Homework 7: Exploring the Bitcoin Blockchain

For this problem, you will be exploring the Bitcoin blockchain, using the website https://blockexplorer.com/. (If you prefer, you may alternatively be able to use https://blockchain.info/ although I wrote up my model answer to this homework using blockexplorer.com.)

Look at block 434726

(a) How many transactions are in this block?

Block #434726

BlockHash 000000000000000000318c164ec7a0d42af3ceae1adb50c853a44ce193d80b5e6

Summary

Number Of Transactions	1876	**Difficulty**	258522748404.51544
Height	434726 (Mainchain)	**Bits**	180440c4
Block Reward	12.5 BTC	**Size (bytes)**	999873
Timestamp	Oct 17, 2016 10:30:49 AM	**Version**	536870912
Mined by	Discus Fish	**Nonce**	4722182
Merkle Root	c741896aadffb07a17bcc2c16bf6bd...	**Next Block**	434727
Previous Block	434725		

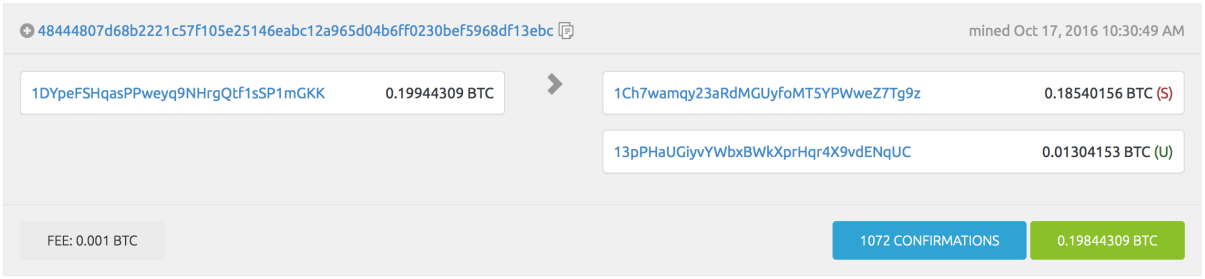
1876 Transactions.

(b) The block reward was 12.5 BTC, but how much in total did the miner who found this block receive for doing so? What accounts for the discrepancy?

Transactions

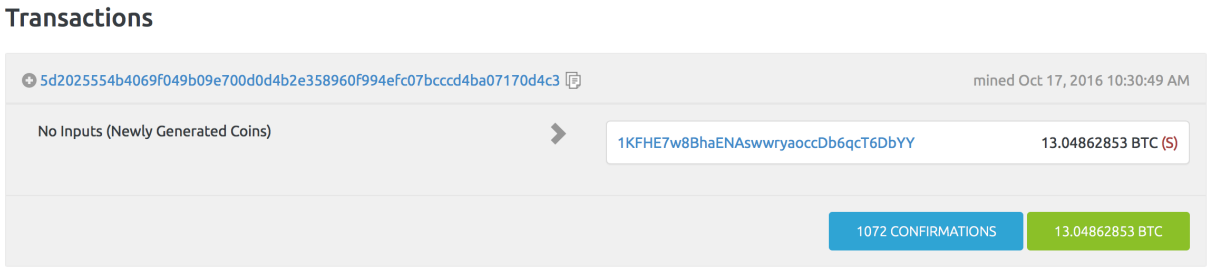
The miner received 13.04862853 BTC for solving the block. The discrepancy is due to the fee the miner received for solving each transaction. For instance, the difference between the input and output in each transaction, is the fee given to the miner for solving that particular transaction. There could also be transactions which are solved without any fee associated in solving it.

(c) Look at the fourth transaction, for 0.19844309 BTC. How many inputs and outputs are there? What is the most likely explanation of why the recipients did not receive the same amount?



In this transaction, there is 1 input and 2 outputs. The recipients did not receive the same amount because in Bitcoin transactions, the exact value of bitcoins could not be sent most of the time as the bitcoin amount cannot be split to send an exact amount to the recipient. In such cases, other bitcoin transactions which have values greater than the amount to be sent serves as input or 2 or more bitcoin transactions which add up (or more than) to the amount to be sent serve as inputs. So, the recipient receives the amount and sends back the change to the sender. That is the reason for 2 outputs of different values.

(d) Still looking at the fourth transaction: what is the sum of the inputs? What is the sum of the outputs? What are the first six characters of the address of the recipient of the difference between (inputs – outputs)?

