# Question 1

## Part 1 (generate bitcoin private key)

For this part, we generate a random 256 bit(32 byte) number for private key.

random\_number = random.getrandbits(256)

private\_key = random\_number.to\_bytes(32, byteorder="big")

To generate the Wallet Import Format (WIF) of a private key, the following steps can be followed:

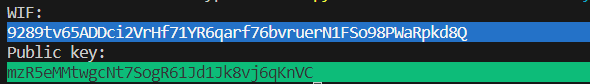
1. Start with the private key in its hexadecimal format.
2. Add the test network prefix (0xEF) to the beginning of the private key (0x80 for main network).
3. Perform a double hash operation on the extended private key using a cryptographic hash function, such as SHA-256.
4. Take the first 4 bytes of the resulting hash and append them to the extended private key.
5. Encode the extended private key, including the appended checksum, into a base58 encoding algorithm.
6. The resulting string is the WIF representation of the private key.1

By following these steps, the private key can be converted into a WIF format that is commonly used for importing private keys into cryptocurrency wallets.

To generate a public key based on a given private key, the following steps can be followed:

1. Utilize the ECDSA (Elliptic Curve Digital Signature Algorithm) to generate a public key corresponding to the provided private key.
2. Add the public key prefix (0x04) to the beginning of the generated public key. This prefix distinguishes uncompressed public keys.
3. Apply a hash function, such as SHA-256, followed by RIPEMD160, to the public key. This process results in a hashed value.
4. Prepend the test network prefix (0x6f) to the hashed value obtained in the previous step. This prefix is used to identify the network or purpose for which the public key is intended.
5. Calculate the double hash of the extended key using SHA-256, obtaining a new hash result.
6. Append the first 4 bytes (checksum) of the double hash to the end of the extended key.
7. The resulting string is the public key derived from the given private key.

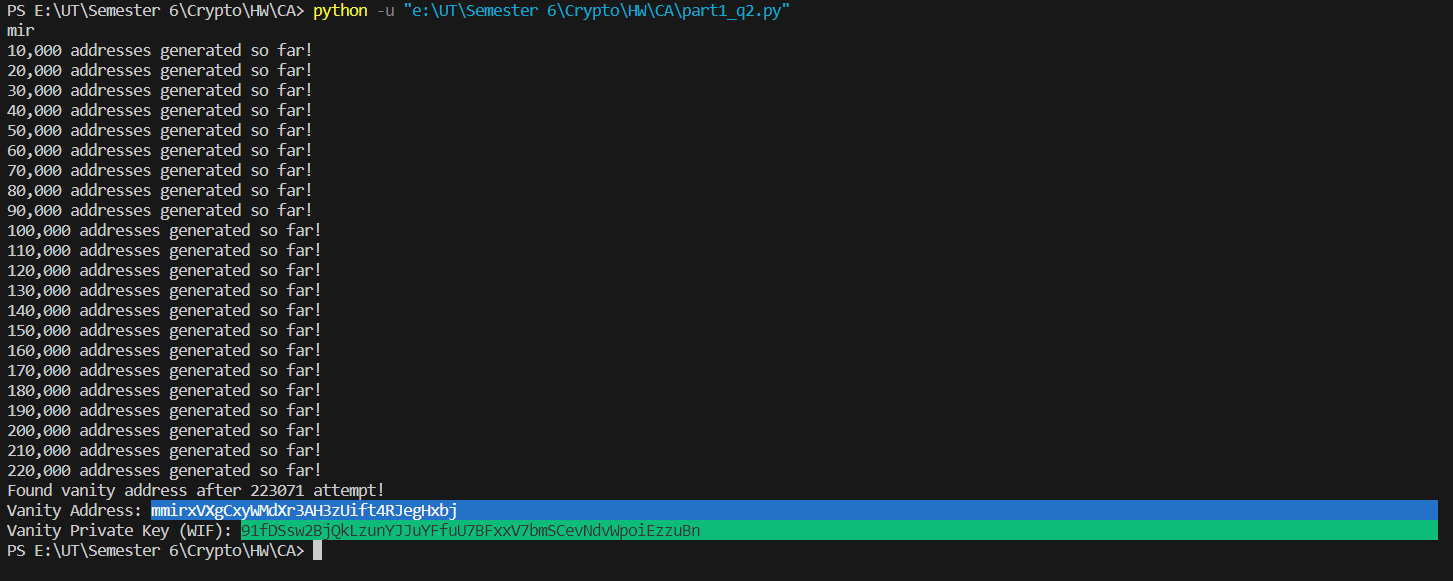
By following these steps, the public key can be obtained from a private key.

