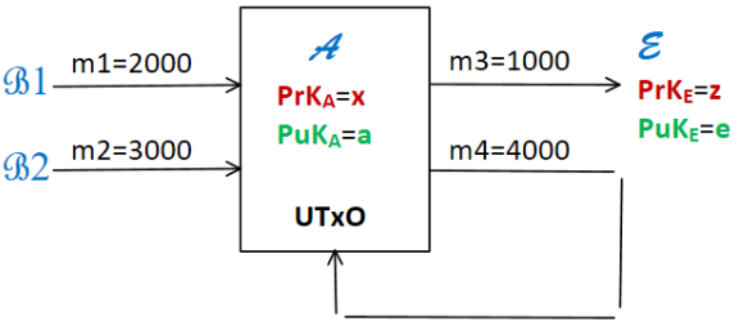



Transakcija yra sąžininga, jeigu pajamų ir išlaidų sumos sutampa, t.y. galioja balansas:

**m1+m2 = m3+m4**

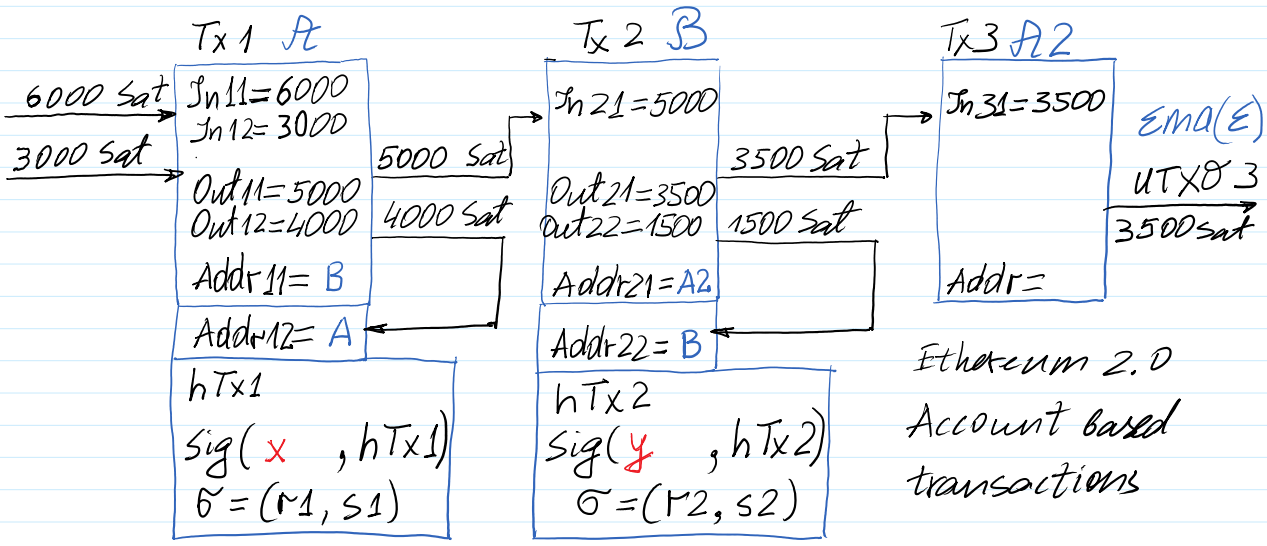
2000 + 3000 = 1000 + 4000 = 5000

Transakcijos duomeys:

1. Įėjimai: Siuntėjas, Suma, Gavėjas.
1. Išėjimai: Siuntėjas, Suma, Gavėjas.

Transakcija Tx: 'B1=A||2000||B2=A||3000||A=E||1000||A=A||4000'

Book-keeping --> Accounting --> Balance --> State UTxO system




Tx1 = '1 : In11 = 6000 || In12 = 3000 || Out11 = 5000 || Out12 = 4000 || Rec1 = B || Rec2 = A'

Tx2 = '2 : In21 = 5000 || Out21 = 3500 || Out22 = 1500 || Rec1 = A2 || Rec2 = B'

Tx3 = '3 : In31 = 3500 || Out31 = 3500 || Rec = E'

$h_1 = H(Tx1) = h28(Tx1)$

$h_2 = H(Tx2) = h28(Tx2)$

$h_3 = H(Tx3) = h28(Tx3)$

Transactions:

Tx_1 = 'Tx_1:In11=6000||In12=3000||Out11=5000||Out12=4000||Rec1=B||Rec2=A'

Tx_2='Tx_2:In21=5000||Out21=3500||Out22=1500||Rec1=A2||Rec2=B'

Tx_3='Tx_3:In31=3500||Out31=3500||Out32=0||Rec1=E||Rec2=A2'

