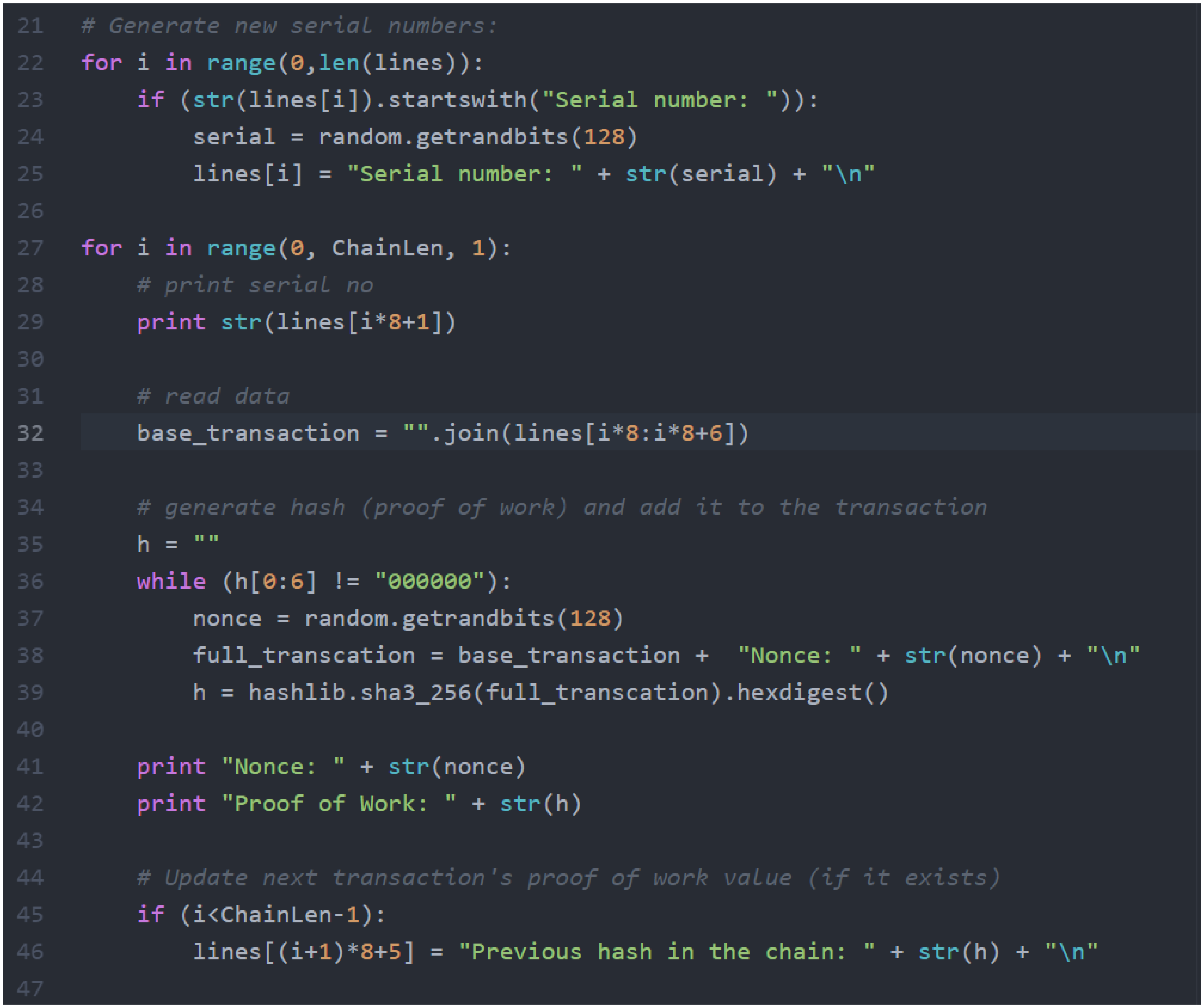
Project Step 1



```
21  # Generate new serial numbers:
22  for i in range(0,len(lines)):
23      if (str(lines[i]).startswith("Serial number: ")):
24          serial = random.getrandbits(128)
25          lines[i] = "Serial number: " + str(serial) + "\n"
26
27  for i in range(0, ChainLen, 1):
28      # print serial no
29      print str(lines[i*8+1])
30
31      # read data
32      base_transaction = "".join(lines[i*8:i*8+6])
33
34      # generate hash (proof of work) and add it to the transaction
35      h = ""
36      while (h[0:6] != "000000"):
37          nonce = random.getrandbits(128)
38          full_transcation = base_transaction +  "Nonce: " + str(nonce) + "\n"
39          h = hashlib.sha3_256(full_transcation).hexdigest()
40
41      print "Nonce: " + str(nonce)
42      print "Proof of Work: " + str(h)
43
44      # Update next transaction's proof of work value (if it exists)
45      if (i<ChainLen-1):
46          lines[(i+1)*8+5] = "Previous hash in the chain: " + str(h) + "\n"
47
```