Figure 1 test result

## Part 2 (generate bitcoin address)

In the following section, we focus on generating a vanity address based on a user-defined input string. A vanity address is an address that contains a specific subset of characters, starting from the second character and ending at the [2+n]th character of the Bitcoin public key address. To determine the number of attempts required to achieve the desired vanity address, we implement a code that iteratively searches for a matching address.

Please note that when the input string is longer than three characters, the calculation process can be time-consuming due to the increased complexity of finding a matching subset.

Figure 2: Vanity address generation result starting with “mir”

Found vanity address after 223071 attempts!

Vanity Address: mmirxVXgCxyWMdXr3AH3zUift4RJegHxbj

Vanity Private Key (WIF): 91fDSsw2BjQkLzunYJJuYFfuU7BFxxV7bmSCevNdvWpoiEzzuBn

# Question 2

To acquire a certain amount of Bitcoin on the test network, we can utilize a faucet website2.

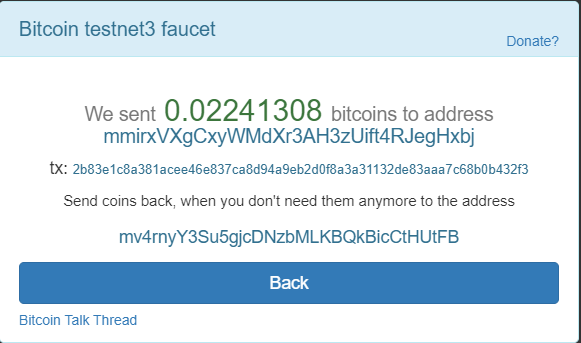


Figure 3: Bitcoin Received on the Provided Address

After initiating a transaction, it is essential to wait for a certain number of blocks to be added to the blockchain to ensure the transaction is securely recorded and considered final. Generally, a common practice is to wait for at least six blocks, which provides a sufficient level of confirmation for the transaction.

We initiated a transaction with one input and two outputs. Figure 4 illustrates the structure of this transaction. The purpose of the two outputs is as follows:

1. The first output, as depicted in Figure 4, is not spendable and is utilized to return the Bitcoin amount to the faucet address. This ensures that any remaining funds or change from the transaction are returned to the original source.
2. The second output, also shown in Figure 4, is spendable and can be used to transfer the specified Bitcoin amount to the provided address. This output allows the Bitcoin to be sent to the designated recipient.

