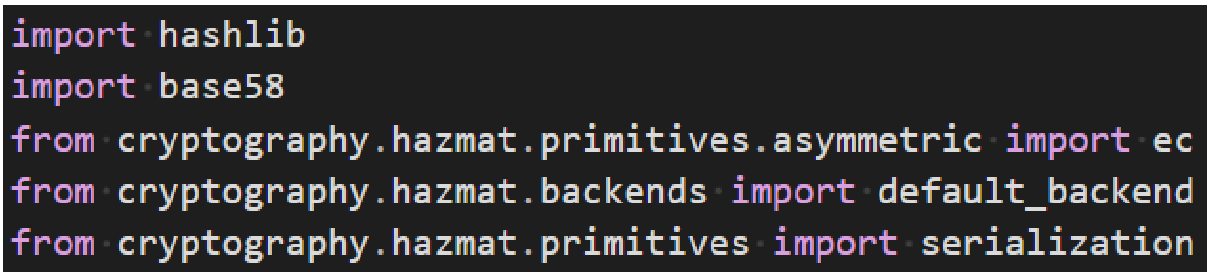
Lab 15-06-2023

1. Write a program to generate a bitcoin wallet from your public key. For that please follow the following steps

   a. Import the required libraries that are mentioned below:

   ```python
   import hashlib
   import base58
   from cryptography.hazmat.primitives.asymmetric import ec
   from cryptography.hazmat.backends import default_backend
   from cryptography.hazmat.primitives import serialization
   ```

   Run the code to check whether you have the above mentioned libraries installed. If you don't have base58 and cryptography libraries installed, you can install it by typing "pip install base58" and "pip install cryptography" in your VSCode terminal.

   b. Write a function that generates and returns the ECDSA public and private keys.

   c. Write a function that takes the ECDSA public key as input parameter and returns a bitcoin wallet address. You can follow the steps shown in figure 1.
   [Note: To pass the public key as bytes you can use the public_bytes method from cryptography library.

   ```
   publicKeyBytes = publicKey.public_bytes(
      encoding=serialization.Encoding.X962,
      format=serialization.PublicFormat.UncompressedPoint
   )]
   ```

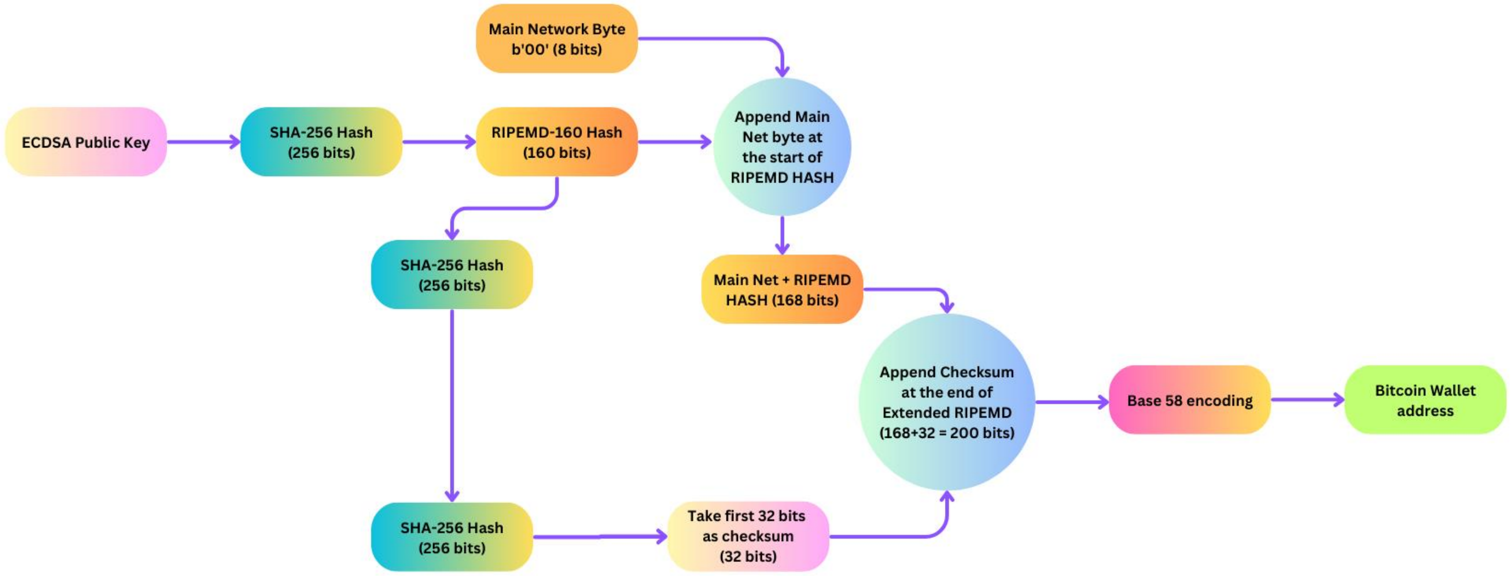
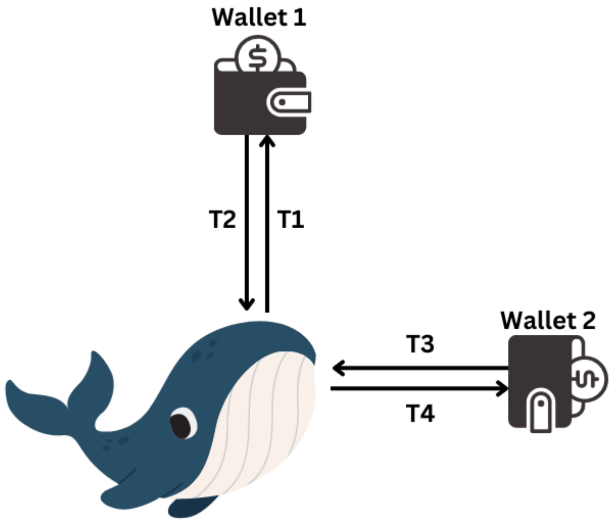

Main Network Byte b'00' (8 bits)
ECDSA Public Key
SHA-256 Hash (256 bits)
RIPEMD-160 Hash (160 bits)
Append Main Net byte at the start of RIPEMD HASH
SHA-256 Hash (256 bits)
Main Net + RIPEMD HASH (168 bits)
Append Checksum at the end of Extended RIPEMD (168+32 = 200 bits)
Base 58 encoding
Bitcoin Wallet address
SHA-256 Hash (256 bits)
Take first 32 bits as checksum (32 bits)

Figure 1 Generation of a Bitcoin address

2. For the next hands on exercise visit blockchain.com, identify any transaction in which more than 20 bitcoins have been exchanged. Note down the wallet address (Wallet A), search for it and find any of the two other wallets (Wallet B & Wallet C) associated in other transactions with it. Establish a pattern such that the wallets have done more than two transactions with each other.


Wallet 1
T2
T1
T3
T4
Wallet 2