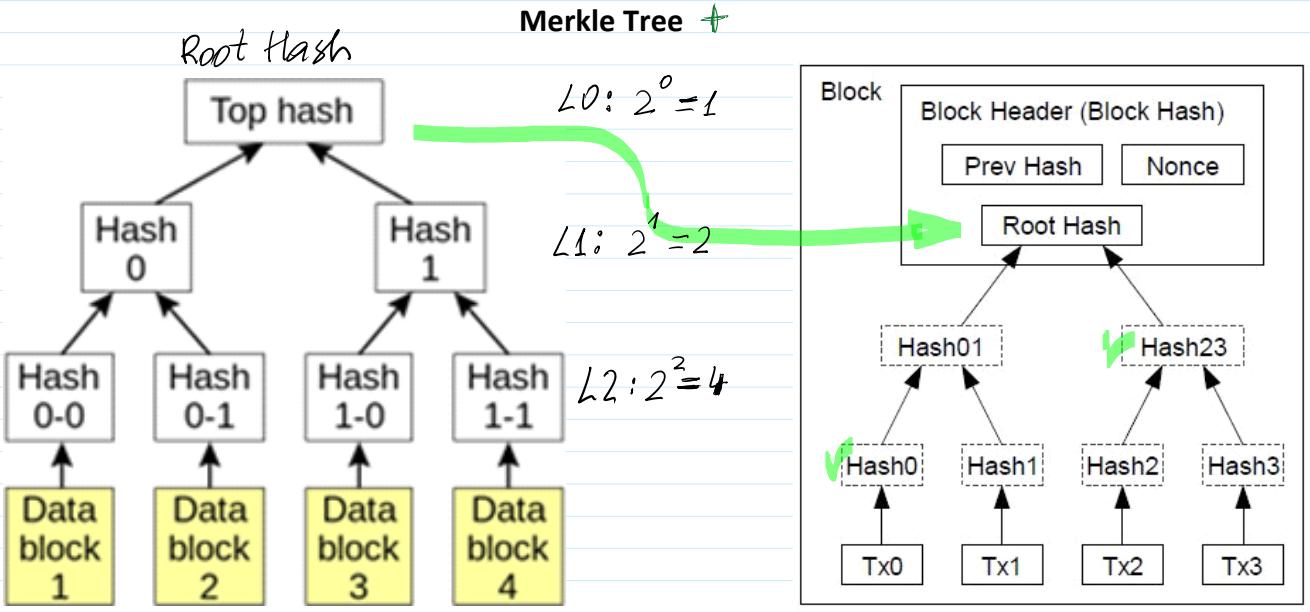
```
>> hTx_1=h28('Tx_1:In11=6000||In12=3000||Out11=5000||Out12=4000||Rec1=B||Rec2=A')
```

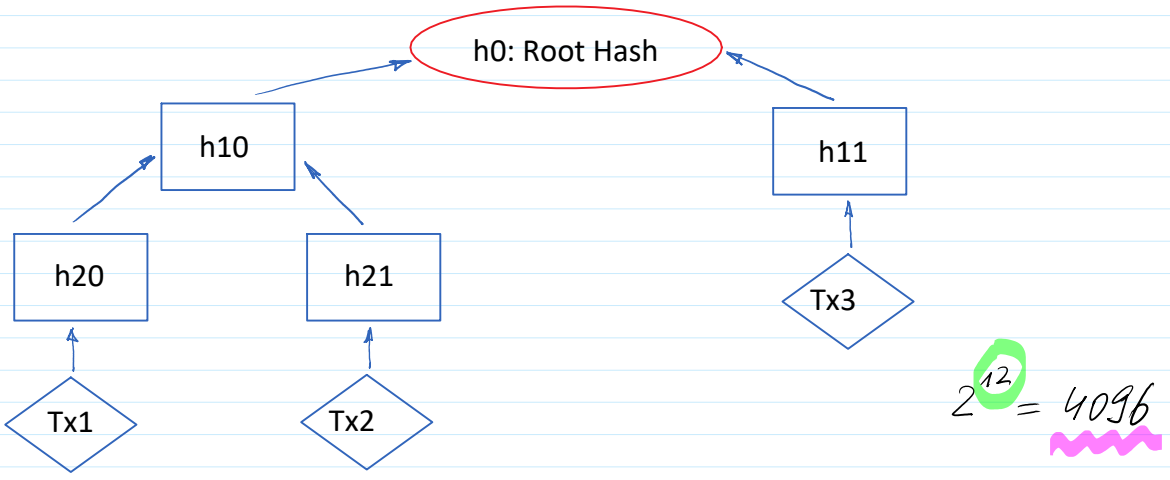
hTx_1 = 996BB7C
>> hTx_1=h28(Tx_1)
hTx_1 = 996BB7C

