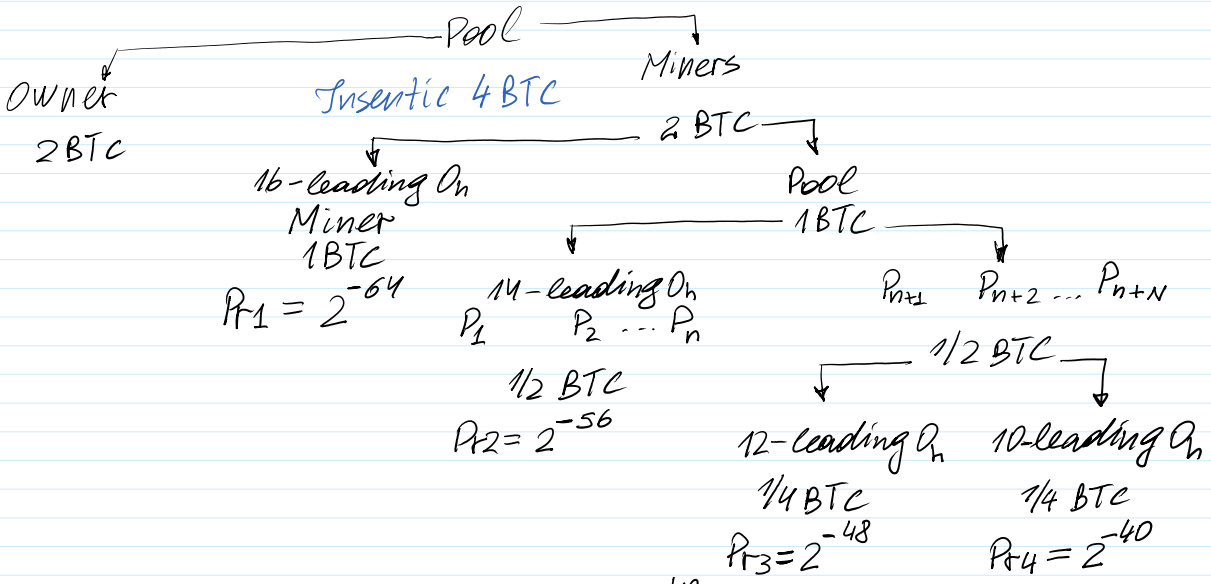
Shares

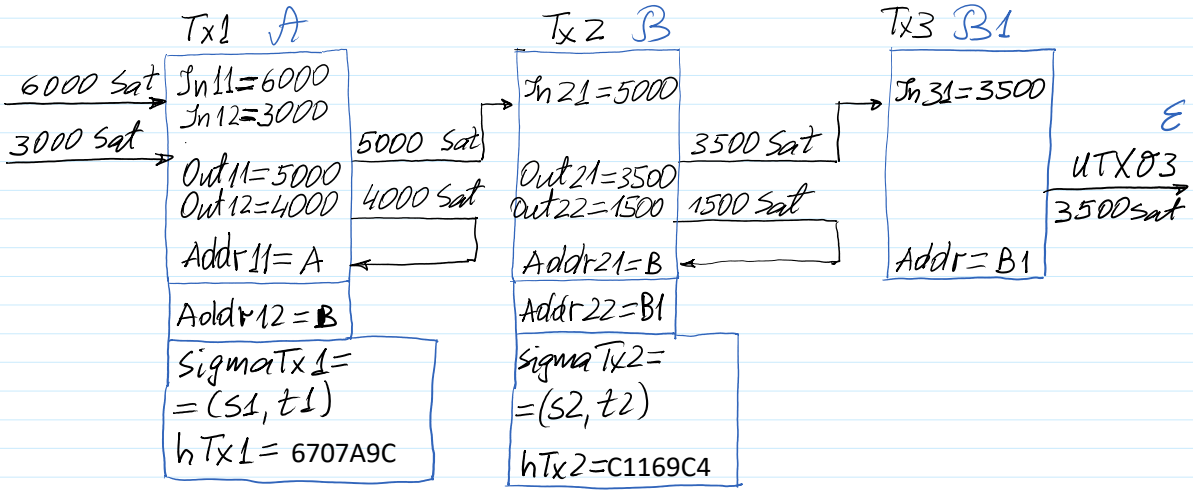
$Pr\{\text{to compute h-value with 16 leading hex n.}\} = \frac{2^{192}}{2^{256}} =$

$= 2^{192} \cdot 2^{-256} = 2^{192-256} = 2^{-64}$ // If $Pr = \frac{1}{2} = 2^{-1} \Rightarrow$ 2 trials in average.



Assume student has $1\,Th/s = 2^{40}\,h/s$.
Let the number of competitors is 2^{20}.
Then the reward for mined 10-leading Q_h
$1 \cdot 2^{-2} / 2^{20} = 2^{-22}$ BTC.

