BlockBloom Project Assignment 2

Manas Todi
Roll Number: 230627

December 29, 2024

Answers

1. Address

`0x45C3b02B1495faA8CC213c8AE41bE4C185cda51e`

2. Ethereum

Ethereum is a blockchain network that allows people to build and run smart contracts and decentralized applications (dApps) without relying on middlemen. It expands the idea of blockchain beyond just digital currency. Ethereum uses smart contracts, which are self-executing pieces of code that run when certain conditions are met. These contracts remove the need for intermediaries and help automate processes securely.

The platform runs on the Ethereum Virtual Machine (EVM), ensuring that any application can run as programmed, no matter where it is executed.

Ethereum initially relied on Proof of Work (PoW) for transaction validation but later transitioned to Proof of Stake (PoS) to make the network more energy-efficient and scalable. It also introduced the concept of gas fees, which are small payments required to perform transactions or execute contracts on the network.

Ethereum has been the foundation for innovations like Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), and Decentralized Autonomous Organizations (DAOs).

3. Contract Deployment

I was unable to deploy the contract as it continuously reported: *Not enough balance. You need to buy more ETH.*

Here is the contract code that was asked to be shared:

```
// SPDX-License-Identifier: MIT
// Compatible with OpenZeppelin Contracts ^5.0.0
pragma solidity ^0.8.22;

import {ERC721} from "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import {ERC721URIStorage} from "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import {Ownable} from "@openzeppelin/contracts/access/Ownable.sol";
```

```
8
9     contract MyToken is ERC721, ERC721URIStorage, Ownable {
10        uint256 private _nextTokenId;
11
12        constructor(address initialOwner)
13            ERC721("MyToken", "MTK")
14            Ownable(initialOwner)
15        {}
16
17        function safeMint(address to, string memory uri) public
              onlyOwner {
18            uint256 tokenId = _nextTokenId++;
19            _safeMint(to, tokenId);
20            _setTokenURI(tokenId, uri);
21        }
22
23        function tokenURI(uint256 tokenId)
24            public
25            view
26            override(ERC721, ERC721URIStorage)
27            returns (string memory)
28        {
29            return super.tokenURI(tokenId);
30        }
31
32        function supportsInterface(bytes4 interfaceId)
33            public
34            view
35            override(ERC721, ERC721URIStorage)
36            returns (bool)
37        {
38            return super.supportsInterface(interfaceId);
39        }
40    }
```

4. Blockchain Wallets

A wallet in blockchain is a tool that allows users to store, send, and receive cryptocurrencies. It doesn't actually store the cryptocurrency itself but securely manages the private keys needed to access and sign transactions on the blockchain.

Software Wallets: Digital applications that store private keys online or on a device (e.g., desktop, mobile). Convenient but vulnerable to hacking.

Hardware Wallets: Physical devices that store private keys offline, offering better security but less convenience.

Examples include:

- Trust Wallet
- Ledger Nano S (Hardware)
- Atomic Wallet

Wallets uphold the principle of decentralization by maintaining user control over private keys and funds, rather than centralizing ownership with the wallet provider.

5. Zero Address in Blockchain

The Zero Address, often represented as `0x0000000000000000000000000000000000000000` in Ethereum, is a special placeholder address with no private key associated. It is used for:

- Removing tokens or assets from circulation.
- Serving as a default value for uninitialized addresses.

Finding the private key corresponding to the Zero Address is computationally infeasible due to the vast cryptographic key space.

6. Brave Browser and BAT Token

The Brave browser, built on Chromium, is known for its ad-blocking features, privacy settings, and the Basic Attention Token (BAT) reward system. It also consumes less RAM compared to Google Chrome.

BAT System: Users can earn BAT tokens by viewing ads and use these tokens to support their favorite creators.

7. ...

8 & 9. The answers to questions 8 and 9 can be found in the following notebook:

Notebook Link.

9. Attempt

Tried but unable to complete.