

Blockchain para moedas virtuais

Trabalho final - Grupo 2

ALTAMIRO DOURADO RODRIGUES

SEIDI BRAGA DO CARMO

TARCÍSIO DA CRUZ SANTOS

● Tarefa 1

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tcp 0 0 127.0.0.1:18443 0.0.0.0:* OÚÇA 1692/bitcoind
tcp 0 0 0.0.0.0:18444 0.0.0.0:* OÚÇA 1692/bitcoind
tcp 0 0 127.0.0.53:53 0.0.0.0:* OÚÇA -
tcp 0 0 127.0.0.1:631 0.0.0.0:* OÚÇA -
tcp 0 1 10.0.2.15:60374 191.176.156.31:18444 SYN_ENVIADO 1692/bitcoind
tcp 0 0 10.0.2.15:33310 172.217.162.98:443 TIME_WAIT -
tcp 0 0 10.0.2.15:58246 172.217.28.3:80 TIME_WAIT -
tcp 0 0 10.0.2.15:49330 216.58.198.163:443 TIME_WAIT -
tcp 0 0 10.0.2.15:52700 192.16.58.8:80 TIME_WAIT -
tcp 0 0 10.0.2.15:37806 216.58.202.134:443 TIME_WAIT -
tcp 0 0 10.0.2.15:42936 172.217.162.100:443 TIME_WAIT -
tcp 0 0 10.0.2.15:33936 52.41.177.216:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:42946 172.217.162.100:443 TIME_WAIT -
tcp 0 0 10.0.2.15:49538 172.217.28.238:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:55458 191.34.33.138:80 TIME_WAIT -
tcp 0 0 10.0.2.15:33420 216.58.199.227:443 TIME_WAIT -
tcp 0 0 10.0.2.15:45620 216.58.202.131:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:44070 172.217.28.227:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:38930 172.217.28.3:443 TIME_WAIT -
tcp 0 0 10.0.2.15:49540 172.217.28.238:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:53560 172.217.30.65:443 TIME_WAIT -
tcp 0 0 10.0.2.15:43854 216.58.202.138:443 TIME_WAIT -
tcp 0 0 10.0.2.15:41760 172.217.29.14:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:34550 172.217.28.237:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:60902 172.217.28.232:443 TIME_WAIT -
tcp 0 0 10.0.2.15:42954 172.217.30.78:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:59198 216.58.202.10:443 TIME_WAIT -
tcp 0 0 10.0.2.15:60230 172.217.192.189:443 TIME_WAIT -
tcp 0 0 10.0.2.15:47144 23.96.103.164:19500 ESTABELECIDO 1692/bitcoind
tcp 0 0 10.0.2.15:38154 172.217.28.14:443 ESTABELECIDO 1318/firefox
tcp 0 0 10.0.2.15:42980 172.217.30.78:443 TIME_WAIT -
tcp6 0 0 :::18443 :::* OÚÇA 1692/bitcoind
tcp6 0 0 :::18444 :::* OÚÇA 1692/bitcoind
tcp6 0 0 :::1:631 :::* OÚÇA -
tarcisio@IESBCOIN:~$
```

Figura 1 - Conexão com o servidor remoto

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getaddednodeinfo
[
  {
    "addednode": "23.96.103.164:19500",
    "connected": true,
    "addresses": [
      {
        "address": "23.96.103.164:19500",
        "connected": "outbound"
      }
    ]
  }
]
tarcisio@IESBCOIN:~$
```

Figura 2 - Confirmação da conexão com o nó principal

Arquivo Editar Ver Pesquisar Terminal Ajuda

Figura 3 - Confirmação de conexão com o nó principal II

Arquivo Editar Ver Pesquisar Terminal Ajuda

Figura 4 - Informações da carteira

● Tarefa 2

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcislo@IESBCOIN:~$ bitcoin-cli -regtest sendtoaddress 2NE6jgxTDgln8FsnKuoBWAct5c9EiurxbYF 20
c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04
tarcislo@IESBCOIN:~$
```

Figura 5 - TXID da transferência de 20 IESBCOIN's

TXID:

c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcislo@IESBCOIN:~$ bitcoin-cli -regtest getrawmempool
[
  "c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04"
]
tarcislo@IESBCOIN:~$ bitcoin-cli -regtest gettransaction c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04
{
  "amount": -20.00000000,
  "fee": -0.00003740,
  "confirmations": 0,
  "trusted": true,
  "txid": "c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04",
  "walletconflicts": [
  ],
  "time": 1552663509,
  "timereceived": 1552663509,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "2NE6jgxTDgln8FsnKuoBWAct5c9EiurxbYF",
      "category": "send",
      "amount": -20.00000000,
      "vout": 0,
      "fee": -0.00003740,
      "abandoned": false
    }
  ],
  "hex": "0200000001ece176729675c8324f4c7307b9e8caeb15072ebd3f578aafd75a947dc2e14410000000004847304402204a2822ea5f7494b045ff2f078fb2d7d52ee63562822dc96286c55987806558e02207ce4300222c53c51dec9bb8178d257eeb569df3157810ece4ef0a662be9123f301feffffff02009435770000000017a914e805001163c344416fd8f99da887de4ddfda74a87f6000000"
}
tarcislo@IESBCOIN:~$
```

