Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Навчально-науковий фізико технічний інститут
Кафедра інформаційної безпеки

Звіт

З практичного завдання №1
із дисципліни «Технологія блокчейн та розподілені системи»
Тема: «Розгортання систем Ethereum та криптовалют»

Виконав:
Студент групи ФБ-41мн
Шерстюк А. В.
Варіант 13

Київ-2025

BitCoin

Створюємо конфігураційний файл
[as@as-manjaro ~]$ mkdir ~/.bitcoin && code ~/.bitcoin/bitcoin.conf

```
regtest=1
server=1
daemon=1
txindex=1
rpcuser=admin
rpcpassword=admin123
rpcallowip=127.0.0.1
fallbackfee=0.0002
datadir=/home/as/kpi/blockchain/data

[regtest]
rpcport=18443
port=18444
```

Встановлюємо і запускаємо
[as@as-manjaro ~]$ sudo pacman -S bitcoin-daemon
[as@as-manjaro ~]$ bitcoind -conf=/home/as/.bitcoin/bitcoin.conf

```
[as@as-manjaro ~]$ bitcoind -conf=/home/as/.bitcoin/bitcoin.conf
Bitcoin Core starting
```

Перевіримо
[as@as-manjaro ~]$ sudo netstat -tulnp | grep bitcoind

```
[as@as-manjaro ~]$  sudo netstat -tulnp | grep bitcoind
tcp        0      0 0.0.0.0:18444           0.0.0.0:*               LISTEN      6199/bitcoind
tcp        0      0 127.0.0.1:18443         0.0.0.0:*               LISTEN      6199/bitcoind
tcp        0      0 127.0.0.1:18445         0.0.0.0:*               LISTEN      6199/bitcoind
tcp6       0      0 ::1:18443               :::*                    LISTEN      6199/bitcoind
tcp6       0      0 :::18444                :::*                    LISTEN      6199/bitcoind
```

[as@as-manjaro ~]$ bitcoin-cli getblockchaininfo

```
[as@as-manjaro ~]$ bitcoin-cli getblockchaininfo
{
  "chain": "regtest",
  "blocks": 0,
  "headers": 0,
  "bestblockhash": "0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206",
  "difficulty": 4.656542373906925e-10,
  "time": 1296688602,
  "mediantime": 1296688602,
  "verificationprogress": 1,
  "initialblockdownload": true,
  "chainwork": "0000000000000000000000000000000000000000000000000000000000000002",
  "size_on_disk": 293,
  "pruned": false,
  "warnings": [
  ]
}
```

Спробуємо згенерувати коїни на неіснуючий гаманець або адресу (має бути помилка)
[as@as-manjaro ~]$ bitcoin-cli generatetoaddress 1 "abc123"

```
[as@as-manjaro ~]$  bitcoin-cli generatetoaddress 1 "abc123"
error code: -5
error message:
Error: Invalid address
```

Створюємо тестовий гаманець
[as@as-manjaro ~]$ bitcoin-cli createwallet "testwallet"

```
[as@as-manjaro ~]$ bitcoin-cli createwallet "testwallet"
{
  "name": "testwallet"
}
```

[as@as-manjaro ~]$ bitcoin-cli getwalletinfo

```
[as@as-manjaro ~]$ bitcoin-cli getwalletinfo
{
  "walletname": "testwallet",
  "walletversion": 169900,
  "format": "sqlite",
  "balance": 0.00000000,
  "unconfirmed_balance": 0.00000000,
  "immature_balance": 0.00000000,
  "txcount": 0,
  "keypoolsize": 4000,
  "keypoolsize_hd_internal": 4000,
  "paytxfee": 0.00000000,
  "private_keys_enabled": true,
  "avoid_reuse": false,
  "scanning": false,
  "descriptors": true,
  "external_signer": false,
  "blank": false,
  "birthtime": 1746469952,
  "lastprocessedblock": {
    "hash": "0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206",
    "height": 0
  }
}
```