Figure 1

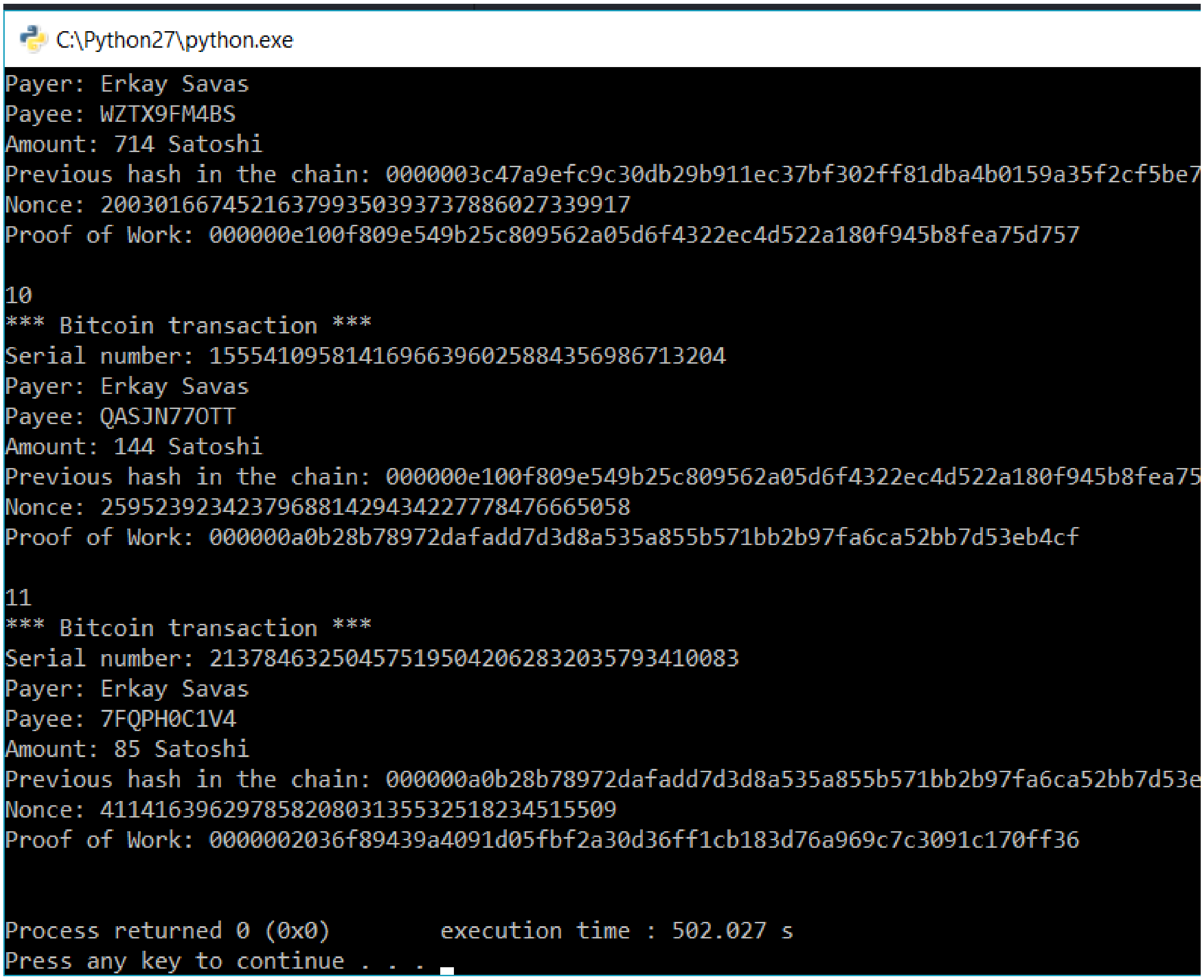
First, I am reading the given file *LongestChain.txt* and modifying its Serial Numbers to supposedly make new transactions.

