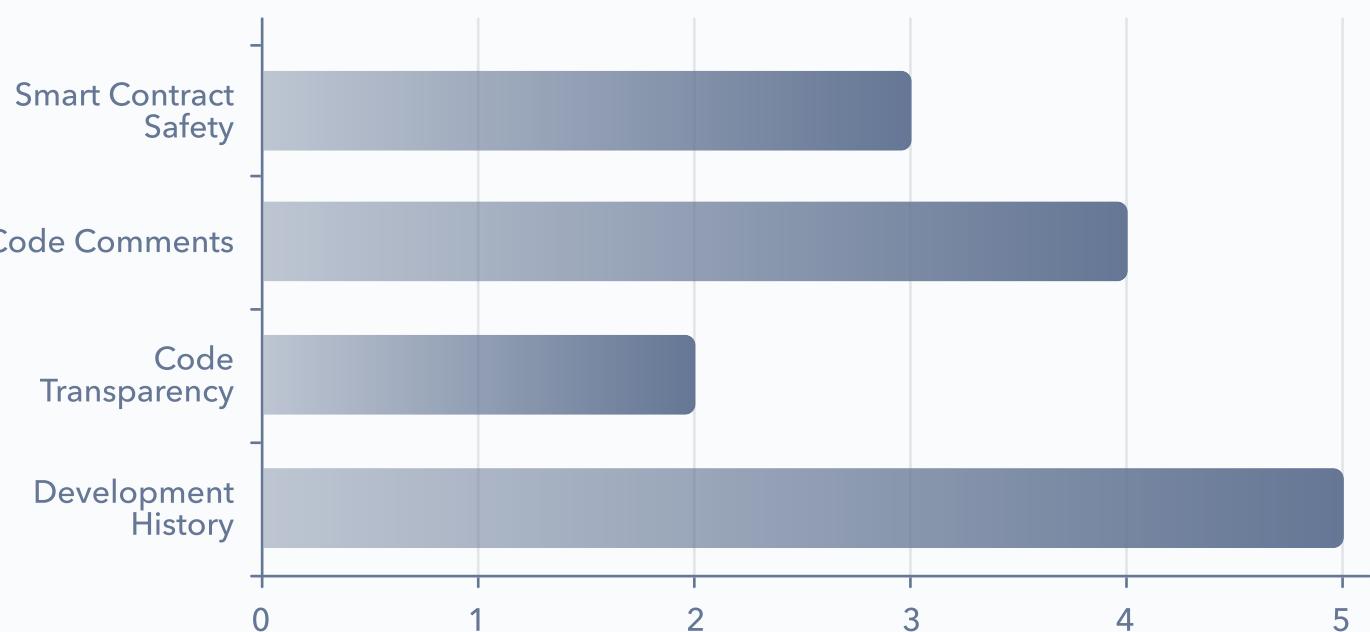
- Not found

 **Tornado cash connections:**

- Not found

 **Risk Level**LOW

## Smart Contracts



## Conclusion

The BSCEX yield farming is based on Binance Smart Chain and run by the [BSCX](#), [BSCXMasterFarmer](#) and [BSCXNTS](#) smart contracts.

Although [BSCXMasterFarmer](#), which owns the BSCEX token smart contract, features the possibility to migrate, this functionality is no longer available as the contract was broken through setting the burn percent rate to 100%. Consequently, the underlying mint function is not available anymore as well.

The total supply of the token is fixed until burning is activated: burning of the token can be executed based on results of voting about adding commission on transfers, which then will be burned.

It's important to point out that above 10% of the token total supply is under control of the dev team. Since 51% of the total supply of the token is locked and the volume in circulation is 49%, the dev team controls 20% of the circulation supply.

bscscan.com/token/0x5ac52ee5b2a633895292ff6d8a89bb9190451587#balances				
Rank	Address	Quantity	Percentage	Value
1	<a href="#">0x1070b9a998c4457c5f393e389f275012e91b31d2</a>	5,168,670.4423449	51.7727%	\$90,298,267.15
2	<a href="#">BsceX: Deployer</a>	608,643.017521826	6.0966%	\$10,633,181.28
3	<a href="#">0xa8cd2bc8140a760d4ac81e415e0296f3af7aa752</a>	441,222.501512889	4.4196%	\$7,708,293.22
4	<a href="#">PancakeSwap: BSCX</a>	420,230.861871586	4.2093%	\$7,341,562.80
5	<a href="#">PancakeSwap: BSCX-zSEED</a>	351,538.172280422	3.5212%	\$6,141,480.32

Moreover, the team is rewarded with 30% of user rewards. Thus, the risk of a quick token dump initiated by the team can be rated as 6/10.

Also, users should pay attention to the fact that pausing can be implemented for fund withdrawal and claiming rewards. But this is not applicable to emergency fund withdrawal.

No funds lock period is implemented and no suspicious functions were found in the smart contracts analyzed. Therefore, the risk level of the project can be estimated as low.

- ! This analysis is not a financial advice
- Conduct your own research before investing
- Track updates of yield farming platforms