Генеруємо адресу і 101 блок, щоб можна було витратити (по замовчуванню має бути 100 підтверджень мінімум)

```
[as@as-manjaro ~]$ ADDR=$(bitcoin-cli getnewaddress)
[as@as-manjaro ~]$ echo "Generated address: $ADDR"
[as@as-manjaro ~]$ bitcoin-cli generatetoaddress 101 "$ADDR"
```

```
[as@as-manjaro ~]$ ADDR=$(bitcoin-cli getnewaddress)
[as@as-manjaro ~]$ echo "Generated address: $ADDR"
Generated address: bcrt1qhjrwuytgn73pyksgfhgutx8tnp4nhqlmnpl6k3
[as@as-manjaro ~]$ bitcoin-cli generatetoaddress 101 "$ADDR"
[
  "52c90b5c6f088c0f30124c97fe3dcdd65536bb53083c2782e239086c70502c74",
  "473c15d64102232163b9a3024f9981d8c9a38e5e5d36cc466b9177279ace53b7",
  "6bcd99e7da68c290f91f662da2c724b6edb52cb083e6b5004a619f9e0a203a63",
  "12abdbaa52783d776f50aa193115638bab53bbec69e0d4d108c041e58eceec7d",
  "25f1c893a0b434f6bf09f819d27d20b8b5e89a4874e7ea30e15db7695fb800eb",
  "3f13bccbae5ef0220247d98f013378df1107349f6afa76651fe4733aa7765c56",
  "61c2a846fbbca846150a9d1f5f84796981b67cd91c0d43a849528aad0f361cfd",
  "3717ff2b3ab72cfcfdf93767ef5777162d722ab65af79d1c06b12d46bc5236a1",
  "34e634394403aeeb365bb66d6fd17eaa49b5c6ff6b6f402bcc7f7d7aabe00de6",
  "15024db8930e90aec4f76c77d3a05cdeb4a037a885967040bd7a603d89794a0c",
  "39edf65ff0b4f0ee8eff339bd4a51eb32ce46e0a4011f97354d5780eb5f624c8",
  "62986d8c7a04162e114c4b333718ef30395b021d5845679de2789553b3d1a0ad",
  "5d1a08446ba3e562c43328141bb656e279b6bc51aa4cf99cabbdd0591105649c",
  "2067eae65bcec0f5abba40144c7b4e7bf5cbef4723ff89d2438a920978f54f34",
  "055470dec02a09fec91c979517e4225fee6562a174bedfa308576eb85762047f",
  "07bdd58dfc650c7883c4ee93e4ae2feff6c2f063a171bc1ea89bb1b535ede674",
  "67bcc01466e5be28a66f0eb8ba4adbd9a56a0f9cc6cc60483ba7ceda2774a523",
  "4ab86530753e96dc8356ff845119c4ec882cdb319ab378d7da0dd86e1ecf7e91",
```

Баланс збільшився

```
[as@as-manjaro ~]$ bitcoin-cli getbalance
```

```
[as@as-manjaro ~]$ bitcoin-cli getbalance
50.00000000
```

Спробуємо переслати на неіснуючу адресу (має бути помилка)

```
[as@as-manjaro ~]$ bitcoin-cli sendtoaddress "abc123" 1.0
```

```
[as@as-manjaro ~]$ bitcoin-cli sendtoaddress "abc123" 1.0
error code: -5
error message:
Invalid Bitcoin address: abc123
```

Створюємо другу адресу і відправляємо 1 коїн

```
[as@as-manjaro ~]$ ADDR2=$(bitcoin-cli getnewaddress)
[as@as-manjaro ~]$ TXID=$(bitcoin-cli sendtoaddress "$ADDR2" 1.0)
[as@as-manjaro ~]$ echo "Transaction ID: $TXID"
```

```
[as@as-manjaro ~]$ ADDR2=$(bitcoin-cli getnewaddress)
[as@as-manjaro ~]$ TXID=$(bitcoin-cli sendtoaddress "$ADDR2" 1.0)
[as@as-manjaro ~]$ echo "Transaction ID: $TXID"
Transaction ID: c7c8397bb409d4403c48a6dc880745f7e7b99d38860845d4226d9ac639856b8f
```

Підтверджуемо

[as@as-manjaro ~]$ bitcoin-cli generatetoaddress 1 "$ADDR"

```
[as@as-manjaro ~]$ bitcoin-cli generatetoaddress 1 "$ADDR"
[
  "7c82f07fc1aaf5ef3decd329783aec4bfaad5abbe6f14b626f15095b531e26be"
]
```

