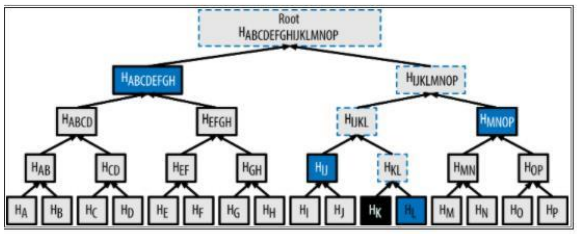
Questions:

How to let any Bitcoin node prove that the Transaction K is included in a block? • •



Please study How to let any Bitcoin node prove that the Transaction K is included in a block? before answering the following questions.

- Please build up the above Merkle Tree using the following data set, and assuming that the hash function is "msg%7"
  - Transaction A: 31
  - Transaction B: 54
  - Transaction C: 29
  - Transaction D: 7
  - Transaction E: 23
  - Transaction F: 21
  - Transaction G: 27
  - Transaction H: 13
  - Transaction I: 15
  - Transaction J: 11
  - Transaction K: 26
  - Transaction L: 34
  - Transaction M: 89
  - Transaction N: 32
  - Transaction O: 18
  - Transaction P: 17
- If a Bitcoin node would like to prove that Transaction H is part of the block.
  - What information does the system need to provide?
  - What does the bitcoin node need to do?

Ans:

As we know the equation is Hash = msg % 7

H(AB) = H(A) + H(B) "HA + HB" is the concatenation of "HA" and "HB"

We calculate the hash for each one first,

Transaction A: 31 % 7 = 3
Transaction B: 54 % 7 = 5
Transaction C: 29 % 7 = 1
Transaction D: 7 % 7 = 0
Transaction E: 23 % 7 = 2
Transaction F: 21 % 7 = 0
Transaction G: 27 % 7 = 6
Transaction H: 13 % 7 = 6
Transaction I: 15 % 7 = 1
Transaction J: 11 % 7 = 4
Transaction K: 26 % 7 = 5
Transaction L: 34 % 7 = 6
Transaction M: 89 % 7 = 5

Transaction N: 32 % 7 = 4
Transaction O: 18 % 7 = 4
Transaction P: 17 % 7 = 3

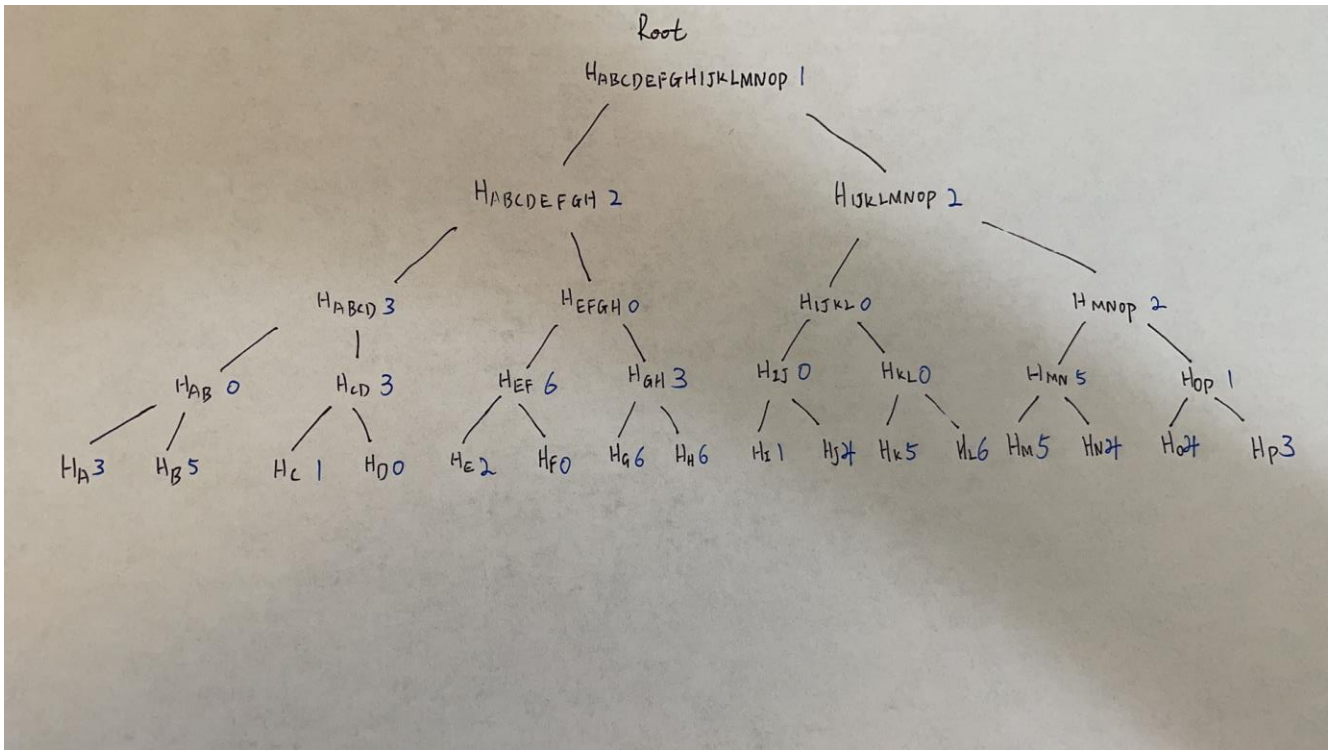
Then, calculate the combinations,

H(AB) = 35 % 7 = 0
H(CD) = 10 % 7 = 3
H(EF) = 20 % 7 = 6
H(GH) = 66 % 7 = 3
H(IJ) = 14 % 7 = 0
H(KL) = 56 % 7 = 0
H(MN) = 54 % 7 = 5
H(OP) = 43 % 7 = 1

H(ABCD) = 3 % 7 = 3
H(EFGH) = 63 % 7 = 0
H(IJKL) = 0 % 7 = 0
H(MNOP) = 51 % 7 = 2

H(ABCDEFGH) = 30 % 7 = 2
H(IJKLMNOP) = 2 % 7 = 2

H(ABCDEFGHIJKLMNOP) = 22 % 7 = 1



Step 1: The system provides two sets of information:

Transaction H ：

H(G) => H(EF) => H(ABCD) => H(IJKLMNOP)

Step 2: The Bitcoin node need to do:

Transaction H ：

H(GH) => H(EFGH) => H(ABCDEFGH) => MERKLE ROOT