BMToken Contract Guidance

Token Contract Architecture

The BMToken contract is deployed as a TransparentUpgradeableProxy contract. The ProxyAdmin contract is the owner of the TransparentUpgradeableProxy contract.

The BMToken contract itself is simply the implementation contract of the TransparentUpgradeableProxy contract. The owner of the BMToken (the proxy) can be different from the owner of the ProxyAdmin contract. Currently, the owner of the ProxyAdmin contract is the owner of the BMToken (this is set to a multisig safe wallet).

BMToken contract implementation: 0x26b9867a7b5c45899525CD3ECC038047785e5446

TransparentUpgradeableProxy: 0x4A813F287e3964Ec403e50430Ded9B71C1aeC89D

ProxyAdmin: 0x3efd06861Ac03c40Ef01A64DA84D0DBab7E0928B

ERC20: Etherscan Link

TransparentUpgradeableProxy docs: link

IMPORTANT:

The current version of the token was implemented based on the"no features" request. This means:

- The token owner can mint more tokens
- The token owner can burn tokens

To block permission for minting and burning tokens, use the token upgradeability feature to remove ability to mint and burn tokens.

Transfer of Ownership

The transfer of ownership breaks to two parts: transfer of ownership of the token and the transfer of ownership of the upgradeability.

Transfer Ownership for the Token

To change the ownership of the **ProxyAdmin** contract, you can call the `transferOwnership` function of the **ProxyAdmin** contract. This will change the owner of the ProxyAdmin contract to the new owner. You can do this using the safe wallet interface easily.

Similarly, to change the ownership of the **BMToken** (who can mint and burn tokens), you can call the `transferOwnership` function of the **BMToken**. This will change the owner of the **BMToken** to the new owner.

To do this, following the following steps:

1. Go to
   https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA
2. Connect wallet of one of the signers of the multisign
3. Click on "New Transaction"
4. Click on "Transaction Builder"
5. Enter the address of the existing ERC20 token
6. Click on "Use Implementation ABI"
7. Select "Transfer Ownership" from the contract method selector dropdown
8. Enter the address of the new owner
9. Click "Add New Transaction"
10. Click on "Create Batch"
11. Click on "Send Batch"
12. Click on "Sign"

After the above is completed, each person on the multi-sig must go to the Safe Dashboard and follow the steps below.

13. Go to the Safe
    https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA

14. Click on "Transactions" in the safe
15. Click on Queue
16. Click on "Sign"
17. This will execute the transaction and this will remove the ownership from the multisig to the new wallet

Transfer Ownership for the Upgradability

This process is very similar to how you upgrade the ownership of the tokens described above. The only difference is that you will use a different address for the steps 5 (instead of using the token address, use the proxy admin address).

Upgrading Token Smart Contract

To upgrade the token smart contract, follow these steps:

1. Make changes to the **BMToken** contract as seen in the `contracts/test/BMTokenUpgrade.sol` file. This is usually done using your own code editor.

2. Write tests to verify the new functionality doesn't cause any bugs. Sometimes, it's necessary to do code security audit.

3. Deploy the new version of the **BMToken** contract (this contract is referred to as the implementation contract).

You will need the guidance of a solidity developer to do this.

4. Go to https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA

5. Connect wallet of one of the signers of the multisign

6. Click on "New Transaction"

7. Click on "Transaction Builder"

8. Enter the address of the **ProxyAdmin**

9. Click on "upgradeAndCall" from contract method selector

10. Enter the **TransparentUpgradeableProxy** address in the "proxy" field

11. Enter the address of the contract deployed in step 3 into the "implementation" field

12. Enter "0x" in the "data (bytes)" field, unless the new version of the contract requires calling one of its methods with data upon being upgraded to

13. Click on "Add New Transaction"

14. Click on "Create Batch"

15. Click on "Send Batch"

16. Click on "Sign"

After the above is completed, each person on the multi-sig must go to the Safe Dashboard and follow the steps below.

18. Go to the Safe https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA

19. Click on "Transactions" in the safe

20. Click on Queue
21. Click on "Sign"
22. This will execute the transaction and this will upgrade the token smart contract
23. Go on etherscan.io
24. Search for the address of the ERC20 token
25. Click on the "Contract" tab
26. Click on "Is this proxy?" under the "More options" tab on the top right above the source code on the top right
27. Click on "Verify"
28. The upgrade has been completed

Minting Tokens

The owner of the BMToken can mint tokens as long as they are given the permission based on the smart contract.

To mint tokens, follow these steps:

1. Go to https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA
2. Connect wallet of one of the signers of the multisign
3. Click on "New Transaction"
4. Click on "Transaction Builder"
5. Enter the address of the existing ERC20 token
6. Click on "Use Implementation ABI"
7. Select "Mint" from the contract method selector dropdown
8. Enter the address of whoever address you want to mint for
9. Enter the amount multiplied by 10 to the power of 18
10. Click "Add New Transaction"
11. Click on "Create Batch"
12. Click on "Send Batch"
13. Click on "Sign"

After the above is completed, each person on the multi-sig must go to the Safe Dashboard and follow the steps below.

14. Go to the Safe https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA
15. Click on "Transactions" in the safe
16. Click on Queue
17. Click on "Sign"
18. This will execute the transaction and will mint new tokens to the specified address

Burning Tokens

The owner of the BMToken can burn tokens as long as they are given the permission based on the smart contract.

To burn tokens, follow these steps:

1. Go to https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA
2. Connect wallet of one of the signers of the multisign
3. Click on "New Transaction"
4. Click on "Transaction Builder"
5. Enter the address of the existing ERC20 token
6. Click on "Use Implementation ABI"
7. Select "Burn" from the contract method selector dropdown
8. Enter the address of whoever address tokens you want to burn
9. Enter the amount multiplied by 10 to the power of 18
10. Click "Add New Transaction"
11. Click on "Create Batch"
12. Click on "Send Batch"
13. Click on "Sign"

After the above is completed, each person on the multi-sig must go to the Safe Dashboard and follow the steps below.

14. Go to the Safe https://app.safe.global/home?safe=sep:0x1b6636861FaaB3410f3EE10Dec5256b149Aa78BA
15. Click on "Transactions" in the safe
16. Click on Queue
17. Click on "Sign"
18. This will execute the transaction and will burn new tokens from the specified address