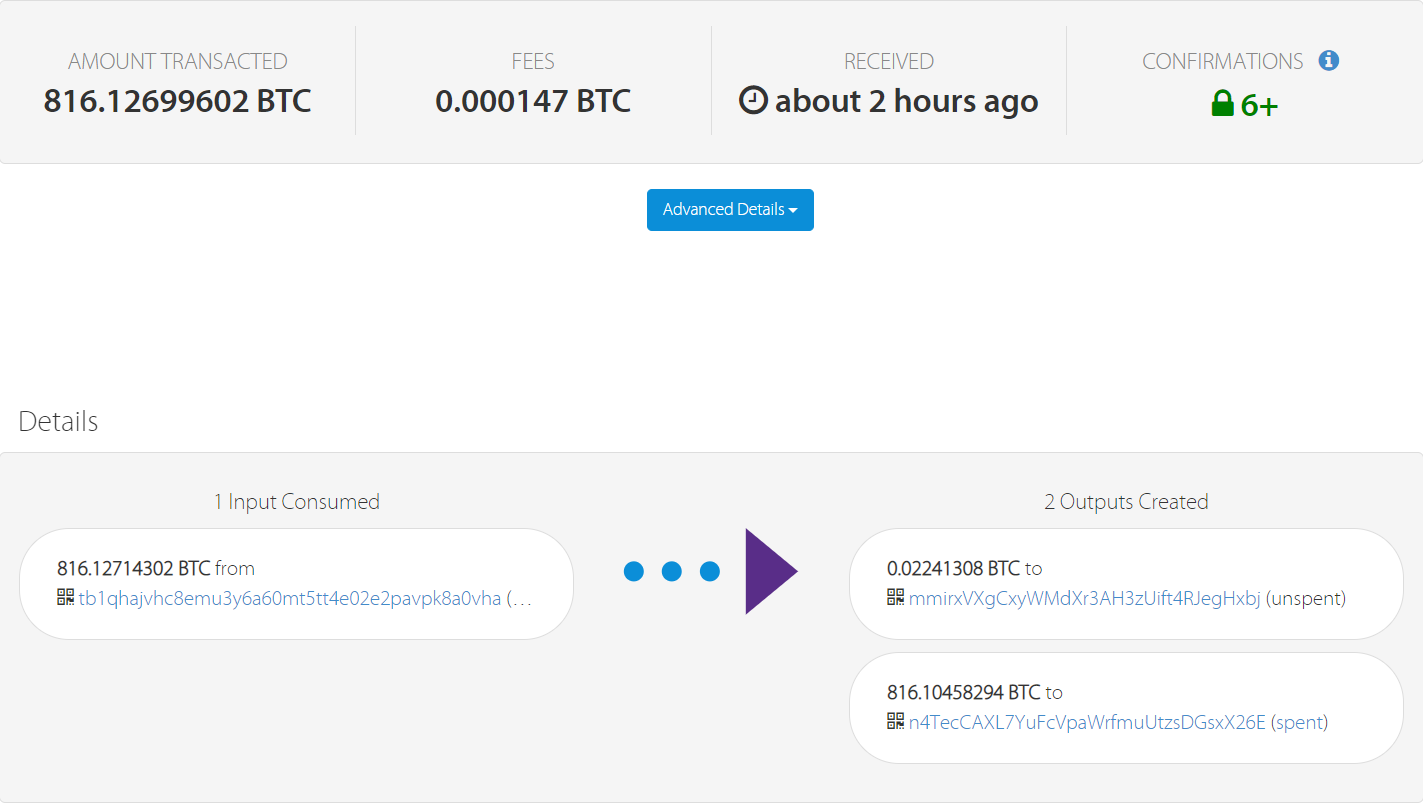
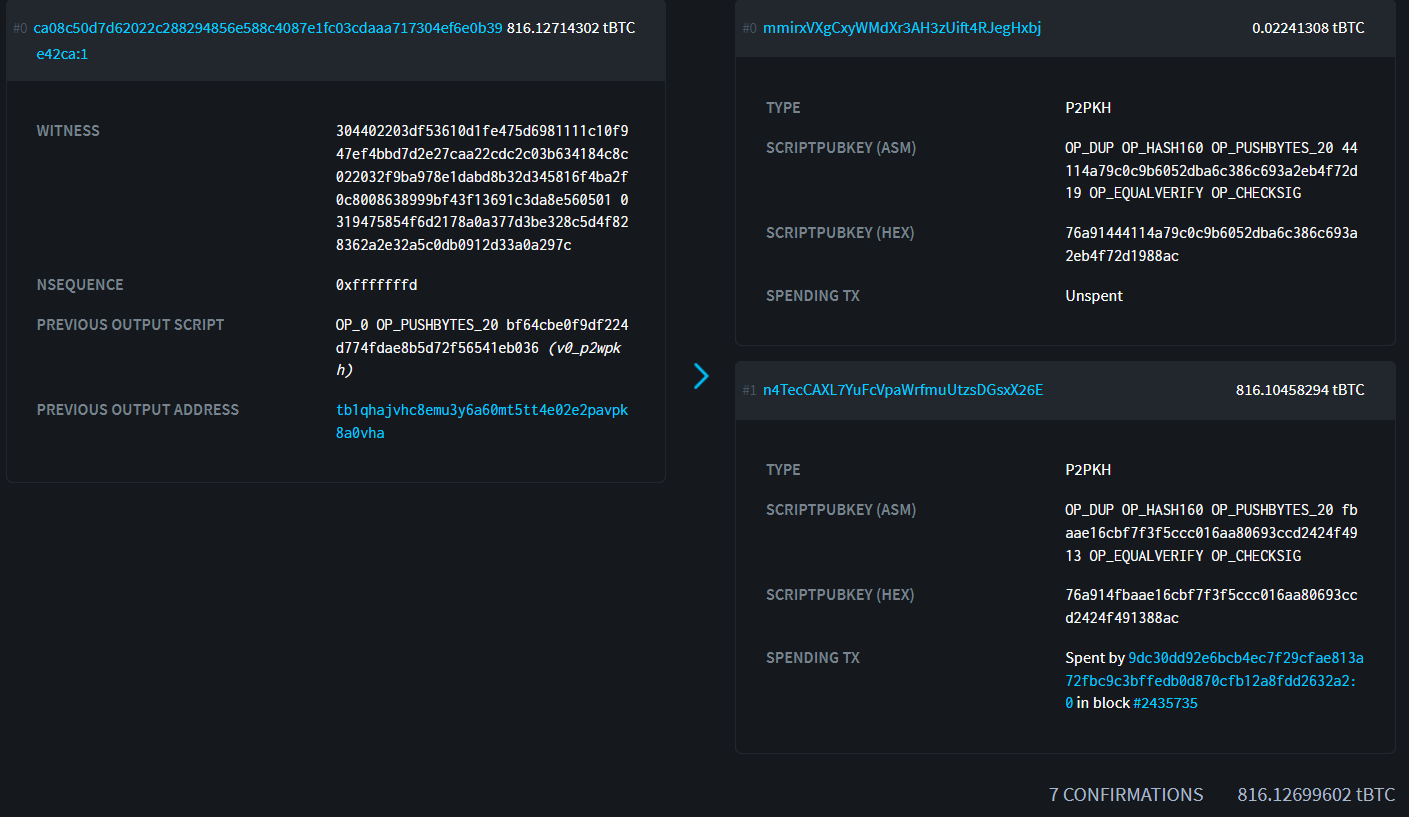


