Middle East Technical University | Department Of Cyber Security

CSEC 519

Blockchain and Cryptocurrency Technologies

Spring 2024-2025

Third Assignment

Name Surname: Alkım Doğan
Student ID: 2521482

1

The hash value of the block is **0000000000000023e1a9140165def5a8a922b30a0f04046d9580b150cd9a155b**. It starts with $4 \times 14 + 2 = 58$. It starts with **58** zeros in terms of bits.

2

The output value is **25.17985793 BTC**. It was mined/broadcasted on 14 Aug 2013 08:23:55 GMT+3. Its block reward is **25 BTC** and transaction fee reward is **0.17985793 BTC**. As far as I have observed, there is no extra to included in the coinbase transaction in order to solve the puzzle. There could have been some message but there is not one.

3

There are **277** transactions in my block. Since it is not possible to count them one by one, I have coded a very basic Python script to count each different type of addresses. The code is below. I have made us of the **API** from our slides.

```
import requests
import json

def get_data(url):
    response = requests.get(url)

    if response.status_code == 200:
        return response.json()
    else:
        return None

def count_addresses(transactions):
    unique_addresses = set()
```

```
    for transaction in transactions:

        outputs = transaction.get('vout', [])

        for output in outputs:

            address = output.get('scriptpubkey_address')

            if address:

                unique_addresses.add(address)

        inputs = transaction.get('vin', [])

        for input in inputs:

            prevout = input.get('prevout')

            if prevout:

                address = prevout.get('scriptpubkey_address')

                if address:

                    unique_addresses.add(address)

    return unique_addresses

def get_stats(unique_addresses):
    p2pkh = 0
    p2sh = 0
    bech32 = 0

    for address in unique_addresses:

        if address.startswith("1"):
            p2pkh += 1
        elif address.startswith("3"):
            p2sh += 1
        elif address.startswith("bc1"):
            bech32 += 1

    print(f'Total Unique Addresses: {len(unique_addresses)}')
    print(f'p2pkh percent: {p2pkh / len(unique_addresses) * 100}')
    print(f'p2sh percent: {p2sh / len(unique_addresses) * 100}')
    print(f'bech32 percent: {bech32 / len(unique_addresses) * 100}')

def main():
    BLOACK_HASH = "0000000000000023↩
       e1a9140165def5a8a922b30a0f04046d9580b150cd9a155b"
    url = f"https://blockstream.info/api/block/{BLOACK_HASH}/txs/"

    page = 0

    data = []

    while True:
```

```
        current_page = url + f'{page}'

        resp = get_data(current_page)

        if resp is None:
            break

        data.extend(get_data(current_page))

        page += 25

    unique_addresses = count_addresses(data)

    get_stats(unique_addresses)

    print(len(data))
    print(json.dumps(data, indent = 4))

if __name__ == '__main__':
    main()
```

The output of the code can be found below.

```
Total Unique Addresses: 871
p2pkh percent: 100.0
p2sh percent: 0.0
bech32 percent: 0.0
# of transactions: 277
```

We can see that all of the addresses are **p2pkh** addresses. There are 277 transactions are 871 unique addresses.

- In 2013, Bitcoin was still in an early development phase, most of the wallets were only supporting p2pkh type of addresses.
- p2sh was introduced in 2012. Hence, it was relatively new to adapt.
- bech32 address type was introduced in 2017. It was not available at the time my block was mined.

4

By using the same script above, I have printed each unique addresses the observe them. I have been able to find vanity addresses. List of the vanity addresses can be found below.

First, I think there are addresses containing **"1dice"**

1. 1dice6YgEVBf88erBFra9BHf6ZMoyvG88
2. 1diceDCd27Cc22HV3qPNZKwGnZ8QwhLTc

3. 1dice5wwEZT2u6ESAdUGG6MHgCpbQqZiy
4. 1dice97ECuByXAvqXpaYzSaQuPVvrtmz6
5. 1dice6DPtUMBpWgv8i4pG8HMjXv9qDJWN
6. 1dice6gJgPDYz8PLQyJb8cgPBnmWqCSuF
7. 1dice7EYzJag7SxkdKXLr8Jn14WUb3Cf1
8. 1dice6GV5Rz2iaifPvX7RMjfhaNPC8SXH
9. 1dice6wBxymYi3t94heUAG6MpG5eceLG1
10. 1dice9wcMu5hLF4g81u8nioL5mmSHTApw
11. 1dicec9k7KpmQaA8Uc8aCCxfWnwEWzpXE
12. 1dice7fUkz5h4z2wPc1wLMPWgB5mDwKDx
13. 1dice1e6pdhLzzWQq7yMidf6j8eAg7pkY
14. 1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp

There are also some addittional vanity addresses but they may be result of a coincidence as well.