Figura 6 - Transação aguardando confirmação

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getrawmempool
{
}
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest gettransaction c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04
{
  "amount": -20.00000000,
  "fee": -0.00003740,
  "confirmations": 1,
  "blockhash": "32fbfec196bb3c828afe0d2526785137c785c8504021648ebbf66ebe6ce45b80",
  "blockindex": 1,
  "blocktime": 1552664356,
  "txid": "c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04",
  "walletconflicts": [
  ],
  "time": 1552663509,
  "timereceived": 1552663509,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "2NE6jgxTDgiN8fsnKuoBWAct5c9EiurxbVF",
      "category": "send",
      "amount": -20.00000000,
      "vout": 0,
      "fee": -0.00003740,
      "abandoned": false
    }
  ],
  "hex": "020000001e1ce176729675c8324f4c7307b9e8caeb15072ebd3f578aafd75a947dc2e14410000000004847304402204a2822ea5f7494b045ff2f078fb2d7d52ee63562822dc96286c55987806558e02207ce4300222c53c51dec9bb8178d257eeb569df3157810ece4ef0a662be9123f301feffffff02009435770000000017a914e4bfb0f02643a074d8df455704b315da84a77a6687644fd0b20000000017a914e805001163c344416fd8f99da887de4ddfadc74a87f6000000"
}
tarcisio@IESBCOIN:~$
```

Figura 7 - Transação confirmada e hash do bloco

BLOCK:

247

BLOCKHASH:

32fbfec196bb3c828afe0d2526785137c785c8504021648ebbf66ebe6ce45b80

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
{
  "address": "2NE6jgxTDgiN8fsnKuoBWAct5c9EiurxbVF",
  "category": "send",
  "amount": -20.00000000,
  "vout": 0,
  "fee": -0.00003740,
  "confirmations": 64,
  "blockhash": "32fbfec196bb3c828afe0d2526785137c785c8504021648ebbf66ebe6ce45b80",
  "blockindex": 1,
  "blocktime": 1552664356,
  "txid": "c2495cb0e3f3f88a27af5b5b8ef962723ef4ca60a641404b41f407795cf93f04",
  "walletconflicts": [
  ],
  "time": 1552663509,
  "timereceived": 1552663509,
  "bip125-replaceable": "no",
  "abandoned": false
},
{
  "address": "n3rdYjzZ2bZ2CEVuAchU8T1yPzNs5afFN1",
  "category": "Immature",
  "amount": 25.00003740,
  "vout": 0,
  "confirmations": 64,
  "generated": true,
  "blockhash": "32fbfec196bb3c828afe0d2526785137c785c8504021648ebbf66ebe6ce45b80",
  "blockindex": 0,
  "blocktime": 1552664356,
  "txid": "9ce49a38eb897f8da62fc24c0ab1460d4ba32619e4a5f1041bc6825a7cbb06ba",
  "walletconflicts": [
  ],
  "time": 1552664356,
  "timereceived": 1552664356,
  "bip125-replaceable": "no"
},
}
```

Figura 8 - Detalhes da transação confirmada

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getwalletinfo
{
  "walletname": "",
  "walletversion": 169900,
  "balance": 479.99996260,
  "unconfirmed_balance": 0.00000000,
  "immature_balance": 25.00003740,
  "txcount": 12,
  "keypoololdest": 1544532803,
  "keypoolsize": 999,
  "keypoolsize_hd_internal": 1000,
  "paytxfee": 0.00000000,
  "hdseedid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "hdmasterkeyid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "private_keys_enabled": true
}
tarcisio@IESBCOIN:~$
```

Figura 9 - Informações da carteira após a confirmação da transação

- Tarefa 3

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ recipient_1=2MvpD41xzKKk7J7HzYFzvPxTj43L tznvJK2
tarcisio@IESBCOIN:~$ recipient_2=2N491Hm462nZyaPkPbFmWxtW8NyKnaHir3x
tarcisio@IESBCOIN:~$ change=2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM
tarcisio@IESBCOIN:~$ utxo_txid_1=$(bitcoin-cli -regtest listunspent | jq -r '[1] | .txid')
tarcisio@IESBCOIN:~$ utxo_txid_2=$(bitcoin-cli -regtest listunspent | jq -r '[2] | .txid')
tarcisio@IESBCOIN:~$ utxo_vout_1=$(bitcoin-cli -regtest listunspent | jq -r '[1] | .vout')
tarcisio@IESBCOIN:~$ utxo_vout_2=$(bitcoin-cli -regtest listunspent | jq -r '[2] | .vout')
tarcisio@IESBCOIN:~$ █

