Install Bitcoin Core

Install the package:

```
sudo apt-add-repository ppa:bitcoin/bitcoin
sudo apt-get update
sudo apt-get install bitcoind
```

Create configuration file:

```
mkdir -p ~/.bitcoin
zcat /usr/share/doc/bitcoind/examples/bitcoin.conf.gz > ~/.bitcoin/bitcoin.conf
```

Edit it to enable regtest and expose JSON-RPC:

```
regtest=1
server=1
```

How to get help

Manpage:

```
man bitcoin-cli
```

List all available commands:

```
bitcoin-cli help
```

Get help on specific command:

```
bitcoin-cli help <command_name>
```

Run the bitcoin daemon

```
bitcoind
```

Start playing!

What information do these commands provide?

```
bitcoin-cli getblockchaininfo
bitcoin-cli getmininginfo
bitcoin-cli getnetworkinfo
bitcoin-cli getnettotals
bitcoin-cli getwalletinfo
```

Create a new address.

What letter does it start with?
Why?
Why doesn't it start with "1"?

List the addresses you have in your wallet.

What is the private key of the address you created?

Verify that your address is valid.

Change a random letter from the address. Try validating it again.

What is the balance of your account?

How many blocks are in the blockchain now?

What is the hash of the latest block?

What block is that? Why does it have a hash?

Generate a block.

What is the hash of the current block?

Show details about the current block.

What is the previous block's hash?
What is the merkleroot value?
Can you find the transactions included in this block?
How many are they?

Show details about the first transaction in the block.

Why is the transaction labeled as "immature"?

What is your account balance now?

Mine 100 more blocks.

What is your account balance now?

Show your UTXOs.

Mine another block.

Show your UTXOs again.

List the addresses you have in your wallet.

Send 1 BTC to the address you created.

Can you find the transaction in the mempool?

List the transaction in the mempool:

How do you confirm the transaction?

Create a backup of your wallet.

How do you import it again?

How do you password protect your wallet?

Python scripting

Suggested libraries:

- https://github.com/karask/python-bitcoin-utils
- https://github.com/petertodd/python-bitcoinlib
- https://github.com/richardkiss/pycoin

Make sure you have python3 and virtualenv installed:

```
sudo apt-get update
sudo apt-get install python3 virtualenv
```

Create a virtualenv:

```
mkdir -p ~/virtualenv/bitcoin
virtualenv -p python3 ~/virtualenv/bitcoin
```

Activate the virtualenv:

```
source ~/virtualenv/bitcoin/bin/activate
```

Install the libraries:

```
pip install bitcoin-utils
pip install python-bitcoinlib
pip install pycoin
```

bitcoin-utils

Setup the network. Some of you use the mainnet and some the testnet.

Create a private key:

Do you all have the same private key?

What is the WIF format (uncompressed) of the private key?

What is the WIF format (compressed) of the private key?

What is the corresponding public key? In uncompressed and compressed forms.

What is the corresponding address?

What does the address start with? Why?

What is the hash160 representation of the address?

What is the scriptPubKey of the address?

Create a segwit (bech32) address using the same private/public keys:

What does the address start with?

What is the hash160 representation of the address?

pycoin and BIP32

Load pycoin with btc:

Find the BIP32 specifications online. Get seed for test vector 1 and try to use it. First create a key:

Verify that the key you created is a private one:

What is the private master key (chain m)?

What does it start with?

What is the public key that corresponds to it?

What does it start with?

What is the corresponding address?

Verify that the keypair is the same as the ones reported in the test vector in BIP32.

Create a hardened m/0 chain, as per the example in BIP32:

What is its public key?

Now create m/0H/1. Verify the private/public keys are correct with BIP32 documentation.

Now create m/0H/1/2H. Verify the private/public keys are correct with BIP32 documentation.

Now create m/0H/1/2H/2. Verify the private/public keys are correct with BIP32 documentation.

Now create m/0H/1/2H/2/1000000000. Verify the private/public keys are correct with BIP32 documentation.

Can you get the last one straight from the master key without all the intermediates?