Ime i prezime: _____

Zadatak 1

Pokrenite virtualni stroj Kriptovalute (Linux) i razvojno sučelje *Eclipse*. U primjeru `Main.java` nalazi se program koji koristi biblioteku *BitcoinJSONRPCClient** za pristup API sučelju poslužitelja Bitcoin Core. Unesite autorizacijske podatke (promijenite vrijednost konfiguracijskih varijabli) tako da program pristupa udaljenom poslužitelju Bitcoin *mainnet* na adresi `blockchain.oss.unist.hr` pa pokrenite program i dohvatite sljedeće podatke:

Broj transakcija u mempoolu: ..... Visina blockchaina: .....

* `https://github.com/Polve/bitcoin-rpc-client`

Zadatak 2

Objekt `client` koristimo za slanje upita udaljenom klijentu (tj. udaljenom poslužitelju). Sljedeća linija koda dohvaća cijeli *mempool* aktivnog klijenta u obliku liste stringova:

```
List<String> mempool = client.getRawMemPool();
```

Ispišite cijeli *mempool* u obliku liste stringova, tj. liste TX identifikatora *(txid)*:

```
System.out.println("Transakcije:  " + mempool.toString());
```

Zadatak 3

Dohvatite *id* prve transakcije u *mempoolu*. U Javi se prvi član liste dohvaća sljedećom sintaksom: `myList.get(0)`.

```
String firstTxId = ...
```

Ispišite *id*:

```
System.out.println("First transaction ID: " + firstTxId);
```

Zadatak 4

Dohvatite transakciju iz prethodnog zadatka u sirovom obliku:

```
RawTransaction firstTxRaw = client.   ...
```

Zadatak 5

Dohvatite i ispišite veličinu te transakcije (u bajtovima).

```
long txSize = firstTxRaw.   ...
```

Zadatak 6

Pretvorite transakciju u heksadekadski string pa je ispišite u sirovom obliku:

```
String firstTxHex = firstTxRaw.  ...
```

Zadatak 7

Dohvatite i ispišite sve izlaze iz te transakcije:

```
List<Out> outputs = ...
```

Zadatak 8

Dohvatite i ispišite prvi izlaz iz te transakcije:

```
Out firstOutput = ...
```

Zadatak 9

Dohvatite i ispišite iznos bitcoina koja se prenosi prvim izlazom.

```
BigDecimal value = ...
```

Zadatak 10

Rezultat iz prethodnog zadatka provjerite u *blockexploreru*.

Zadatak 11

Dohvatite i ispišite skriptu koja se nalazi u prvom izlazu te transakcije:

```
ScriptPubKey script = firstOutput.  ...
```

Zadatak 12

Objekt `script` iz prethodnog zadatka sadrži polja `hex` i `asm` koja su u osnovi ista: `hex` sadrži serijaliziranu, a `asm`, *assembly*, deserijaliziranu skriptu. Koji OP kodovi su korišteni u dohvaćenoj skripti? U slučaju da biblioteka BitcoinJSONRPCClient nije ništa dekodirala, upišite samo indeks prvog koda, `asm=x`.

. . . . . .

Zadatak 13

Preuzmite i isprobajte izvorni kôd s Moodla koji ispisuje primjere svih skripti koje se koriste u 100 slučajno odabranih transakcija u *mempoolu*. Koji su sve tipovi skripti vidljivi?

. . . . . .