```

Figura 10 - Carregamento dos endereços das transferências nas variáveis

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ rawtxhex=$( bitcoin-cli -regtest createrawtransaction "[ { \"txid\": \"$utxo_txid_1\", \"vout\": $utxo_vout_1 }, { \"txid\": \"$utxo_txid_2\", \"vout\": $utxo_vout_2 } ]" "{ \"$recipient_1\": 25.0, \"$recipient_2\": 62.4, \"$change\": 12.5 }")
tarcisio@IESBCOIN:~$ █

```

Figura 11 - Construção da transação: Transferência de 25 IESCOIN's + Transferência de 62,4 IESBCOIN's + Troco de 12,5 IESBCOIN's - Fee de 0,1 IESBCOIN's

```

Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
tarcsio@TESBCOIN:~$ bitcoin-cli -regtest decoderawtransaction $rawtxhex
{
  "txid": "474dccc791ae254b6a7b7f4af76087e7cd9315de2b724e46a07b2d3ab9ba2ae8",
  "hash": "474dccc791ae254b6a7b7f4af76087e7cd9315de2b724e46a07b2d3ab9ba2ae8",
  "version": 2,
  "size": 188,
  "vsize": 188,
  "weight": 752,
  "locktime": 0,
  "vin": [
    {
      "txid": "11de66bbd9411314f50114f7c1d2b4c4e35f2e8399c46fe802e773c91d4e4c1a",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "sequence": 4294967295
    },
    {
      "txid": "c06bc4a1411ab1d717677be25cd36ef4eac2976073441c6117319e2d5441e74e",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 25.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 272552b47c02cd70cdfaaadda3b90fc66bc72929 OP_EQUAL",
        "hex": "a914272552b47c02cd70cdfaaadda3b90fc66bc7292900",

```

```

Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
      "reqSigs": 1,
      "type": "scripthash",
      "addresses": [
        "2MvpD41xzKXk7J7WzYFzVPxTj43LtnvJK2"
      ]
    },
    {
      "value": 62.40000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 777c499b3195cb75745e3a15e66955a4e94d4c OP_EQUAL",
        "hex": "a914777c499b3195cb75745e3a15e66955a4e94d4c87",
        "reqSigs": 1,
        "type": "scripthash",
        "addresses": [
          "2N491Hn462nZyaPkPbFMwXtW8NyKnaHlr3x"
        ]
      }
    },
    {
      "value": 12.50000000,
      "n": 2,
      "scriptPubKey": {
        "asm": "OP_HASH160 49b94a7c94448cd289a9d9453b797d5255b28dcd OP_EQUAL",
        "hex": "a91449b94a7c94448cd289a9d9453b797d5255b28dcd87",
        "reqSigs": 1,
        "type": "scripthash",
        "addresses": [
          "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM"
        ]
      }
    }
  ]
}

```

Figura 12 - Transação decodificada

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ signedtx=$(bitcoin-cli -regtest signrawtransactionwithwallet $rawtxhex | jq -r '.hex')
tarcisio@IESBCOIN:~$
```

Figura 13 - Assinatura da transação

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest decoderawtransaction $signedtx
{
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "hash": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "version": 2,
  "size": 332,
  "vsize": 332,
  "weight": 1328,
  "locktime": 0,
  "vin": [
    {
      "txid": "11de66bbd9411314f50114f7c1d2b4c4e35f2e8399c46fe802e773c91d4e4c1a",
      "vout": 0,
      "scriptSig": {
        "asm": "304402207d6454597fb135e745ad5cc762a8ecf2324aaaff3e2436334fc9e9fe381d50a402204502cf02d7546de764f4e1d376ae8eb6571dd914b5c18c5b4893e05b03711d57[ALL]",
        "hex": "47304402207d6454597fb135e745ad5cc762a8ecf2324aaaff3e2436334fc9e9fe381d50a402204502cf02d7546de764f4e1d376ae8eb6571dd914b5c18c5b4893e05b03711d5701"
      },
      "sequence": 4294967295
    },
    {
      "txid": "c06bc4a1411ab1d717677be25cd36ef4eac2976073441c6117319e2d5441e74e",
      "vout": 0,
      "scriptSig": {
        "asm": "3044022067bd04dbbcd9f5e8be27e0f364da94eb136d820d7d1c6057e0be17dcbc23d5ba02203b25088e4f7cba2b57ed99eb9e7af73d53526761bef0b8c05bf29b247e76661a[ALL]",
        "hex": "473044022067bd04dbbcd9f5e8be27e0f364da94eb136d820d7d1c6057e0be17dcbc23d5ba02203b25088e4f7cba2b57ed99eb9e7af73d53526761bef0b8c05bf29b247e76661a01"
      },
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 25.00000000
    }
  ]
}
```



