Mambo Token Security Standard (MTSS)

for decentralized Stable Coins and Tokens

This applies only for Tokens, that are aimed to have the mint and burn function, as it is normally the case for any kind of **stable coins**, since the quantity of tokens is adapted to the supply and demand to help maintain the pegged price in the market.

For some other coins, minting or burning or both functions makes sense. But it must be clearly described in the tokenomy or withepaper why it has those functions.

A Stable Coin or Token that aims to be as decentralized as possible must have following functions and restriction:

1. Only the contract owner or delegated MinterBurner can mint or burn tokens.

2. The contract owner or MinterBurner can only mint into his account or burn from his account.

This makes abusive burn intervention by central authorities, blackmail, corruption or error impossible.

3. The delegated MinterBurner has no authority to delegated the mint or burn function to others.

4. The contract owner can take back the MintBurn function from the delegated minterburner to himself or delegate another one.

5. No one can burn his own tokens.

-.-.-.-.-

The following tests and checks should be made to make sure that the token contract code fulfills those requirements:

1. Contract owner can burn his token or mint into his account. True, true
2. Contract owner can burn others tokens or mint into others accounts: No, no
3. Anybody can mint or burn: No, no
4. Someone can self authorize ChangeMinterBurner to himself: No
5. Contract owner can delegate a MinterBurner: True
6. Contract owner can no longer mint or burn: true, true
7. New MinterBurner can mint to or burn form contract owner tokens: No
8. New MinterBurner can burn someone else token or mint to someone else: No
9. New MinterBurner can mint into or burn out from his account: true, true
10. New MinterBurner can delegate the mint-burn role to another account: No
11. Contract owner can take back the mint burn funciton: take back true, mint true, burn true
12. Old MinterBurner can no longer mint or burn: true, true

Testnet contract example which fulfills those requirements fully:

zil1k3hxq95yxaf6urdzpp0kafcl8tglsnwymmn3uh Token: Choco1

Expected results of the 22 transactions for the 12 test questions

1: 2x (mint and burn) true, success

2: 2x error 6 (not sender)

3: 2x error 5 (not minterburner)

4: error 4 (not owner)

5. true, success

6. 2x error 5, not minterburner

7. 2x error 6, not sender

8. 2x error 6, not sender

9. 2x true, success

10. error 4, not owner

11. 3x true, success

12. 2x error 5, not minterburner

Testnet contract example which fulfills those requirements fully:

zil1k3hxq95yxaf6urdzpp0kafcl8tglsnwymmn3uh Token: Choco1