

The screenshot shows a web interface for deploying and running transactions. The left sidebar contains a 'DEPLOY & RUN TRANSACTIONS' panel with various input fields and buttons. The main area displays the Solidity code for 'ERC20_AccessControl.sol'. The code includes functions 'mint' and 'burn' with role-based access control. Below the code, a transaction history shows a successful deployment to the Rinkeby testnet, including a constructor call and subsequent calls to 'MINTER_ROLE' and 'BURNER_ROLE'.

```
15 }
16
17 * function mint(address to, uint256 amount) public {
18     require(hasRole(MINTER_ROLE, msg.sender), "Caller is not a minter");
19     _mint(to, amount);
20 }
21
22 * function burn(address from, uint256 amount) public {
23     require(hasRole(BURNER_ROLE, msg.sender), "Caller is not a burner");
24     _burn(from, amount);
25 }
26 }
```

ContractDefinition ERC20_Covid19_Token_AccessControl 0 reference(s) ^ v

0 listen on network Search with transaction hash or address

<https://rinkeby.etherscan.io/tx/0x65024d6702101653082d7a7dc4067d66afbbbc3c69a003cfd75f7850e9a4b158>

[block:7923168 txIndex:5] from: 0x616...75209 to: ERC20_Covid19_Token_AccessControl.(constructor) value: 0 wei data: 0x608...75209 logs: 2 hash: 0x650...4b158 Debug v

call to ERC20_Covid19_Token_AccessControl.MINTER_ROLE

[call] from: 0x616dAC0287cE79A3A537562058993F09C9275209 to: ERC20_Covid19_Token_AccessControl.MINTER_ROLE() data: 0xd53...91393 Debug v

call to ERC20_Covid19_Token_AccessControl.BURNER_ROLE

[call] from: 0x616dAC0287cE79A3A537562058993F09C9275209 to: ERC20_Covid19_Token_AccessControl.BURNER_ROLE() data: 0x282...c51f3 Debug v

<https://rinkeby.etherscan.io/tx/0x65024d6702101653082d7a7dc4067d66afbbbc3c69a003cfd75f7850e9a4b158>