Block mining

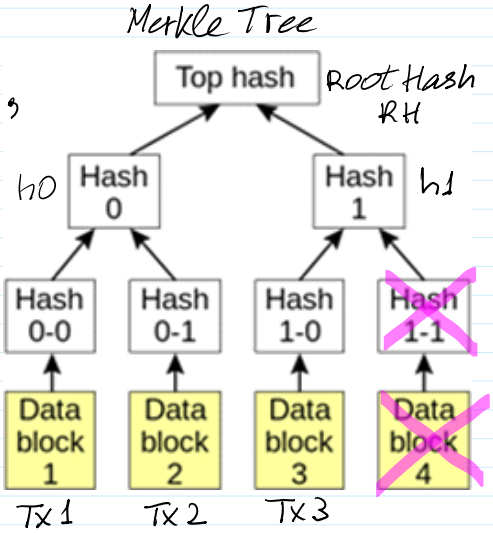


Tx1 = '1 : In = 9000 || Out1 = 5000 || Out2 = 4000 || B || A'
Tx2 = '2 : In = 5000 || Out1 = 3500 || Out2 = 1500 || B1 || B'

Tx3 = '3 : In=3500||Out1=3500||Out2=0||E||B1'

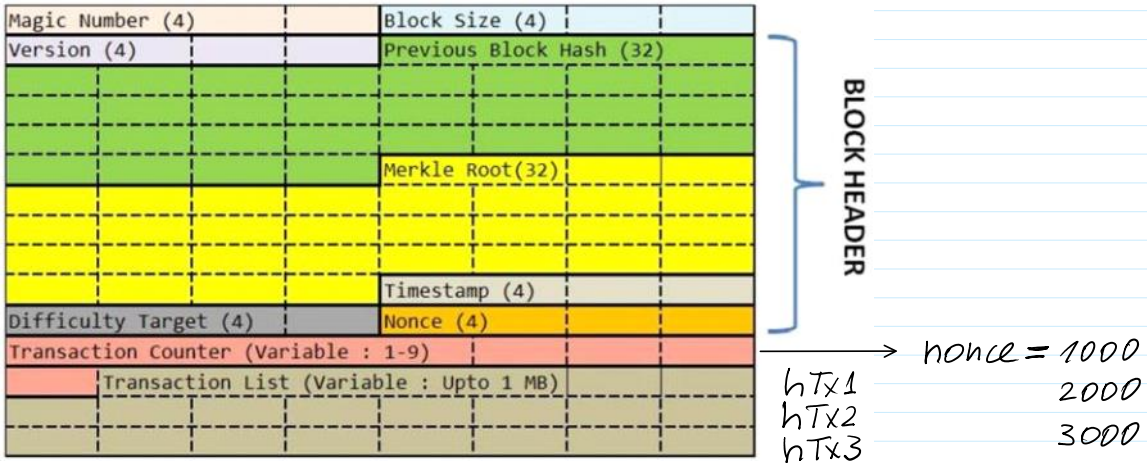
3 Transactions: 1 Input --> 2 Output
Merkle Tree 3 --> 1

>> h00 = h28(Tx1) % h00 = 'ansv'
>> h01 = h28(Tx2)
>> h10 = h28(Tx3)
>> h0 = h28(h00||h01)
>> h1 = h10
>> RH = h28(h0||h1)



>> hTx1=dec2hex(h1Sig)
hTx1 = 6707A9C

>> hTx2=dec2hex(h2Sig)
hTx2 = C1169C4



>> PrBlh=h28('nonce=1020')
PrBlh = 0CAF06F

Dificulty target DT = ϕHHHHHH

Block1: PrBlh: PrBlh=0CAF06F

Rh : Rh=89B5B94

hTx1=6707A9C

hTx2=C1169C4

nonce : nonce=1000 Person No 1 in AIS list
nonce=2000 No2

nonce : nonce=1000 Person No 1 in AIS list
nonce=2000 No2
nonce=3000 No3
.....

Block numbers corresponds to your numbers in AIS list.

'Bl1 : PrBl = ... || Rh1 = ... || hTx1 = ... || hTx2 = ... || nonce = 1000'

```
>> Bl1M=h28('Bl1:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=1000')
Bl1M = D99C1E7

>> Bl1M=h28('Bl1:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=2018')
Bl1M = 06B0772
```

h28 : computes h - value of 28 bits
According to the difficulty target the adequate mined block must have leading hexadecimal 0 or 4 leading 0_b bits.
All available h - values with 28 bits length is equal to

```
>> 2^28   ans =  268435456
```

The number of adequate mined values is equal to any 28 - 4 = 24 bits values

```
>> 2^24   ans =  16777216
```

The probability to mine a block is the following:

$$Pr = \frac{\text{adequat number of values}}{\text{total number of values}} = \frac{2^{24}}{2^{28}} = 2^{-4} = 1/16$$

http://crypto.fmf.ktu.lt/xdownload/

- octave-6.3.0-w64-installer.exe
- Octave_Stud_2021.10 Updated.7z

Uprated functions: h24(), hd24(), AES128().