HÖGSKOLAN VÄST

2018-04-06, TL, v2

Modul 5 inlämningsuppgift: Transaktioner i Python

Den här inlämningsuppgiften går ut på att lära sig mer om adresser och nycklar samt transaktioner i Bitcoin. Denna gången är uppgiften lite lösare specificerad och det är därför fritt fram (inom vissa ramar) att använda olika stödbibliotek eller RPC-anrop för att lösa uppgifterna.

Som minimumkrav ska programmet klara:

- Att generera och skriva ut nya nycklar och adresser i olika format:
  - **Privat nyckel**, både som heltal, hex och i wif-format
  - **Public nyckel** både som "compressed" och som "uncompressed"
  - **Bitcoin adress** (från både compressed och uncompressed public key)
- Att genomföra (minst) två transaktioner (med egengenererade adresser). Den första ska spendera en befintlig output på kedjan och den andra en eller flera outputs från den första transaktionen. T ex:

```
Ange adress att skicka från: 1AdB
Ange adress att skicka till: 1edu
Ange belopp: 1.5
Ange växeladress: 1AdB
Ange fee per kB: 0,0002
```

  RPC-anropen "create/sign/send-rawtransaction" bör användas.

Överkursuppgifter (frivillig):

- Prova transaktioner med olika adresstyper: 1..., 3..., bc1...
- Genomför en multisig-transaktion (och lyckas spendera den), t ex, en 2-av-3 multisig.

Tips

Detaljer, tips:

- Det räcker att klara av **traditionella 1-adresser** för addressgeneratorn.
- **Tidigare outputs** som ska spenderas får lov att anges manuellt (txid, output n) eller hårdkodade i programmet (t ex en lista i programmet), då slipper man leta automatiskt efter spenderbara tidigare outputs.
- Man behöver använda ett paket för ECDSA-algoritmen. Paketet "pycoin" verkar fungerande och bra. Det är svårt att klara sig utan lite hjälpbibliotek: **"from pycoin import ecdsa, key, encoding"** kan vara lämpligt. Överkurs är ju att klara av allt med egen kod förstås... :)

Inlämning

Praktiska saker:

- Det är bra att zippa ihop allt till en fil som man lämnar in (zip, tgz, rar, etc)
- Lämna in färdigt program på disco (M5: Tx Python).
- Lämna in kort rapport (1-3 sidor, valfritt format) där ni visar att programmet fungerar (ifall vi inte lyckas testköra programmet). Demonstrera adressgenerering och transaktionsgenomförandet (txid och blocknummer i blockkedjan Bitcoin Edu).