Figure 4

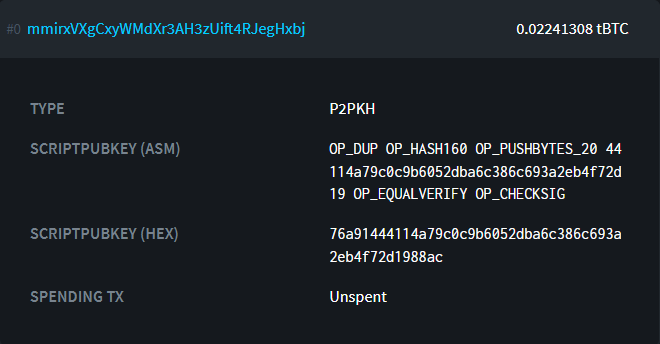
To complete the transaction.py file, we utilized a specific [website](https://blockstream.info/testnet/tx) to study our transaction and analyze the script used within it. This website provided valuable insights and information regarding the transaction structure and associated scripts as shown in figure 5.

Figure 5

## Part 1

Utilizing the provided script, we implemented the necessary logic using script shown in figure 6 within the transaction.py file. This logic allows us to spend the unspent portion of the faucet transaction and generate a new transaction with one input and two outputs.

The first output is designated as spendable, allowing the specified Bitcoin amount to be sent to the desired address. The second output is configured as not spendable, serving the purpose of returning any remaining funds or change back to the faucet address.

Figure 6