Modul 7 inlämningsuppgift P3

Author: Samuel Östholm, samuel.ostholm@student.hv.se

För att konstruera blocken som produceras av mitt program så har jag till stor del använt mig av redan genererade block som jag manuellt avkodat med hjälp av officiella dokumentationen: https://en.bitcoin.it/wiki/Protocol_documentation

Även Ranzhangs kod har varit en stor hjälp för att förstå hur det rent praktiskt går till att bygga en header i little endian:

https://github.com/ranzhang/blockchain/tree/master/Bitcoin/headerhashing?utm_campaign=News&utm_medium=Community&utm_source=DataCamp.com

Programmet startar genom att man kör bterpc.py som kommer skapa en instans av sig själv och sedan anropa metoden start_mine med 100000 försök att hitta rätt hash. Programmet kommer sedan skriva ut lägsta hashen för varje process som körs. Med kommer även en utskrift av blocket och en avkodning från decodeBlock samt hastighet och hur lång tid det tog.

All kod är kommenterad, så titta på den för en djupare beskrivning.

Nedan syns ett block som jag har genererat.

Block info:

version: 02000000
prev_block_header:
3c3873e63b7942b7b6907f471ef163444c02418c96102792ea8d674600000000
merkle root: b005a1936de203068e76805a4754ea5c8c84b12209d9d96e6c1b87939e39d7a7
time: 44642f5c
nbits: 52c4001d
nonce: 00000000
tx count: 01
raw transaction:
01000000000101000000000000000000000000000000000000000000000000000000000000000000ffffffff0403849d00ffffffff0200f2052a010000001976a9144b7da9f99bac968111826ac177107ee046500db788ac0000000000000000266a24aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48bebd836974e8cf90120000000000000000000000000000000000000000000000000000000000000000000000000000000000

Här är det avkodade blocket med hjälp av decodeBlock:

Decode block:

Version: 0x2
Hash 30cc24d1250da211e8c6178ed519c1b517d7e47646178c873ab1b65db3d49550
Previous Hash 0000000046678dea922710968c41024c4463f11e477f90b6b742793be673383c
Merkle Root a7d7399e93871b6c6ed9d90922b1848c5cea54475a80768e0603e26d93a105b0
Time stamp 2019-01-04 13:48:52.000000+00:00 (UTC)
Difficulty 0x1d00c452
Nonce 0x00000000
None
1

########## Block Header ##########
Version: 0x2
Hash 30cc24d1250da211e8c6178ed519c1b517d7e47646178c873ab1b65db3d49550
Previous Hash 0000000046678dea922710968c41024c4463f11e477f90b6b742793be673383c
Merkle Root a7d7399e93871b6c6ed9d90922b1848c5cea54475a80768e0603e26d93a105b0
Time stamp 2019-01-04 13:48:52.000000+00:00 (UTC)
Difficulty 0x1d00c452
Nonce 0x00000000

Tx Count: 1

========== No. 0 Transaction ==========
Txid: a7d7399e93871b6c6ed9d90922b1848c5cea54475a80768e0603e26d93a105b0
Tx Version: 0x1
Witness flag: True
Inputs: 1
Prev. Tx Hash:
0000000000000000000000000000000000000000000000000000000000000000
Prev. Index: ffffffff (coinbase)
Script Length: 4
ScriptSig: 03849d00
ScriptSig, txt: b'\x03\x84\x9d\x00'
Sequence: ffffffff
Outputs: 2
Value: 5000000000 satoshi
Script Len: 25
ScriptPubkey: 76a9144b7da9f99bac968111826ac177107ee046500db788ac
Value: 0 satoshi
Script Len: 38

ScriptPubkey:
6a24aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48bebd836974e8cf9
Witness chunks: 1
Data length: 32
Witness data:
0000000000000000000000000000000000000000000000000000000000000000
Lock Time: 0
end of all 1 transactions
None

Som bas för coinbase transaktionen använde jag mig av transaktionen:
51286b72de4e7712cd614c34ae086afb0ac8532d83b361471e41dd86046af488

Notering:
Upptäckte att merkleroten för ett block när det är endast en coinbase tx är txid.