Перевіряємо

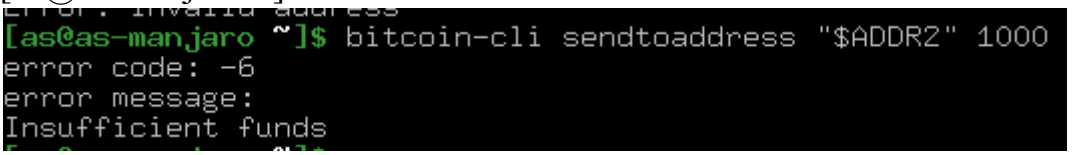
[as@as-manjaro ~]$ bitcoin-cli gettransaction "$TXID"


```
[as@as-manjaro ~]$ bitcoin-cli gettransaction "$TXID"
{
  "amount": 0.00000000,
  "fee": -0.00002820,
  "confirmations": 1,
  "blockhash": "7c82f07fc1aaf5ef3decd329783aec4bfaad5abbe6f14b626f15095b531e26be",
  "blockheight": 102,
  "blockindex": 1,
  "blocktime": 1746470672,
  "txid": "c7c8397bb409d4403c48a6dc880745f7e7b99d38860845d4226d9ac639856b8f",
  "wtxid": "bc3bdb1ece18e3bf72e93c9e25a4a30cc43d4f47ba73e63fb29d5889d76a1454",
  "walletconflicts": [
  ],
  "mempoolconflicts": [
  ],
  "time": 1746470656,
  "timereceived": 1746470656,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "bcrt1qsf3qt763j3tjpwe28ezzlt694mdte6gn69yu00",
      "category": "send",
      "amount": -1.00000000,
      "label": "",
      "vout": 1,
      "fee": -0.00002820,
      "abandoned": false
    },
    {
      "address": "bcrt1qsf3qt763j3tjpwe28ezzlt694mdte6gn69yu00",
      "parent_descs": [
        "wpkh(tpubD6NzVbkrYhZ4XXkkzjwDYG3oENHCQcYrKjKCitYXEW1vmq3yaLoozaXkkCCkhgKH1dtWhodUJB8mfwsfuWa6hkK9vb8zd7kKMxTBnM3NPpK/84h/1h/0h/0/*)#nxdc8ax4"
      ],
      "category": "receive",
      "amount": 1.00000000,
      "label": "",
      "vout": 1,
      "abandoned": false
    }
  ],
  "hex": "020000000001019979d9a12cbe211c7b688b94d1cc2049ab5d863be62f4e8ff9d74026842e9b75d0000000000fdffffff02fc0510240100000016001432186 8e868904a5a411193c29c6c56f42348faa200e1f505000000001600148262 05fb51945720bb2a3e442faf45aedabce9130247304022047eb6647f45f70b8fceba6c51a3a75565cac9cc663d1910b7f317da7d5abf3a502205cd802acabd583a3b0f04de83dfda9307e3eb72fbfabe3e2cc48883c25c09818012102db29fce6eb6a230a4e85bd93883507dfb8b5012dc955d571978b0468cf4cf7c865000000",
  "lastprocessedblock": {
    "hash": "7c82f07fc1aaf5ef3decd329783aec4bfaad5abbe6f14b626f15095b531e26be",
    "height": 102
  }
}
```