```

Arquivo Editar Ver Pesquisar Terminal Ajuda
{
  "value": 25.00000000,
  "n": 0,
  "scriptPubKey": {
    "asm": "OP_HASH160 272552b47c02cd70cdfaaadda3b90fc66bc72929 OP_EQUAL",
    "hex": "a914272552b47c02cd70cdfaaadda3b90fc66bc7292987",
    "reqSigs": 1,
    "type": "scripthash",
    "addresses": [
      "2MvpD41xzKXk7J7WzVFzvPxTj43LtznvJK2"
    ]
  }
},
{
  "value": 62.40000000,
  "n": 1,
  "scriptPubKey": {
    "asm": "OP_HASH160 777c499b3195cb75745e3a15e66955a4e4e94d4c OP_EQUAL",
    "hex": "a914777c499b3195cb75745e3a15e66955a4e4e94d4c87",
    "reqSigs": 1,
    "type": "scripthash",
    "addresses": [
      "2N491Hm462hZyaPkPbFMwXtW8NyKnaHlr3x"
    ]
  }
},
{
  "value": 12.50000000,
  "n": 2,
  "scriptPubKey": {
    "asm": "OP_HASH160 49b94a7c94448cd289a9d9453b797d5255b28dcd OP_EQUAL",
    "hex": "a91449b94a7c94448cd289a9d9453b797d5255b28dcd87",
    "reqSigs": 1,
    "type": "scripthash",
    "addresses": [
      "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM"
    ]
  }
}

```

Figura 14 - Transação assinada decodificada

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarclis@IESBCOIN:~$ bitcoin-cli -regtest sendrawtransaction $signedtx
f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893
tarclis@IESBCOIN:~$ bitcoin-cli -regtest getrawmempool
[
  "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893"
]
tarclis@IESBCOIN:~$ 

```

Figura 15 - Envio da transação para a rede

TXID:

f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarclislo@IESBCOIN:~$ bitcoin-cli -regtest gettransaction f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893
{
  "amount": -87.40000000,
  "fee": -0.10000000,
  "confirmations": 0,
  "trusted": true,
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "walletconflicts": [
  ],
  "time": 1552871125,
  "timereceived": 1552871125,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "2MvpD41xzKXk7J7WzYFzvPxTj43LtnvJK2",
      "category": "send",
      "amount": -25.00000000,
      "vout": 0,
      "fee": -0.10000000,
      "abandoned": false
    },
    {
      "address": "2N491Hm462nZyaPkPbFMwXtW8NyKnaHlr3x",
      "category": "send",
      "amount": -62.40000000,
      "vout": 1,
      "fee": -0.10000000,
      "abandoned": false
    },
    {
      "address": "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM",
      "category": "send",
      "amount": -12.50000000,
      "label": "",
      "vout": 2,
      "fee": -0.10000000,
      "abandoned": false
    }
  ],
  "hex": "02000000021a4c4e1dc973e702e86fc499832e5fe3c4b4d2c1f71401f5141341d9bb66de11000000004847304402207d6454597fb135e745ad5cc762a8ecf2324aaaff3e2436334fc9e9fe381d50a402204502cf02d7546de764f4e1d376ae8eb6371dd914b5c18c5b4893e05b03711d5701ffffffffff4ee741542d9e3117611c44736097c2eaf46ed35ce27b6717d7b11a41a1c46bc000000000048473044022067bd04dbbcd9f5e8be27e0f364da94eb136d820d7d1c6057e0be17dcbc23d5ba02203b25088e4f7cba2b57ed999eb9e7af73d53526761bef0b8c05bf29b247e76661a01ffffffffff0300f902950000000017a914272552b47c02cd70cd7faaadda3b90fc66bc729298700d8ee730100000017a914777c499b3195cb75745e3a15e66955a4e4e94d4c87807c814a0000000017a91449b94a7c94448cd289a9d9453b797d5255b28cd8700000000"
}
tarclislo@IESBCOIN:~$
```

Figura 16 - Transação aguardando confirmação