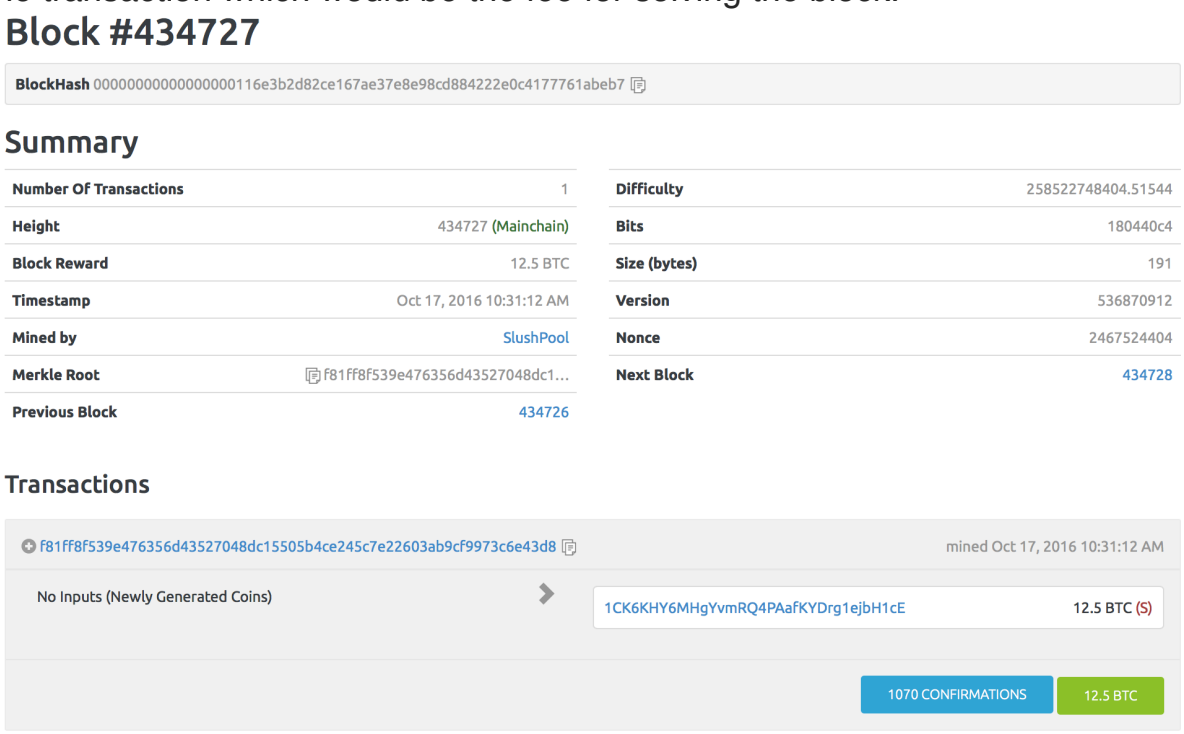


Sum of the inputs = 0.19944309 BTC
Sum of the outputs = 0.19844309 BTC
The difference of 0.001 BTC is the fee paid to the miner for solving the transaction.
First six characters of the address of recipient of difference between inputs and outputs is 1KFHE7

Look at the block 434727.

(a) What is unusual about this block? What is the most likely reason that this unusual occurrence happened?

This block has no input (but contains newly generated bitcoins) but has an output. The unusual thing about this block is that there is only one transaction and that pays the miner's fee for solving the block. This happens because the probability of solving a block increases with time and peaks at 10 mins and then the probability decreases. Most of the miners take close to 10 mins to solve the block until which the number of transactions in the block keeps increasing. There are instances, where the block is solved as soon as it enters into the miner's pool. So, there is just one transaction which would be the fee for solving the block.



Block #434727

BlockHash 00000000000000000116e3b2d82ce167ae37e8e98cd884222e0c4177761abeb7

Summary

Number Of Transactions	1	**Difficulty**	258522748404.51544
Height	434727 (Mainchain)	**Bits**	180440c4
Block Reward	12.5 BTC	**Size (bytes)**	191
Timestamp	Oct 17, 2016 10:31:12 AM	**Version**	536870912
Mined by	SlushPool	**Nonce**	2467524404
Merkle Root	f81ff8f539e476356d43527048dc1...	**Next Block**	434728
Previous Block	434726		

Transactions

f81ff8f539e476356d43527048dc15505b4ce245c7e22603ab9cf9973c6e43d8 — mined Oct 17, 2016 10:31:12 AM

No Inputs (Newly Generated Coins) → 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE 12.5 BTC (S)