Then, I copy everything except the nonces (notice i*8+6 instead of i*8+7 on line 32).

Then, until the while condition is satisfied, I keep creating a random 128-bit integer as the nonce and hashing all the information together as the validation example, using sha3_256 hashing function.

I also carry the proof of work hash to the next transaction. (lines 45-46)

The output is shown below in Figure 2.



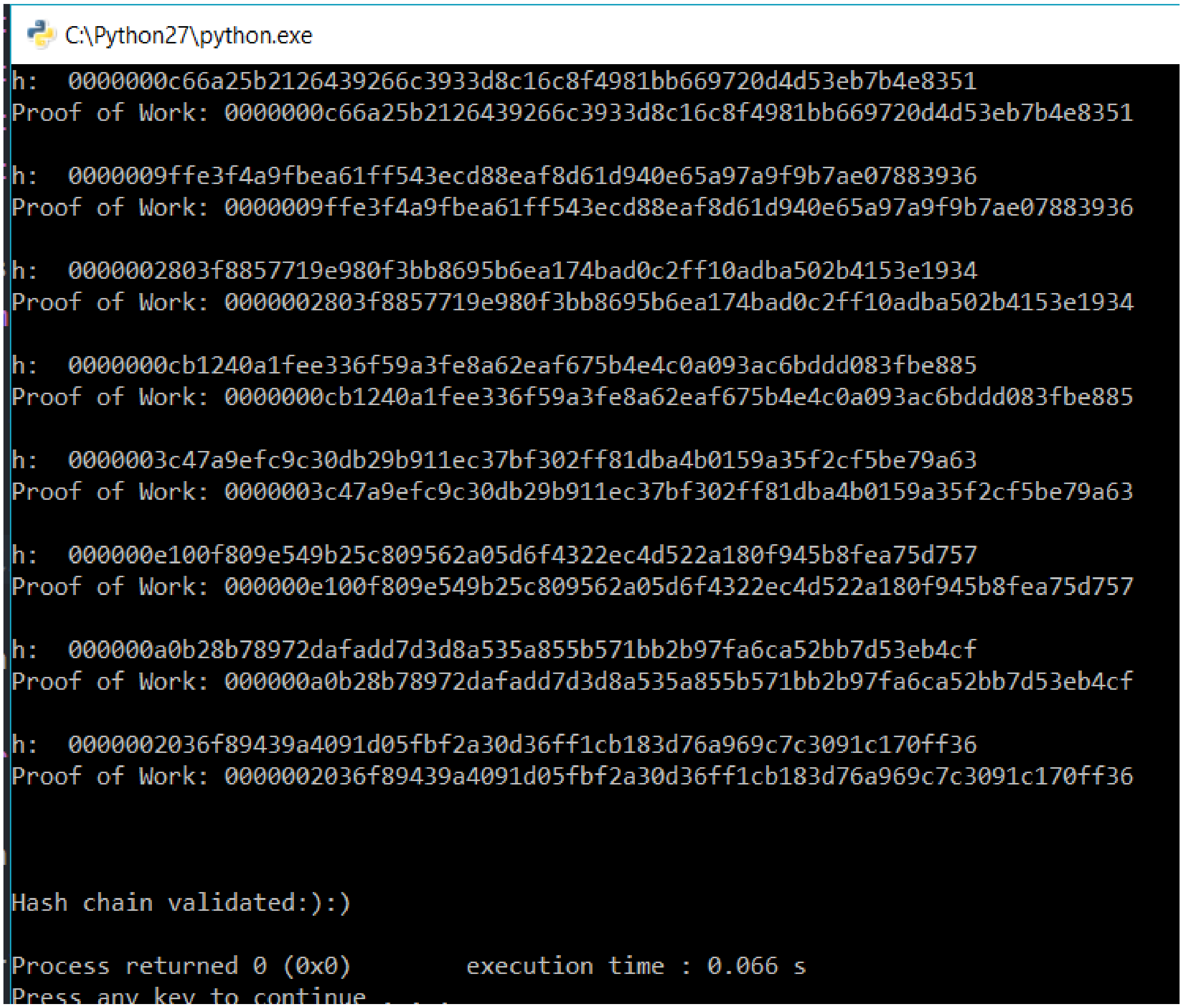
C:\Python27\python.exe

```
Payer: Erkay Savas
Payee: WZTX9FM4BS
Amount: 714 Satoshi
Previous hash in the chain: 0000003c47a9efc9c30db29b911ec37bf302ff81dba4b0159a35f2cf5be7
Nonce: 200301667452163799350393737886027339917
Proof of Work: 000000e100f809e549b25c809562a05d6f4322ec4d522a180f945b8fea75d757

10
*** Bitcoin transaction ***
Serial number: 15554109581416966396025884356986713204
Payer: Erkay Savas
Payee: QASJN77OTT
Amount: 144 Satoshi
Previous hash in the chain: 000000e100f809e549b25c809562a05d6f4322ec4d522a180f945b8fea75
Nonce: 259523923423796881429434227778476665058
Proof of Work: 000000a0b28b78972dafadd7d3d8a535a855b571bb2b97fa6ca52bb7d53eb4cf

11
*** Bitcoin transaction ***
Serial number: 213784632504575195042062832035793410083
Payer: Erkay Savas
Payee: 7FQPH0C1V4
Amount: 85 Satoshi
Previous hash in the chain: 000000a0b28b78972dafadd7d3d8a535a855b571bb2b97fa6ca52bb7d53e
Nonce: 41141639629785820803135532518234515509
Proof of Work: 0000002036f89439a4091d05fbf2a30d36ff1cb183d76a969c7c3091c170ff36


Process returned 0 (0x0)        execution time : 502.027 s
Press any key to continue . . .
```