```
Arquivo Editar Ver Pesquisar Terminal Ajuda
{
  "address": "2N491Hm462nZyaPkPbFMwXtW8NyKnaHlr3x",
  "category": "send",
  "amount": -62.40000000,
  "vout": 1,
  "fee": -0.10000000,
  "confirmations": 1,
  "blockhash": "0e4b766684c2c1602afc94df92a479fd127ca630dbe24a04a77223539e8fc9a4",
  "blockindex": 1,
  "blocktime": 1552871461,
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "walletconflicts": [
  ],
  "time": 1552871125,
  "timereceived": 1552871125,
  "bip125-replaceable": "no",
  "abandoned": false
},
{
  "address": "2MvpD41xzKXk7J7WzVFzvPxTj43LtzvJK2",
  "category": "send",
  "amount": -25.00000000,
  "vout": 0,
  "fee": -0.10000000,
  "confirmations": 1,
  "blockhash": "0e4b766684c2c1602afc94df92a479fd127ca630dbe24a04a77223539e8fc9a4",
  "blockindex": 1,
  "blocktime": 1552871461,
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "walletconflicts": [
  ],
  "time": 1552871125,
  "timereceived": 1552871125,
  "bip125-replaceable": "no",
  "abandoned": false
},
}
```

Figura 18 - Detalhes das transferências

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
{
  "address": "2Myy3HXFCPXj7RhpAUETaMuWShraR6rHexM",
  "category": "receive",
  "amount": 12.50000000,
  "label": "",
  "vout": 2,
  "confirmations": 1,
  "blockhash": "0e4b766684c2c1602afc94df92a479fd127ca630dbe24a04a77223539e8fc9a4",
  "blockindex": 1,
  "blocktime": 1552871461,
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "walletconflicts": [
  ],
  "time": 1552871125,
  "timereceived": 1552871125,
  "bip125-replaceable": "no"
},
{
  "address": "2Myy3HXFCPXj7RhpAUETaMuWShraR6rHexM",
  "category": "send",
  "amount": -12.50000000,
  "label": "",
  "vout": 2,
  "fee": -0.10000000,
  "confirmations": 1,
  "blockhash": "0e4b766684c2c1602afc94df92a479fd127ca630dbe24a04a77223539e8fc9a4",
  "blockindex": 1,
  "blocktime": 1552871461,
  "txid": "f12952b62155912bbf92ae48384f4a843035d3d84adf6acddd1f4e060fa21893",
  "walletconflicts": [
  ],
  "time": 1552871125,
  "timereceived": 1552871125,
  "bip125-replaceable": "no",
  "abandoned": false
},
}
```

Figura 19 - Detalhes do troco

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getwalletinfo
{
  "walletname": "",
  "walletversion": 169900,
  "balance": 392.49996260,
  "unconfirmed_balance": 0.00000000,
  "immature_balance": 37.60003740,
  "txcount": 14,
  "keypoololdest": 1544532803,
  "keypoolsize": 999,
  "keypoolsize_hd_internal": 1000,
  "paytxfee": 0.00000000,
  "hdseedid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "hdmasterkeyid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "private_keys_enabled": true
}
tarcisio@IESBCOIN:~$
```

Figura 20 - Informações da carteira após a confirmação da transação

● Tarefa 4

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest validateaddress "2MzeT16MKzBsdiZAnZ6w7JRRkb5gdLkuiPU"
{
  "isvalid": true,
  "address": "2MzeT16MKzBsdiZAnZ6w7JRRkb5gdLkuiPU",
  "scriptPubKey": "a914512d4fa4a77b90053d3cd8252dbcfa3f9452c26c87",
  "isscript": true,
  "iswitness": false
}
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest validateaddress "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM"
{
  "isvalid": true,
  "address": "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM",
  "scriptPubKey": "a91449b94a7c94448cd289a9d9453b797d5255b28dcd87",
  "isscript": true,
  "iswitness": false
}
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest validateaddress "2N5fxgBcCwpUxyNGFkVmjf9yJsStwaEyGgJ"
{
  "isvalid": true,
  "address": "2N5fxgBcCwpUxyNGFkVmjf9yJsStwaEyGgJ",
  "scriptPubKey": "a914884f2067364cfa03c5df610f1edf0ce416b73dcb87",
  "isscript": true,
  "iswitness": false
}
tarcisio@IESBCOIN:~$
```

Figura 21 - Endereços envolvidos na transação Multisig

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ utxo_txid=$(bitcoin-cli -regtest listunspent | jq -r '.[7] | .txid')
tarcisio@IESBCOIN:~$ utxo_vout=$(bitcoin-cli -regtest listunspent | jq -r '.[7] | .vout')
tarcisio@IESBCOIN:~$ utxo_spk=$(bitcoin-cli -regtest listunspent | jq -r '.[7] | .scriptPubKey')
tarcisio@IESBCOIN:~$ redeem_script="522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652ae"
tarcisio@IESBCOIN:~$ recipient=$(bitcoin-cli -regtest getrawchangeaddress)
tarcisio@IESBCOIN:~$ recipient2=2NFA1GwatZagK3MnflvplD80cRje1En147z
tarcisio@IESBCOIN:~$ rawtxhex=$(bitcoin-cli -regtest createrawtransaction " [{"txid": "\$utxo_txid", "vout": \$utxo_vout }]" [{"\$recipient": 24.98000000, "\$recipient2": 25.00000000 }])
tarcisio@IESBCOIN:~$

```

Figura 22 - Construção da transação

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest signrawtransaction $rawtxhex "[{"txid": "\$utxo_txid", "vout": \$utxo_vout, "scriptPubKey": "\$utxo_spk"}, {"redeemScript": "\$redeem_script"}]" '[{"cNH6XuhRFkwTk6AY68uf9a8ZWEkn4ALtxwZYCE9iL6hjXJJg3zbT"}]'
{
  "hex": "0200000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c900000009200473044022064cd7354915b372445f0c0f0672a239f8527c4fcd2818fc24ca9261f335df3a6022042f3fdea1994ac2b1265b0648a93df9d7e216bb4a569ff93ef310ccc77ee7a32010047522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652aefffffffff0280626a94000000017a914a32f91c52c7d961e7a70fbd9f56bec5866bfc988700f902950000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000",
  "complete": false,
  "errors": [
    {
      "txid": "c965ec45578bf6ab0a55cddb52bccf340fc83302fd2468934446aa29b5bf3fbc",
      "vout": 0,
      "witness": [
        ],
      "scriptSig": "00473044022064cd7354915b372445f0c0f0672a239f8527c4fcd2818fc24ca9261f335df3a6022042f3fdea1994ac2b1265b0648a93df9d7e216bb4a569ff93ef310ccc77ee7a32010047522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652ae",
      "sequence": 4294967295,
      "error": "Signature must be zero for failed CHECK(MULTI)SIG operation"
    }
  ]
}
tarcisio@IESBCOIN:~$