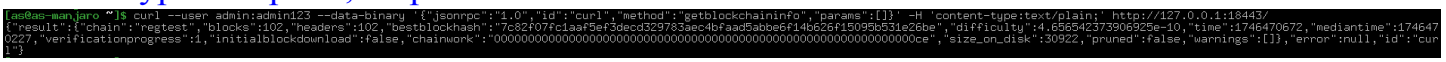

[as@as-manjaro ~]$ bitcoin-cli listunspent


```
[as@as-manjaro ~]$ bitcoin-cli listunspent
[
  {
    "txid": "c7c8397bb409d4403c48a6dc880745f7e7b99d38860845d4226d9ac639856b8f",
    "vout": 0,
    "address": "bcrt1qxgvx36rgjp995sg3j0pfcmzk7s35374z3h2upg",
    "scriptPubKey": "0014321868e868904a5a411193c29c6c56f42348faa2",
    "amount": 48.99997180,
    "confirmations": 1,
    "spendable": true,
    "solvable": true,
    "desc": "wpkh([1b0e4878/84h/1h/0h/1/0]03f2e9bc64d43a9aa71dd92004f4e1e204083a900d0cf27f5de9b0291718032bdd)#3qq97zp9",
    "parent_descs": [
      "wpkh(tpubD6NzVbkrYhZ4XXkkzjwDYG3oENHCQcYrKjKCitYXEW1vmq3yaLoozaXkkCCkhgKH1dtWhodUJB8mfwsfuWa6hkK9vb8zd7kKMxTBnM3NPpK/84h/1h/0h/1/*)#zjge6gkd"
    ],
    "safe": true
  },
  {
    "txid": "c7c8397bb409d4403c48a6dc880745f7e7b99d38860845d4226d9ac639856b8f",
    "vout": 1,
    "address": "bcrt1qsf3qt763j3tjpwe28ezzlt694mdte6gn69yu00",
    "label": "",
    "scriptPubKey": "0014826205fb51945720bb2a3e442faf45aedabce913",
    "amount": 1.00000000,
    "confirmations": 1,
    "spendable": true,
    "solvable": true,
    "desc": "wpkh([1b0e4878/84h/1h/0h/0/2]026ed24693dfb1386dcf59ea6d961ec9e1958b4a2cecd161d275e3b6320b57f37e)#hk9cjrwr",
    "parent_descs": [
      "wpkh(tpubD6NzVbkrYhZ4XXkkzjwDYG3oENHCQcYrKjKCitYXEW1vmq3yaLoozaXkkCCkhgKH1dtWhodUJB8mfwsfuWa6hkK9vb8zd7kKMxTBnM3NPpK/84h/1h/0h/0/*)#nxdc8ax4"
    ],
    "safe": true
  },
  {
    "txid": "abe6259d68ebc4fc3598754dd3b31fe95fd9b045437f9356275374450a6126ec",
    "vout": 0,
    "address": "bcrt1qhjrwuytgn73pyksgfhgutx8tnp4nhqlmnpl6k3",
    "label": "",
    "scriptPubKey": "0014bc86ee11689fa2125a084dd1c598eb986b3b83fb",
    "amount": 50.00000000,
    "confirmations": 101,
    "spendable": true,
    "solvable": true,
    "desc": "wpkh([1b0e4878/84h/1h/0h/0/1]02db29fce6eb6a230a4e85bd93883507dfb8b5012dc955d571978b0468cf4cf7c8)#n93h5wq7",
    "parent_descs": [
      "wpkh(tpubD6NzVbkrYhZ4XXkkzjwDYG3oENHCQcYrKjKCitYXEW1vmq3yaLoozaXkkCCkhgKH1dtWhodUJB8mfwsfuWa6hkK9vb8zd7kKMxTBnM3NPpK/84h/1h/0h/0/*)#nxdc8ax4"
    ],
    "safe": true
  }
]
```

Спробуємо відправити більше ніж на рахунку
[as@as-manjaro ~]$ bitcoin-cli sendtoaddress "$ADDR2" 1000



Зробимо RPC виклик
[as@as-manjaro ~]$ curl --user admin:admin123 --data-binary '{"jsonrpc":"1.0","id":"curl","method":"getblockchaininfo","params":[]}' -H 'content-type:text/plain;' http://127.0.0.1:18443/



{"result":{"chain":"regtest","blocks":102,"headers":102,"bestblockhash":"7c82f07fc1aaf5ef3decd329783aec4bfaad5abbe6f14b626f15095b531e26be","difficulty":4.656542373906925e-10,"time":1746470672,"mediantime":1746470227,"verificationprogress":1,"initialblockdownload":false,"chainwork":"0000000000000000000000000000000000000000000000000000000000000ce","size_on_disk":30922,"pruned":false,"warnings":[]},"error":null,"id":"curl"}

Виводи: У ході лабораторної роботи було розгорнуто приватну блокчейн-мережу Bitcoin у режимі regtest, створено гаманець, згенеровано блоки з coinbase-винагородою та виконано тестові транзакції з подальшим підтвердженням шляхом майнінгу. Продемонстровано принцип блокування coinbase-транзакцій на 100 блоків, а також опрацьовано типові помилки (недостатній баланс, некоректна адреса) й методи їх усунення. Робота підтвердила базові механізми функціонування мережі Bitcoin та принципи взаємодії з вузлом через RPC.