BlockBloom Assignment 2

1. Create a Metamask account and share your address.
   Account Address : 0x11AE6Bd39C774946535D5e0d78754B03027922f7
2. Summary :
   ETHEREUM WHITEPAPER -Vitalik Buterin, 2014.

- Limitations with Scripting languages such as used in Bitcoin :
  - Loops are not supported which prevents any potential Denial of Service or DoS attacks. As there are no loop, every script is assured to be terminated. But this make the language **Turing Incomplete**. Now for imitating loops, we'll have to repeat maybe the if statments which leads to space inefficiency. For eg: implementing the alternative elliptic curve signature algorithm.
  - Bitcoin's UTXO model treats outputs as discrete units of cryptocurrency with no awareness of their value in terms of external metrics (e.g., USD). A UTXO is either spent entirely or not at all; partial withdrawals are not possible. So if you want to pay someone in dollars, firstly the oracle will determine the value of 1 USD and then too, to make up the sum we would need different denominations of BTC.

- **ETHEREUM** :
  - Basically what it does differently in fundamental aspect is provide a blockchain with *TURING COMPLETE* language. What is means is say you have a logic to build a specific contract that cater to your needs, boom you can implement that in ethereum. Now you can create
    your own rules for ownership, transaction formats and state transition functions
  - Alternative protocol for dApps with rapid dev time, efficient in interactions.

- **ETHEREUM ACCOUNT**
  - HAS FOUR FIELDS : NONCE, ETHER BALANCE, CONTRACT CODE AND STORAGE.
  - Two types of accounts : Externally Owned Accounts (has a private key) or EOAs and Contract Accounts (has some executable code which controls it). Contract here means like some autonomous agent which are activated when called upon.

- **Transactions**
  - Transaction is basically sending a message from externally owned account but it has to contain few more essential things.
  - The recipient of the message
  - A signature identifying the sender

    - The amount of ether to transfer from the sender to the recipient
    - An optional data field
    - A STARTGAS value, representing the maximum number of computational steps the transaction execution is allowed to take.
    - A GASPRICE value, representing the fee the sender pays per computational step.
    - Because unlike Bitcoin, we can write for loops in Ethereum. The concept of gas is essential to stop infinite loops or computational wastage.
- **Messages**
    - Messages are a way for contract to send informations/commands to other contracts. Note there are no external actors. These are vitrual objects that exist in Ethereum execution environment only.
    - Unlike Transactions, there are few less fields in it namely :
    - The sender of the message (implicit)
    - The recipient of the message
    - The amount of ether to transfer alongside the message
    - An optional data field
    - A STARTGAS value
    - This way contracts can have relationships with other contracts in exactly the same way that external actors can.

- **ETHEREUM STATE TRANSITION FUNCTION**
    - Transaction Validation:
        - Ensure the transaction is well-formed, the signature is valid, and the nonce matches the sender's account. Return an error if these checks fail.
    - Transaction Fee Calculation:
        - Compute the fee as STARTGAS * GASPRICE.
        - Deduct the fee from the sender’s balance and increment the sender's nonce.
        - Return an error if the sender lacks sufficient balance.
    - Gas Initialization:
        - Set GAS = STARTGAS.
        - Deduct gas per byte for transaction data.
    - Value Transfer and Contract Execution:
        - Transfer the transaction value to the recipient.
        - Create the recipient account if it does not exist.
        - If the recipient is a contract, execute its code until completion or gas depletion.

        - Failure Handling:
            - Revert state changes (except fee deduction) if the transfer fails or gas is exhausted.
            - Add the fees to the miner's account.
        - Gas Refund and Miner Reward:
            - Refund unused gas fees to the sender.
            - Pay gas fees for consumed gas to the miner.
    - **CODE EXECUTION**
        - The code is written in EVM or Ethereum virtual machine code. It is a bytecode language, basically the code consists of bytes each of which represents an operation, so we need to just read the bytes one by one and do the operation untill there are no more bytes or stop operation is encountered.
        - The contracts has stack and memory for carrying out operations and a storage for storing data that may be used even after the computation has ended.

3. Contract Address : 0xFF695d79BEc2515F862fF854DC3324c8Cdc65193

4. What is a wallet? What are software and hardware wallets? Why don’t wallets break the principle of decentralization? List out a few wallets other than Metamask.

    - A wallet is a device, program, or online service that stores and manages your cryptocurrency keys and coins.
    - These may be web based like SOFTWARE wallets. For eg. Metamask.
    - These may be physical devices that can perform offline transactions.
    - Wallets store your private keys but they use
    - Some wallets other than Metamask : Coinbase, Exodus, CoinDCX, Zebpay.

5. What is the relevance of Zero address? Comment on the effort required to get the private key corresponding to the Zero address.

    - The zero address, also known as the null address or the zero account, refers to the Ethereum address: 0x0000000000000000000000000000000000000000 .
    - It is a special because since address are generated from a fix method, it is very difficult to recover the private key from the address, so we can treat this address as dummy or dustbin where the token to be burned are transferred to this account. Or tentative token and contracts are associated with this address.
    - It is often used as the default address when no valid address is set or for initializing address-type variables in smart contracts. When tokens or assets are sent to the

Zero Address, they are effectively "burned," making them unrecoverable and removing them from circulation.

   - Ethereum addresses are derived using the Keccak-256 hash function, which ensures a one-way mapping. Finding the private key that maps to the Zero Address would require inverting this cryptographic hash function.
   - To discover the private key by brute force, one would have to test 2^ 256 possible private keys. This is an astronomically large number, far beyond the capability of any existing computational resources.

6. Find out what is Brave Browser and BAT token. (For interested people: Install Brave Browser and explore it.)

   - Brave is a browser developed by the creator of javascript and mozilla. It is different from the contemporaries in a way that it allows a means to blocks ads that **pop up** while using regular browsers.
   - But the creators usually earn through these ads, now since Brave stopped these ads, this means of earning vanished for creators but to tackle this, they created a **brave creator program** where they can earn in cryptocurrency and the users of the browser are also incentivized through the same crypto if they opt to see ads. Brave created a new ads showing technique, they use ML algorithms to track user activity and based on that data which never leave the device of the user, from a catalogue of ads, most relevant of them are shown to the user and that also is dependent on the user how many ads they want to see per hours, and the rewards is also relative.
   - The cryptocurrency is named as Brave Attention Token or BAT. The users can in return support their favourite creators by paying them in BAT they earn as rewards.