1070 CONFIRMATIONS | 12.5 BTC

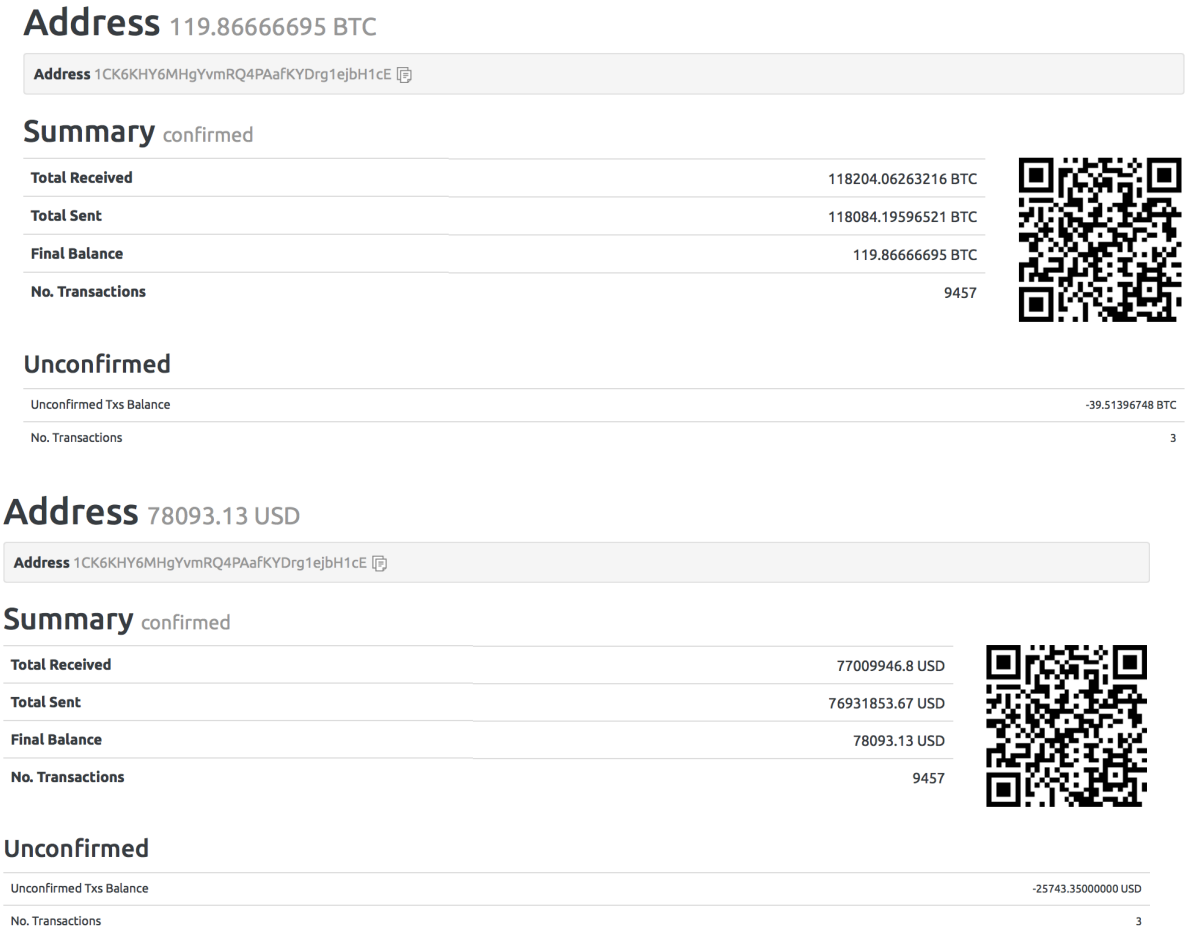
(b) What nonce did this miner find?

This miner found the nonce 2467524404.

(c) On average, how many hashes would you expect a miner to need to try to find this particular nonce?

Average hashes to try before finding a particular nonce = difficulty * 2^32 = 258522748404.51544 * 2^32 = 1.1103467e+21 hashes

(d) Look at *all* the total of all bitcoin transactions that this miner has received over the lifetime of Bitcoin. (State the precise time (in PDT) that your figure is accurate as of – which should be a time between 10/18/16 and 10/25/16). What is the total amount of bitcoins? Roughly how much is this in US dollars? How has this miner managed to receive so many bitcoins in transactions?
Oct 24, 9.36 PM



Address 119.86666695 BTC

Address 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE

Summary confirmed

Total Received	118204.06263216 BTC
Total Sent	118084.19596521 BTC
Final Balance	119.86666695 BTC
No. Transactions	9457

Unconfirmed

Unconfirmed Txs Balance	-39.51396748 BTC
No. Transactions	3

Address 78093.13 USD

Address 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE

Summary confirmed

Total Received	77009946.8 USD
Total Sent	76931853.67 USD
Final Balance	78093.13 USD
No. Transactions	9457

Unconfirmed

Unconfirmed Txs Balance	-25743.35000000 USD
No. Transactions	3

Total bitcoins received 118204.06263216 BTC
That is equal to 77009946.8 USD

The miner has managed to receive so many bitcoins because the miner belongs to a pool of miners with huge computing power. This enables him to solve many blocks and receive a huge amount of bitcoins.