Practical 5

Blockchain Technology 2CSDE93

Dhruv Sonani 20BCE527

Date

November 14, 2022



Department of Computer Science and Engineering Institute of Technology

Nirma University
Ahmedabad

Aim: To implement a custom token like ERC_20 token of ethereum blockchain and add functionalities like burn tokens, mint new tokens and whitelist a address(whitelisting allows the contract to transfer tokens only if address is whitelisted by Owner).

Code

```
pragma solidity ^0.5.1;
// SAFE Mathematical Operations
library SafeMath {
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
      assert(b <= a); //error handling condition</pre>
      return a - b; //To Avoid Overflows
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
      uint256 c = a + b;
      assert(c >= a);
     return c;
contract IntelliContract {
    string public constant name = "CustomEnergyToken"; // solidity
automatically creates a getter function for public variables
    string public constant symbol = "CET"; // getter function is a function
    uint8 public constant decimals = 18; // Similar to Ether
    event Approval(address indexed tokenOwner, address indexed spender, uint
tokens);
    event Transfer(address indexed from, address indexed to, uint tokens);
    modifier onlyOwner {
        require (msg.sender == ownerCon);
        _;
```

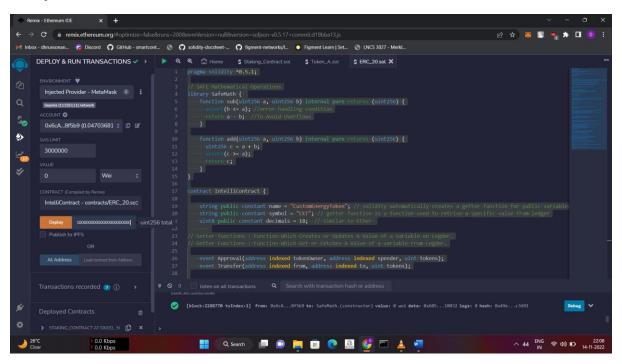
```
mapping(address => uint256) balances;
   mapping(address => bool) whiteList addresses;
   mapping(address => mapping (address => uint256)) allowed; // nested
   uint256 totalSupply_;
   address ownerCon;
   using SafeMath for uint256;
   constructor(uint256 total) public { // special function , only called at
time of deployemnet
    totalSupply_ = total ;
    balances[msg.sender] = total ; // To Deposit all the newly generated
   whiteList_addresses[msg.sender] = true;
    ownerCon = msg.sender;
    function totalSupply() public view returns (uint256) {
    return totalSupply_;
    function balanceOf(address inputAddress) public view returns (uint) {
       return balances[inputAddress];
    function transfer(address receiver, uint numTokens) public
IsWhiteListed(receiver) returns (bool) {
        require(numTokens <= balances[msg.sender], "Not Sufficient Balance");</pre>
        balances[msg.sender] = balances[msg.sender].sub(numTokens);
        balances[receiver] = balances[receiver].add(numTokens);
        emit Transfer(msg.sender, receiver, numTokens); // logging these
       return true;
```

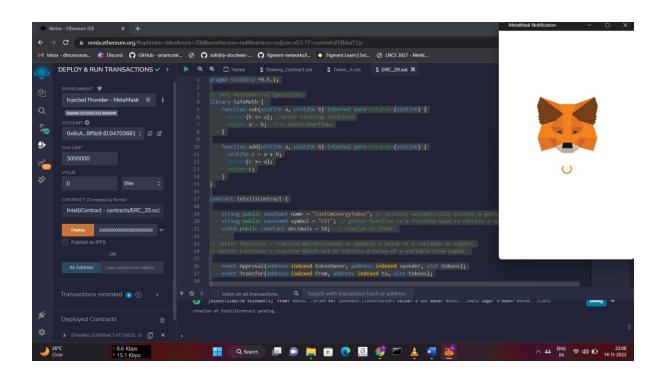
```
function approve(address approved_addr, uint numTokens) public returns
(bool) {
        allowed[msg.sender][approved addr] = numTokens;
        emit Approval(msg.sender, approved_addr, numTokens);
        return true;
    function allowance(address owner, address token manger) public view
returns (uint) {
       return allowed[owner][token_manger];
    function transferFrom(address owner, address buyer, uint numTokens) public
returns (bool) {
        require(numTokens <= balances[owner]);</pre>
        require(numTokens <= allowed[owner][msg.sender]);</pre>
        balances[owner] = balances[owner].sub(numTokens);
        allowed[owner][msg.sender] =
allowed[owner][msg.sender].sub(numTokens);
        balances[buyer] = balances[buyer].add(numTokens);
        emit Transfer(owner, buyer, numTokens);
       return true;
    function Mint_New_Tokens(uint256 numTokens)external onlyOwner{
        require(numTokens>0, "Enter the number of tokens more than 0");
        balances[msg.sender] = balances[msg.sender].add(numTokens);
        totalSupply_ = totalSupply_.add(numTokens);
        emit Transfer(address(0), msg.sender, numTokens);
    function burnTokens(uint256 numTokens) external onlyOwner{
        require(numTokens<=balances[msg.sender],"Not enough tokens to burn");</pre>
        require(numTokens>0, "Enter the number of tokens more than 0");
        balances[msg.sender] = balances[msg.sender].sub(numTokens);
        totalSupply_ = totalSupply_.sub(numTokens);
        emit Transfer(msg.sender,address(0),numTokens);
    function whiteList_A_Address(address add_To_whitelist)public onlyOwner{
        whiteList_addresses[add_To_whitelist] = true;
    modifier IsAlreadyWhitelisted(address VerifyAddress){
```