- **18FC2t2pR3SzCemcbEyjKgLorGszXFSPwU** contains Cem Bey.
- **1BYt6AMt4yRC1fKcTmMppRbYvuj2no6MzT** contains by 6 a.m.
- **16HaYRiY47HFShvfnM4xr7adbtXMbJfow1** contains Hayri.
- **1MNxrgnzThD68VtCRYoT3APmRmoJ78V3B8** contains cry.
- **13BAdG3LNFntyWj4akKjBNyGLCnL2eNMg2** contains bad.
- **1HnzoXbETvfKEXGTUsa4XWn1rtzomsQ74b** contains USA.
- **1AxuBabemncuo7RksCeZ8k7PW5TD9kraUw** contains babe.
- **1CarfVw2sNzMtbkogCAnhcpGMj5ibHS1hM** contains car.
- **1LT3QisaZeVTkGC1YR2gZiyzt3ZZU3GVC5** contains Isa.

5

- Transaction:**77bf573006e64c3eee43b993a4aa95a42ce394ff6ef2e58eb3b77859b2d9d1d2** - "Mined by BTC Guild" is the message. This is the coinbase transaction. I tried to look at the each transaction. There were 1032 of sigscript field.
- Transaction: **bbae84d44e372ba28563d97d6bc385f7e7da4f63d1722ef769d3f445957ec4e5**. The ascii of the message is the below.

  ```
  G0D ,`GzF±3×Álg_×ðRºSäp,K
  mû \Ú¬ã]fvŰ«¨¥ý
  HahâOkµÜê+ñ£SLG$Aõ1u¹¶¨»RWÿË8(ÍC¾¡(Ôñ§lîètûZÕ8Ì #Ôl7)Aà-4*RÛ@D
  ```

  This message contains HahaOk as we can see.

6

This block contains the transaction **856a30ff40471055cb59db41348809e962104d86d955376ee5dccd258f9d6c6**. It has the following sigscript value.

045d6b000004e33d2d1e0449ee6703483045022100dbc501f185b30ed0c6ba69b81cbed36e75139a84a7fa238ec8438eb652d77ac0022026ff4f645c9f141b11a3c6d3371257038eb3392b8af063967d10eaa8b203ccd6412102bb851abca9d940f01091691b5bac42a3c1ecd11f50f5168a84a9dac31c1e3d784dc30102000000cd570ef72d99686f69bcee3a4c1342408efa259715c15ebb49edb47b9d8ccf27c992651ac89a97aecd0811c1761915a8e2c8f5153d1bdd994a789e6bd86ab717280c3bedf4238b17752d0cf3250e98e98a788d26bfdc4fb0eb1ee7dc11926ae002000000fd2401045c6b000020d6876f0fce603be43f15d34348bb1de1a8d688e1152596543da033a060cff798040084d7175302e01003cbc0095779820128947f777601207f75597982012c947f757601687f777678827758947f7576538b7f77765c7982777f011179011179ad011179828c7f756079a8011279bb011479815e7981788c88765b79968b0114795e795279965480880400000000011579bc7e0112790117797eaa765f797f757681008854011a797e56797e170000000000000000396a04534c50000101044d494e54200113797e030102087e54797e0c2202000000000000001976a914011879a97e0288ac7e0b220200000000000017a9145379a97e01877e527952797e787eaa607988587901127993b175516b6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6c2202000000000000feffffff6375950675d95eb155abb84cda7837004e07447d150570a112f1827f91d49688282c0a00410000001742434820495320544845205245414c20424954434f494e4d2401045c6b000020d6876f0fce603be43f15d34348bb1de1a8d688e1152596543da033a060cff798040084d7175302e01003cbc0095779820128947f777601207f75597982012c947f757601687f777678827758947f7576538b7f77765c7982777f011179011179ad011179828c7f756079a8011279bb011479815e7981788c88765b79968b0114795e795279965480880400000000011579bc7e0112790117797eaa765f797f757681008854011a797e56797e170000000000000000396a04534c50000101044d494e54200113797e030102087e54797e0c2202000000000000001976a914011879a97e0288ac7e0b220200000000000017a9145379a97e01877e527952797e787eaa607988587901127993b175516b6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6c

If we try to convert it into ASCII char, we will see **"BCH IS THE REAL BITCOIN"** somewhere in the middle of the text.