Figure 2

As seen, it took quite a bit of time (~8 minutes) to find the hashes.

Later, I copy-pasted the new values from the output to the file *transactions.txt,* while removing the empty lines and element numbers. The validation worked as seen in Figure 3 below.



```
h:  0000000c66a25b2126439266c3933d8c16c8f4981bb669720d4d53eb7b4e8351
Proof of Work: 0000000c66a25b2126439266c3933d8c16c8f4981bb669720d4d53eb7b4e8351

h:  0000009ffe3f4a9fbea61ff543ecd88eaf8d61d940e65a97a9f9b7ae07883936
Proof of Work: 0000009ffe3f4a9fbea61ff543ecd88eaf8d61d940e65a97a9f9b7ae07883936

h:  0000002803f8857719e980f3bb8695b6ea174bad0c2ff10adba502b4153e1934
Proof of Work: 0000002803f8857719e980f3bb8695b6ea174bad0c2ff10adba502b4153e1934

h:  0000000cb1240a1fee336f59a3fe8a62eaf675b4e4c0a093ac6bddd083fbe885
Proof of Work: 0000000cb1240a1fee336f59a3fe8a62eaf675b4e4c0a093ac6bddd083fbe885

h:  0000003c47a9efc9c30db29b911ec37bf302ff81dba4b0159a35f2cf5be79a63
Proof of Work: 0000003c47a9efc9c30db29b911ec37bf302ff81dba4b0159a35f2cf5be79a63

h:  000000e100f809e549b25c809562a05d6f4322ec4d522a180f945b8fea75d757
Proof of Work: 000000e100f809e549b25c809562a05d6f4322ec4d522a180f945b8fea75d757

h:  000000a0b28b78972dafadd7d3d8a535a855b571bb2b97fa6ca52bb7d53eb4cf
Proof of Work: 000000a0b28b78972dafadd7d3d8a535a855b571bb2b97fa6ca52bb7d53eb4cf

h:  0000002036f89439a4091d05fbf2a30d36ff1cb183d76a969c7c3091c170ff36
Proof of Work: 0000002036f89439a4091d05fbf2a30d36ff1cb183d76a969c7c3091c170ff36



Hash chain validated:):)

Process returned 0 (0x0)        execution time : 0.066 s
Press any key to continue . . .
```

Figure 3