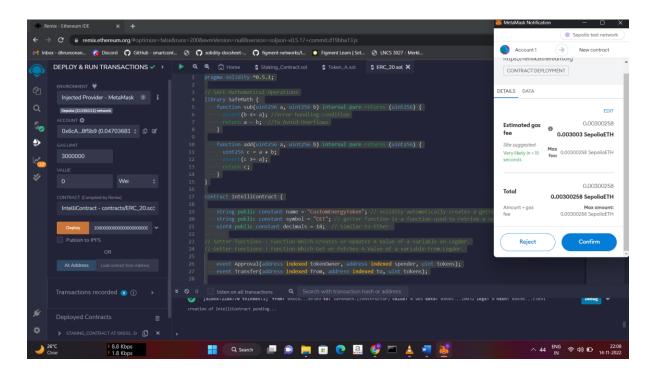
```
require(whiteList_addresses[VerifyAddress] == true, "Address is
already whitelisted");
    _;
}

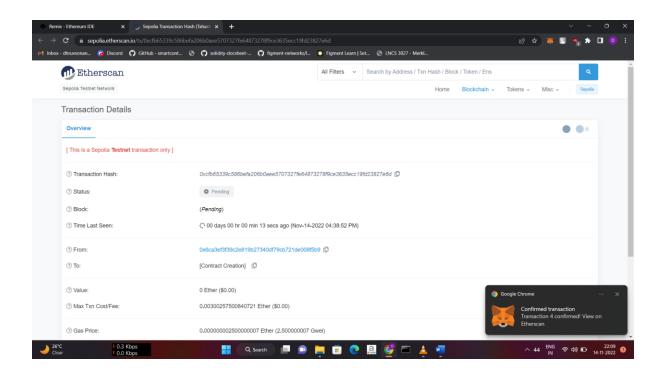
modifier IsWhiteListed(address VerifyAddress){
    require(whiteList_addresses[VerifyAddress] == true, "Address needs to
be whitelisted");
    _;
}
}
```

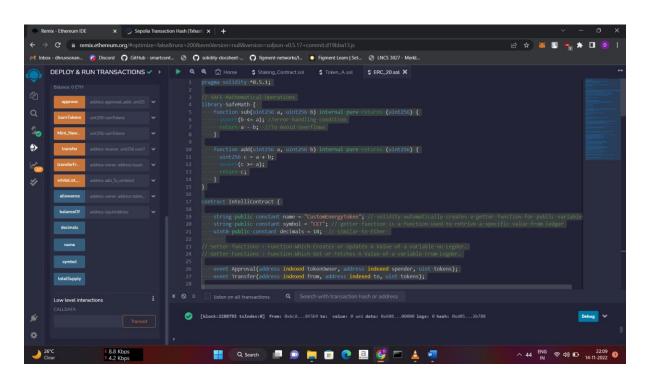
Output:



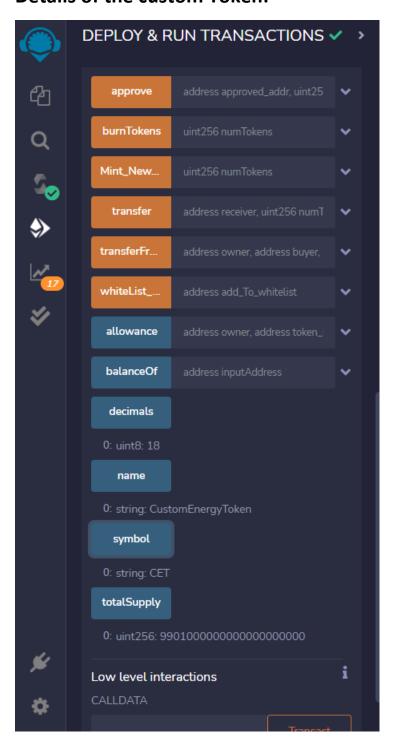




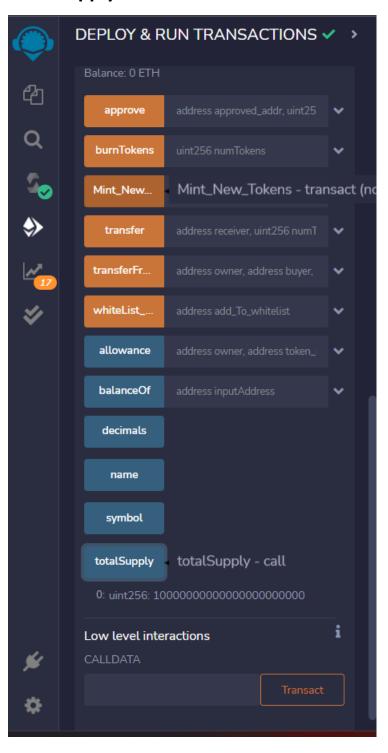




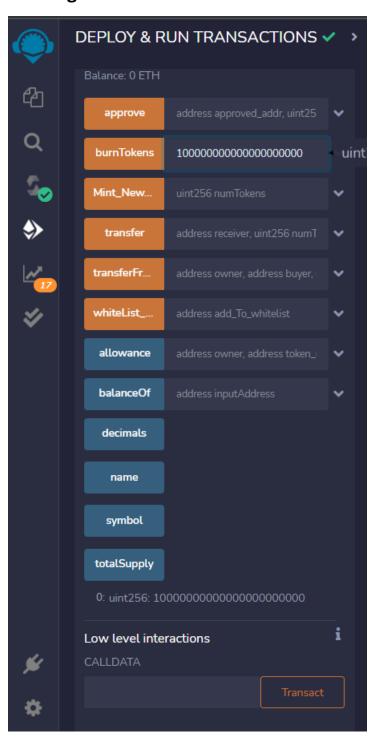
Details of the custom Token:

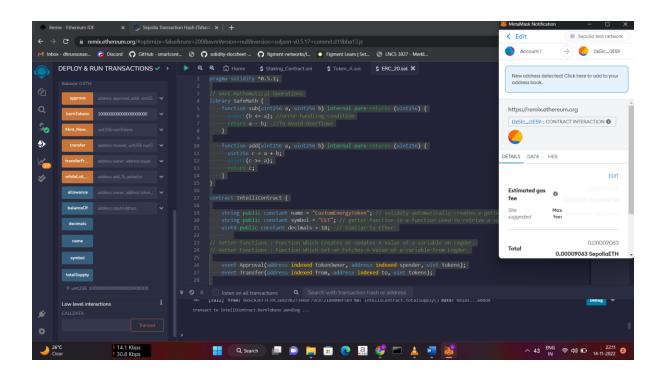


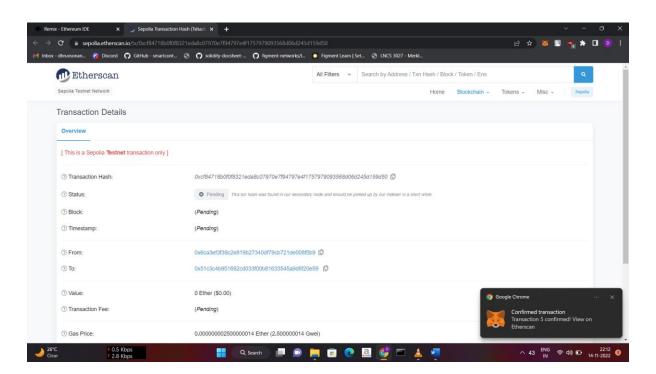
Total supply of custom token:

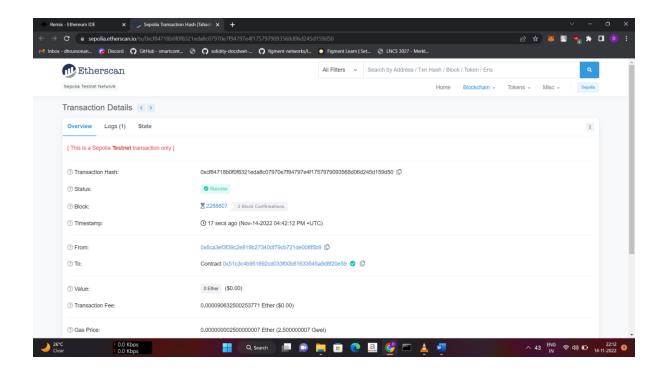


Burning 100 Custom Tokens:

