

1/

	k=2	k=3	k=4	k=5	k=6
(xS,hash value)	(1859057315this_is_a_bitcoin_block_of_43435708,0056046a282a59b3df085394bcd93f37159d1888a05177a7c0c23e4718b132d7)	(25619047this_is_a_bitcoin_block_of_43435708,0002f43f03672e5ce1aa622328c5d3022d98dbf1f078369adda84cef911593ff)	(1050088280this_is_a_bitcoin_block_of_43435708,0000951df7cf543b9f924d060a9eb884ceb2b8449a2f4e8b4bcb3821a3c5d04a)	(1456362837this_is_a_bitcoin_block_of_43435708,000009b3609f78d6713b56cc62a01bbd281e8e73e4bcb5983e7878a637e5d4b7)	(1703000360this_is_a_bitcoin_block_of_43435708,00000049d427729d69166d9ecb6a52513ebf99052d9606cad880979699d040b3)
n trials	10000	10000	100000	1000000	10000000
Time elapsed	3s	3s	4s	6s	31s

2/

### Result:

k = 7

n trials = 500000000

(xS, hash value) =

(110518648this\_is\_a\_bitcoin\_block\_of\_43435708,00000004aa0b4bac88ecbfbbb9615b6f318d4296e31ef659027fae70e3e94fff)

Time elapsed:1238s

### Cluster's configuration:

Master node: Standard (1 master, N workers)

Machine type: n1-standard-4

Number of GPUs: 0

Primary disk type: pd-standard

Primary disk size: 500GB

Local SSDs: 0

Worker nodes: 2

Machine type: c2-standard-4

Number of GPUs: 0

Primary disk type: pd-standard

Primary disk size: 500GB

Local SSDs: 0

I tried 10 million trials as I did with k=6 but I could not find the correct xS, so I adjusted to 20 million trials, and then 50 million trials when I finally found the right xS.

3/

```
//iter.map(x => rand.nextInt(Int.MaxValue - 1) + 1)
iter.map(x => x + 1)
```

	k=2	k=3	k=4	k=5	k=6
(xS,hash value)	(391this_ is_a_bitc oin_block of_43435 708,0023e 55ba2d08c 1ce14bbaa b43aa5942 99051f767 0924a67dd 8cb0a4826 68647)	(1633this _is_a_bit coin_bloc k_of_4343 5708,000b 6080a63bd b3fb191c2 72dc39355 2f6a858f2 c3a279087 6d57c69aa 094e01)	(63884thi s_is_a_bi tcoin_blo ck_of_434 35708,000 08f0b7e87 b95efa6f1 1a7e95fd7 2af990897 e3ef8d6da e757ea1e0 627a91e)	(816558th is_is_a_b itcoin_bl ock_of_43 435708,00 000181942 ea57bb6bd 049885bff 0155e32cd 960bf3d32 f9bd5a759 80ef3647)	
n trials	10000 391	10000 1633	100000 63884	1000000 816558	10000000 Not exists
Time elapsed	3s	3s	4s	6s	27s

Using this method to find the correct xS is fast if k is small. When k grows, xS grows even faster, so it takes so many trials until we get a correct xS. As demonstrated in the table, when k=6, 10000000 trials were not enough to get a correct xS. But with the random method, we could get a correct xS.

Thus, for k that is large, we may have a better chance of getting the correct xS if we use the random method instead of the linear method.