TOKEN AUDIT SECURITY BY COIN TOOL

Base Info

- Token Name
  Bitcoin X REVOLUTION
- Symbol BITCOIN
- Chain Polygon
- PolygonContract Address
  0xD6F5284239C2C11635A349fB55A8e207064a7380
  Supply
  100000000000000000000Decimal
  18Burn
  0.00%
  Owner address
  0x12320e4eee46419c40af2e06013af16ea0adafa4
  Creator address
  0x12320e4eee46419c40af2e06013af16ea0adafa4
  Is open source? Is open source

Risk analysis

- Buy tax 0% Sell tax 0%
  Is honeypot? Security
  Can edit tax? Security
  Is anti whale? Security
  Can take back ownership? Security
  Is blacklisted? Security
  Is whitelisted? Security
  Is mintable? Security
  Is proxy contract? Security
  Can transfer pausable? Security
  Is Trading with CooldownTime? Security

THREAT SCAN SUMMARY
Threat Score 100/100

ThreatScan, a smart contract analysis tool, is built by the SolidityScan team. It is designed to assist users in identifying potential rug pull scams by providing an in-depth analysis of a smart contract's code and highlighting any potential red flags that may indicate a scam.

IS SOURCE CODE VERIFIED
The contract's source code is verified.
Source code verification provides transparency for users interacting with smart contracts. Block explorers validate the compiled code with the one on the blockchain. This also gives users a chance to audit the contracts.

PRESENCE OF MINTING FUNCTION
The contract cannot mint new tokens. The `_mint` functions was not detected in the contracts.
Mint functions are used to create new tokens and transfer them to the user's/owner's wallet to whom the tokens are minted. This increases the overall circulation of the tokens.

PRESENCE OF BURN FUNCTION
The tokens can not be burned in this contract.
Burn functions are used to increase the total value of the tokens by decreasing the total supply.

SOLIDITY PRAGMA VERSION
The contract can not be compiled with an older Solidity version.
Pragma versions decide the compiler version with which the contract can be compiled. Having older pragma versions means that the code may be compiled

with outdated and vulnerable compiler versions, potentially introducing vulnerabilities and CVEs.

PROXY-BASED UPGRADABLE CONTRACT
This is not an upgradable contract.
Having upgradeable contracts or proxy patterns allows owners to make changes to the contract's functions, token circulation, and distribution.

OWNERS CANNOT BLACKLIST TOKENS OR USERS
Owners cannot blacklist tokens or users.
If the owner of a contract has permission to blacklist users or tokens, all the transactions related to those entities will be halted immediately.

PAUSABLE CONTRACTS
This is not a Pausable contract.
If a contract is pausable, it allows privileged users or owners to halt the execution of certain critical functions of the contract in case malicious transactions are found.

CRITICAL ADMINISTRATIVE FUNCTIONS
Critical functions that add, update, or delete owner/admin addresses are not detected
These functions control the ownership of the contract and allow privileged users to add, update, or delete owner or administrative addresses. Owners are usually allowed to control all the critical aspects of the contract.

CONTRACT/TOKEN SELF DESTRUCT
The contract cannot be self-destructed by owners.
`selfdestruct()` is a special function in Solidity that destroys the contract and

transfers all the remaining funds to the address specified during the call. This is usually access-control protected.

ERC20 RACE CONDITION
The contract is not vulnerable to ERC-20 approve Race condition vulnerability.
ERC-20 approve function is vulnerable to a frontrunning attack which can be exploited by the token receiver to withdraw more tokens than the allowance.
Proper mitigation steps should be implemented to prevent such vulnerabilities.

RENOUNCED OWNERSHIP
The contract's owner was not found.
Renounced ownership shows that the contract is truly decentralized and once deployed, it can’t be manipulated by administrators.

USERS WITH TOKEN BALANCE MORE THAN 5%
No addresses contains more than 5% of circulating token supply.. Token distribution plays an important role when controlling the price of an asset.

OVERPOWERED OWNERS
The contracts have not defined any owner-controlled functions.
Giving too many privileges to the owners via critical functions might put the user's funds at risk if the owners are compromised or if a rug-pulling attack happens.

COOLDOWN FEATURE
The contract does not have a cooldown feature.
Cooldown functions are used to halt trading or other contract workflows for a certain amount of time so as to prevent users from repeatedly executing transactions or buying and selling tokens.

OWNERS WHITELISTING TOKENS/USERS
Owners can not whitelist tokens or users.
If the owner of a contract has permission to whitelist users or tokens, it'll be unfair toward other users or the transaction flow may not be executed impartially.

OWNERS CAN SET/UPDATE FEES
Owners can not set or update Fees in the contract.

HARDCODED ADDRESSES
The contract was not hardcoding addresses in the code.

OWNERS UPDATING TOKEN BALANCE
The contract does not have any owner-controlled functions modifying token balances for users or the contract

FUNCTION RETRIEVING OWNERSHIP
No such functions were found
If this function exists, it is possible for the project owner to regain ownership even after relinquishing it.

Token holders (10) 2024/02/01

Top 10 :

0x12320e4eee46419c40af2e06013af16ea0adafa4
Creator 100.00%
99999999999972188358 BITCOIN

0x3eeb80f61d8c996a0a3a9c34b1897e44329afbb1
25780681 BITCOIN

0xb61273b29292b85fa246c94d5e8e30a457806703
1000000 BITCOIN

0xadd7ab5f8d79890996c17bd3546989430431530f
1000000 BITCOIN

0x4c65a2a9adbf53261c4ebeeb98afab2d7f036819
15000 BITCOIN

0x392dd5e98c9751a004fe8917e393a84d45d6f7f2
10000 BITCOIN

0x9625d4438f910bde72924c2884372a1e935c5511
4949 BITCOIN

0x903dc2fe2e0433e0165079acd01c303fe4dc00c1
1000 BITCOIN

0x0b5bdca6a88d41098d1a78367a7a053a9e23bcb3
10 BITCOIN

0xa48b3aa7af88c797c94dc5af463f5d429fe28836
0 BITCOIN