```

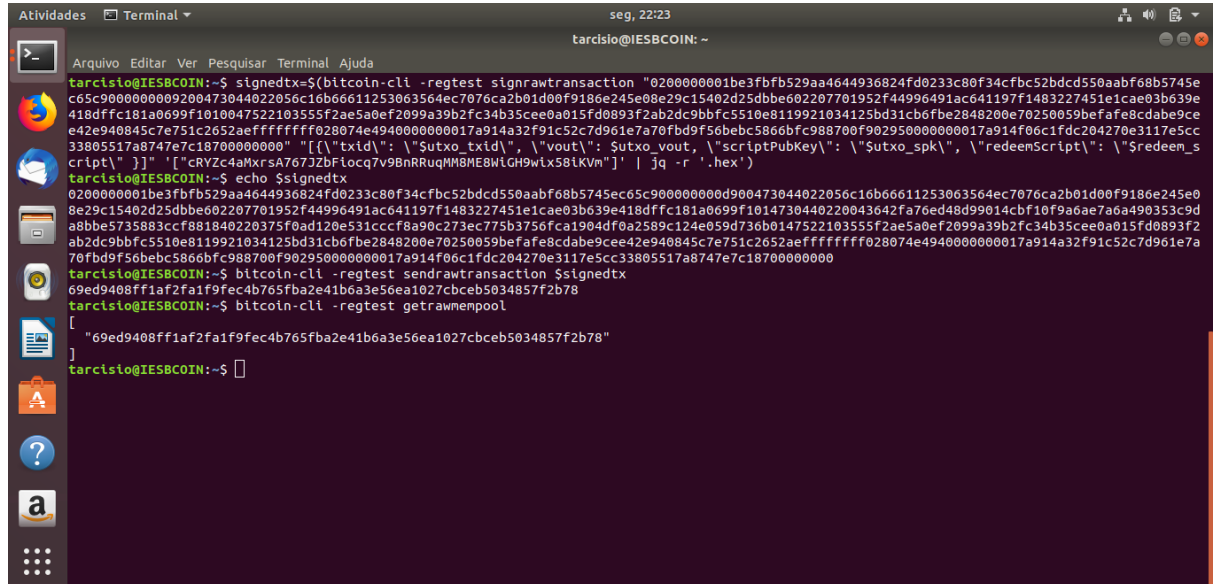
Figura 23 - Primeira assinatura da transação

