Floyce Shitandi

Assignment 2 : Keys, Addresses and Wallets

POW : RPC COMMANDS

Bitcoin-cli -regtest getwalletinfo: Outputs the wallet information

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getwalletinfo
{
  "walletname": "Flo1",
  "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": 1762961284,
  "lastprocessedblock": {
    "hash": "5da1587defd98e986ab75e91c7744f4d46c241cf240dbaebd37741bf902f346c",
    "height": 306
```

This gets the mining information

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getmininginfo
{
  "blocks": 306,
  "difficulty": 4.656542373906925e-10,
  "networkhashps": 0.0001389990102112148,
  "pooledtx": 0,
  "chain": "regtest",
  "warnings": [
    "This is a pre-release test build - use at your own risk - do not use for mining or mer
chant applications"
  ]
}
```

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getblockcount
306
```

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnewaddress
bcrt1qs2u2wf42danmjxwjv0q2pxn6wnjt5qljhvk2x9
black_dev@Black:~/bitcoin-network-Floyce$
```

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnetworkinfo >> output.txt
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnetworkinfo
{
  "version": 289900,
  "subversion": "/Satoshi:28.99.0/",
  "protocolversion": 70016,
  "localservices": "0000000000000c09",
  "localservicesnames": [
    "NETWORK",
    "WITNESS",
    "NETWORK_LIMITED",
    "P2P_V2"
  ],
  "localrelay": true,
  "timeoffset": 0,
  "networkactive": true,
  "connections": 1,
  "connections_in": 1,
  "connections_out": 0,
  "networks": [
    {
      "name": "ipv4",
      "limited": false,
      "reachable": true,
      "proxy": "",
      "proxy_randomize_credentials": false
    },
    {
      "name": "ipv6",
      "limited": false,
      "reachable": true,
      "proxy": "",
      "proxy_randomize_credentials": false
    },
    {
      "name": "onion",
```

```
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getblockcount
306
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnewaddress
bcrt1qs2u2wf42danmjxwjv0q2pxn6wnjt5qljhvk2x9
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnetworkinfo >> output.txt

bitcoin-cli -regtest getwalletinfo >> output.txt
bitcoin-cli -regtest getmininginfo >> output.txt
bitcoin-cli -regtest getblockcount >> output.txt
bitcoin-cli -regtest getnewaddress >> output.txt
black_dev@Black:~/bitcoin-network-Floyce$ ./test/functional/test_runner.py
-bash: ./test/functional/test_runner.py: No such file or directory
black_dev@Black:~/bitcoin-network-Floyce$ ./test/functional/filename_test.py
-bash: ./test/functional/filename_test.py: No such file or directory
black_dev@Black:~/bitcoin-network-Floyce$ bitcoin-cli -regtest getnetworkinfo >> output.txt

bitcoin-cli -regtest getwalletinfo >> output.txt
bitcoin-cli -regtest getmininginfo >> output.txt
bitcoin-cli -regtest getblockcount >> output.txt
black_dev@Black:~/bitcoin-network-Floyce$ git add output.txt
git commit -m "Add 5 RPC commands output for Assignment 1"
[main 152f4a0] Add 5 RPC commands output for Assignment 1
 1 file changed, 255 insertions(+)
black_dev@Black:~/bitcoin-network-Floyce$ git remote set-url origin git@github.com:DadaDeve
lopers/bitcoin-network-Floyce.git
git push origin main
Enter passphrase for key '/home/black_dev/.ssh/id_rsa':
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 8 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 1.19 KiB | 1.19 MiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To github.com:DadaDevelopers/bitcoin-network-Floyce.git
   27fbc36..152f4a0  main -> main
black_dev@Black:~/bitcoin-network-Floyce$
```

```
lack_dev@Black:~/keys-addresses-and-wallets-Floyce$ bitcoin-cli -regtest -rpcwallet=assignment2wallet getnewaddress ""
legacy
gFwM7y9HM5j7x6UB8gYr4qf2AhDtLCioX
lack_dev@Black:~/keys-addresses-and-wallets-Floyce$ bitcoin-cli -regtest -rpcwallet=assignment2wallet getnewaddress ""
bech32
crt1q2ml0cj2pgqelt6eq07q5cn9pdf6r04evhlgvmz
lack_dev@Black:~/keys-addresses-and-wallets-Floyce$ bitcoin-cli -regtest -rpcwallet=assignment2wallet getnewaddress ""
bech32m
crt1pt8epjenmh705ctwu7c5kdpfkq376j3lrsas9p4fsdcezzlk707qqvah3pr
lack_dev@Black:~/keys-addresses-and-wallets-Floyce$
```

2. Explain the difference between hardened and non-hardened keys

- **Hardened vs Non-Hardened Keys:**

- **Hardened keys:** Derived in a way that the child private key cannot be used to compute the parent private key. Safer if someone gets access to a child key.
- **Non-hardened keys:** Child keys can reveal parent public keys if compromised. Easier for some wallet operations but slightly less secure.

3. Why Deterministic Wallets are preferred:

- Deterministic wallets generate all keys from a single seed phrase (BIP32/BIP39).

  Advantages: Easy backup, recoverable with just the seed, all addresses can be generated deterministically. No need to store multiple private keys.