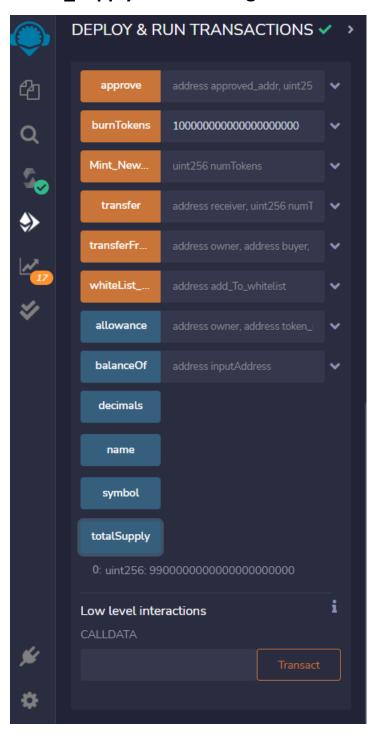




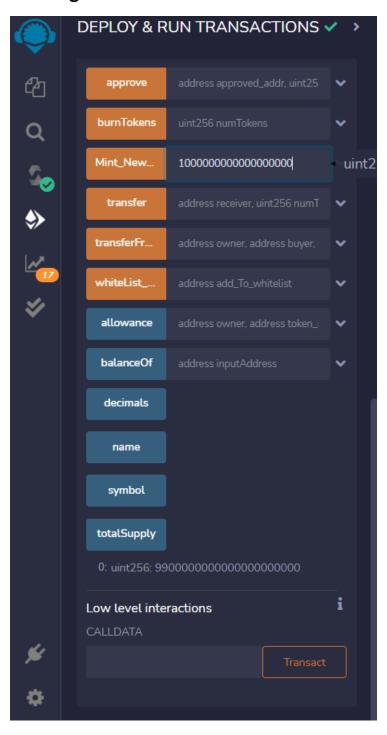


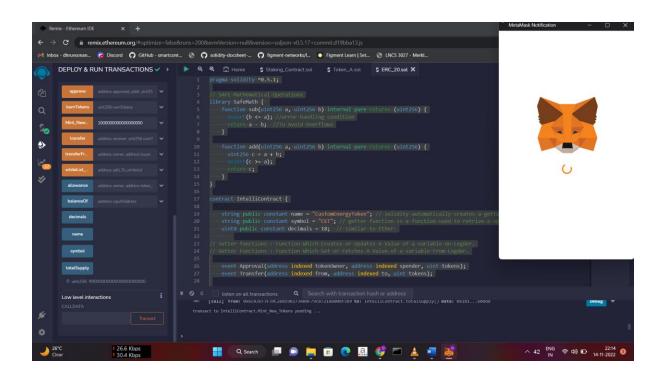


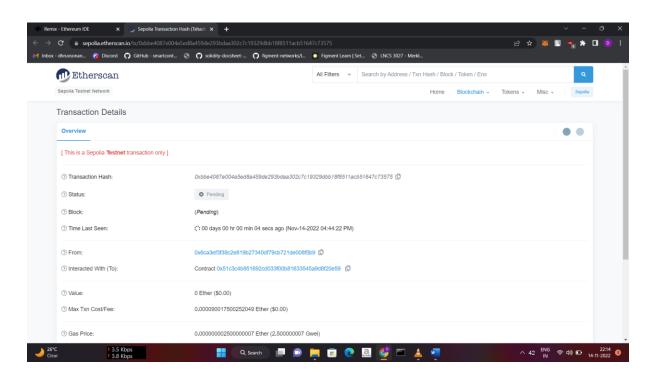
Token_Supply after burning:

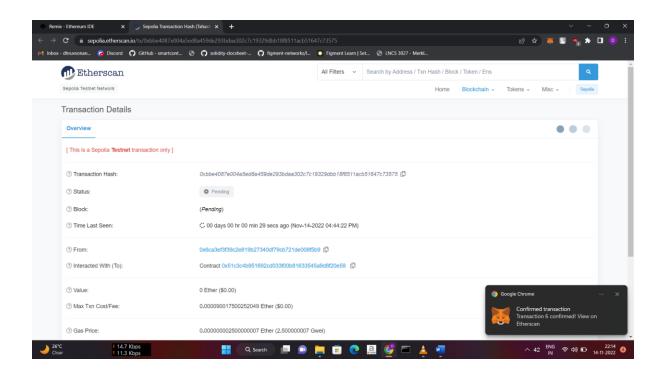


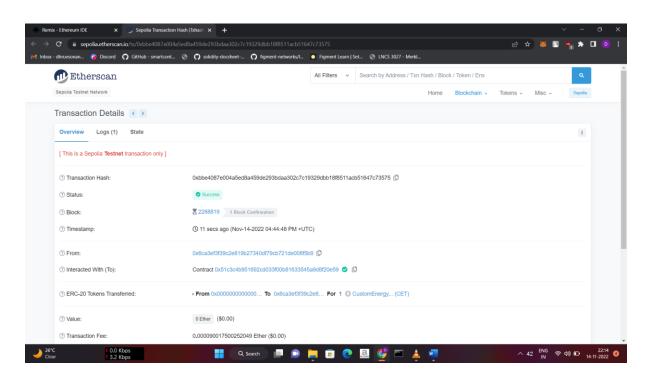
Minting new custom tokens:



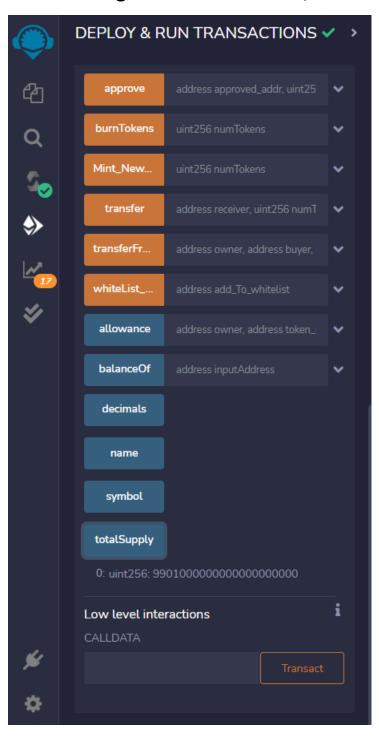




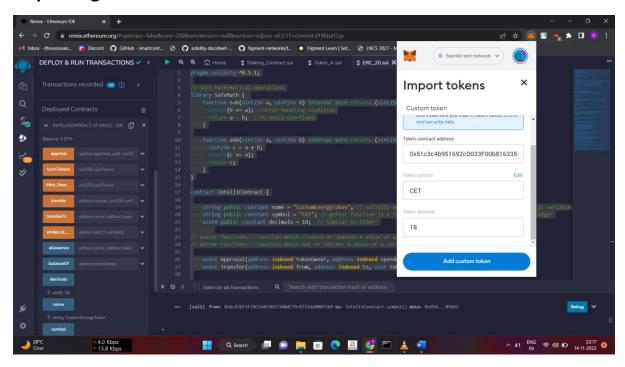


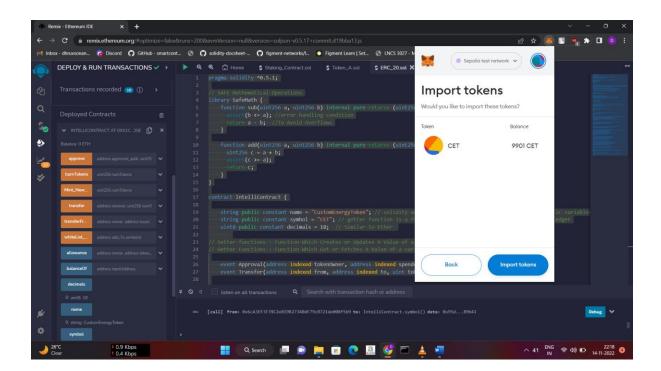


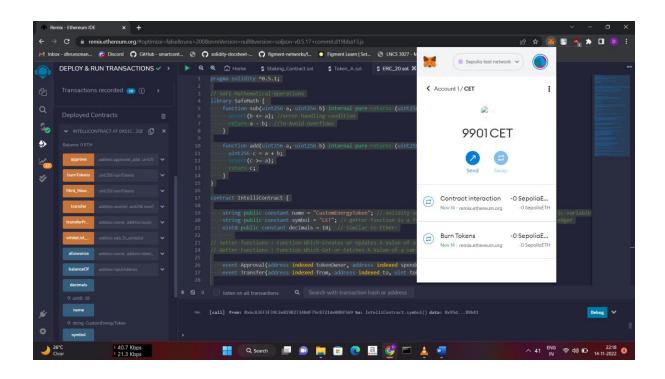
After minting new custom tokens, total supply:



Importing Tokens into metamask wallet:







Whitelist a address(here we are whitelisting our account 2 of metamask):