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest signrawtransaction "0200000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c900000009200473044022056c16b66611253063564ec7076ca2b01d00f9186e245e08e29c15402d25dbbe602207701952f44996491ac641197f1483227451e1cae03b639e418dfffc181a0699f1010047522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652aefffffffff028074e494000000017a914a32f91c52c7d961e7a70fbd9f56bec5866bfc988700f90295000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000" [{"txid": "\$utxo_txid", "vout": \$utxo_vout, "scriptPubKey": "\$utxo_spk", "redeemScript": "\$redeem_script"}]" '[{"cRYZc4aMxrsA767JZbFlocq7v9BnRRuqMM8ME8WlGH9wix58iKVm"}]'
{
  "hex": "0200000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c90000000d900473044022056c16b66611253063564ec7076ca2b01d00f9186e245e08e29c15402d25dbbe602207701952f44996491ac641197f1483227451e1cae03b639e418dfffc181a0699f1014730440220043642fa76ed48d99014cbf10f9a6ae7a6a490353c9da8bbe5735883ccf881840220375f0ad120e531cccf8a90c273ec775b3756fca1904df0a2589c124e059d736b0147522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652aefffffffff028074e494000000017a914a32f91c52c7d961e7a70fbd9f56bec5866bfc988700f90295000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000",
  "complete": true
}
tarcisio@IESBCOIN:~$

```

Figura 24 - Segunda assinatura da transação



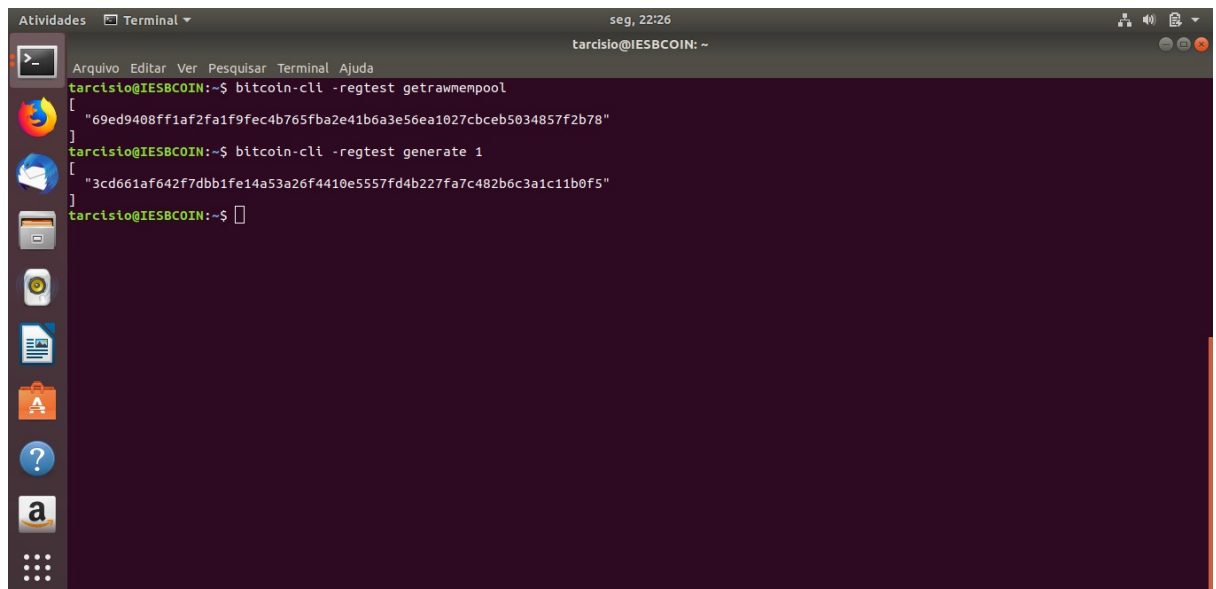
A terminal window titled 'seg, 22:23' with the user 'tarcisio@IESBCOIN: ~'. The terminal shows the following commands and output:

```
tarcisio@IESBCOIN:~$ signedtx=$(bitcoin-cli -regtest signrawtransaction "020000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c900000009200473044022056c16b66611253063564ec7076ca2b01d00f9186e245e08e29c15402d25dbbe602207701952f44996491ac641197f1483227451e1cae03b639e418dfc181a0699f1010047522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9ce42e940845c7e751c2652aefffffffff028074e4940000000017a914a32f91c52c7d961e7a70fbd9f56ebc5866bfc988700f902950000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000" "[{"txid": \"$utxo_txid\", \"vout\": $utxo_vout, \"scriptPubKey\": \"$utxo_spk\", \"redeemScript\": \"$redeem_script\"}]" '["cRYZc4MxrsA767JZbFlocq7V9BnRRuqMM8ME8WlGH9wLx58IKVm"]' | jq -r '.hex')
tarcisio@IESBCOIN:~$ echo $signedtx
020000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c900000000d900473044022056c16b66611253063564ec7076ca2b01d00f9186e245e08e29c15402d25dbbe602207701952f44996491ac641197f1483227451e1cae03b639e418dfc181a0699f101004730440220043642fa76ed48d99014cbf10f9a6ae7a6a490353c9da8bbe5735883ccf881840220375f0ad120e531ccc8a90c273ec775b3756fca1904df0a2589c124e059d736b0147522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652aefffffffff028074e4940000000017a914a32f91c52c7d961e7a70fbd9f56ebc5866bfc988700f902950000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest sendrawtransaction $signedtx
69ed9408ffa1af2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getrawmempool
[
  "69ed9408ffa1af2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78"
]
tarcisio@IESBCOIN:~$
```

Figura 25 - Envio da transação assinada

TXID:

69ed9408ffa1af2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78



A terminal window titled 'seg, 22:26' with the user 'tarcisio@IESBCOIN: ~'. The terminal shows the following commands and output:

```
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest getrawmempool
[
  "69ed9408ffa1af2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78"
]
tarcisio@IESBCOIN:~$ bitcoin-cli -regtest generate 1
[
  "3cd661af642f7dbb1fe14a53a26f4410e5557fd4b227fa7c482b6c3a1c11b0f5"
]
tarcisio@IESBCOIN:~$
```

Figura 26 - Confirmação da transação

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarclislo@IESBCOIN:~$ bitcoin-cli -regtest gettransaction 69ed9408ffa2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78
{
  "amount": 24.98000000,
  "confirmations": 1,
  "blockhash": "3cd661af642f7dbb1fe14a53a26f4410e5557fd4b227fa7c482b6c3a1c11b0f5",
  "blockindex": 1,
  "blocktime": 1553563576,
  "txid": "69ed9408ffa2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78",
  "walletconflicts": [
  ],
  "time": 1553563368,
  "timereceived": 1553563368,
  "bip125-replaceable": "no",
  "details": [
    {
      "involvesWatchonly": true,
      "address": "2N8857jUjssdaxtG3wt4TzPek3ChwfsPbKT",
      "category": "receive",
      "amount": 24.98000000,
      "vout": 0
    }
  ],
  "hex": "0200000001be3fbfb529aa4644936824fd0233c80f34cfbc52bdc550aabf68b5745ec65c900000000d900473044022056c16b66611253063564ec7076ca2b01d00f9186e245e08e29c15402d25dbbe602207701952f44996491ac641197f1483227451e1cae03b639e418dfc181a0699f1014730440220043642fa76ed48d99014cbf10f9a6ae7a6a490353c9da8bbe5735883ccf881840220375f0ad120e531cccf8a90c273ec775b3756fca1904df0a2589c124e059d736b0147522103555f2ae5a0ef2099a39b2fc34b35cee0a015fd0893f2ab2dc9bbfc5510e8119921034125bd31cb6fbe2848200e70250059befafe8cdabe9cee42e940845c7e751c2652aefffffffff028074e494000000017a914a32f91c52c7d961e7a70fbd9f56bec5866bfc988700f902950000000017a914f06c1fdc204270e3117e5cc33805517a8747e7c18700000000"
}
tarclislo@IESBCOIN:~$ █

```

Figura 27 - Transação confirmada

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
tarclislo@IESBCOIN:~$ bitcoin-cli -regtest getblock 3cd661af642f7dbb1fe14a53a26f4410e5557fd4b227fa7c482b6c3a1c11b0f5
{
  "hash": "3cd661af642f7dbb1fe14a53a26f4410e5557fd4b227fa7c482b6c3a1c11b0f5",
  "confirmations": 1,
  "strippedsize": 560,
  "size": 596,
  "weight": 2276,
  "height": 314,
  "version": 805306369,
  "versionHex": "30000001",
  "merkleroot": "905452d912be67a85bda997f3ee599303d155320e5de01dc17fdbcf5ef028311b",
  "tx": [
    {
      "5fe4727e5c3ba070e57058e40c633a09c757100faa3faf932f9855e0807b8b5d",
      "69ed9408ffa2fa1f9fec4b765fba2e41b6a3e56ea1027cbceb5034857f2b78"
    }
  ],
  "time": 1553563576,
  "mediantime": 1552774890,
  "nonce": 1,
  "bits": "207fffff",
  "difficulty": 4.656542373906925e-10,
  "chainwork": "00000000000000000000000000000000000000000000000000000000000000276",
  "nTx": 2,
  "previousblockhash": "455cebc391e7c2b2e8e36acc80558b2162ae7a272d67717a5cdf87edc263e38"
}
tarclislo@IESBCOIN:~$ █

```

Figura 28 - Bloco e hash

BLOCK:

314

BLOCKHASH:

3cd661af642f7dbb1fe14a53a26f4410e5557fd4b227fa7c482b6c3a1c11b0f5


```
Arquivo Editar Ver Pesquisar Terminal Ajuda
[
  [
    "n3rdYjzZ2bZ2CEVuACHU8T1yPzNsSafFN1",
    0.00000000
  ],
  [
    [
      "n4gGffR9lReJ2WbpS8U3j8J9SaCA8HoLLx",
      350.00000000
    ],
    [
      "2NEQ2kDKFBD6B4As9ghnPFFo5bpoA7xfapJ",
      29.99996260
    ]
  ],
  [
    [
      "2Myy3HXfCPXj7RhpAUETaMuWShraR6rHexM",
      12.50000000,
      ""
    ]
  ],
  [
    [
      "2NSfxgBcCwpUxyNGFkVmJf9yJsStwaEyGgJ",
      0.00000000,
      ""
    ]
  ],
  [
    [
      "2N8857jUjssdxtG3wt4TzPek3ChwfsPbKT",
      24.98000000
    ]
  ]
]
tarclislo@IESBCOIN:~$
```

Figura 29 - Posição dos endereços envolvidos após o envio da transação

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
tarclislo@IESBCOIN:~$ bitcoin-cli -regtest getwalletinfo
{
  "walletname": "",
  "walletversion": 169900,
  "balance": 417.47996260,
  "unconfirmed_balance": 0.00000000,
  "immature_balance": 62.61003740,
  "txcount": 18,
  "keypoololdest": 1544532803,
  "keypoolsize": 1000,
  "keypoolsize_hd_internal": 999,
  "paytxfee": 0.00000000,
  "hdseedid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "hdmasterkeyid": "0ed60abca4e252c639e499bf11d6435ea0345ff5",
  "private_keys_enabled": true
}
tarclislo@IESBCOIN:~$
```

Figura 30 - Informações da carteira após o envio da transação