>> hTx_2=h28('Tx_2:In21=5000||Out21=3500||Out22=1500||Rec1=A2||Rec2=B')
>> hTx_2=h28(Tx_2)
hTx_2 = 977D75B

>> hTx_3=h28('Tx_3:In31=3500||Out31=3500||Out32=0||Rec1=E||Rec2=A2')
>> hTx_3=h28(Tx_3)
hTx_3 = 9201218

**Merkle Tree**




>> h20=h28(hTx_1)
**h20** = 996BB7C
>> h21=h28(hTx_2)
**h21** = 977D75B

>> h10=h28('996BB7C||977D75B')
h10 = 77F058A

**Root Hash: h0**

>> h21=h28(hTx_2)
**h21** = 977D75B
>> h11=h28(hTx_3)
**h11** = 9201218

>> h10=h28('996BB7C||977D75B')
h10 = 77F058A

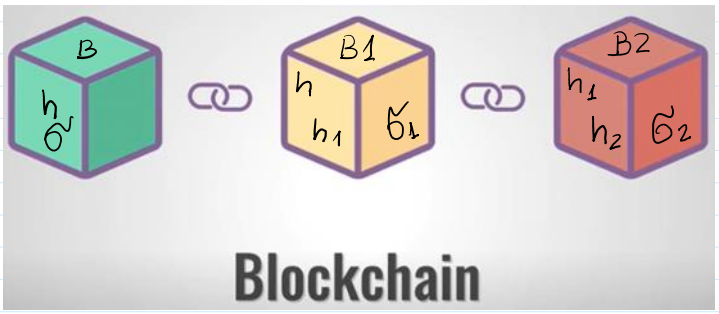
**Root Hash: h0**

>> h0=h28('77F058A||9201218')
**h0** = **91EFFF6**

Python : sha256

h20: 996BB7C
h21: 977D75B
h11: 9201218

h10: 77F058A
h0: **91EFFF6**




>> sha256('RootHash PrevHash 737327631')
ans = F4AE534CD226FAF799 8C8424B348E020BA80639A687E93A0B8C5130ED C51E6DE
C51E6DE
>> sha256('RootHash PrevHash 737327632')
ans = B856211DF2EE15E30AB770C1A43CE014ECFE573182AFD885B28D96854DBC5F21
>> sha256('RootHash PrevHash 737327633')
ans = 9C18C764E347A58E57AC3F7A3C2874D5889A0E802699FEA47EEFF8C03BFEDA69

>> RootHash=h0
RootHash = 91EFFF6
>> PrevHash='C51E6DE'
PrevHash = C51E6DE

nonce = 100 000 001
nonce = 200 000 001
nonce = 300 000 001

>> sha256('RootHash PrevHash 737327631')
ans = F4AE534CD226FAF7998C8424B348E020BA80639A687E93A0B8C5130EDC51E6DE
>> sha256('RootHash PrevHash 737327632')
ans = B856211DF2EE15E30AB770C1A43CE014ECFE573182AFD885B28D96854DBC5F21
>> sha256('RootHash PrevHash 737327633')
ans = 9C18C764E347A58E57AC3F7A3C2874D5889A0E802699FEA47EEFF8C03BFEDA69
>> sha256('RootHash PrevHash 737327634')
ans = 32B2108A70C39565485CCED9C948E5B7A0027D1EE98642E09D5E4D3D84E16814
>> sha256('RootHash PrevHash 737327635')
ans = A281AC77F5C9AEDEEFFDEDEA85DCEA1C5D76E4222AB80D8A456AEB2AA9EB0F44
>> sha256('RootHash PrevHash 737327636')
ans = 1EE3D5FE00488A79EEFEBF5A88A3BF76D02EA8C2E53617B52D6CA6E57AE49FE1
>> sha256('RootHash PrevHash 737327637')
ans = D452B2E614C5F890ECAB2A7DB0EF6763A6874EDA0A69C45ACC7C66C35BDD8A46

```
>> sha256('RootHash PrevHash 737327638')
ans = 93625F9A6F66BCBA91AC39595E15885D359D0E12A3F98570251082ED1B483F8A
>> sha256('RootHash PrevHash 737327639')
ans = B45BA38E07CD2503CCA10C70E09212480C93EDD2C2087BA01EDEB9ADF77D415C
>> sha256('RootHash PrevHash 737327640')
ans = C41D1FB4B41F6427D3D33A7242FC0EF49E45D5888AA174B5255B8B4434CEEA4E
>> sha256('RootHash PrevHash 737327641')
ans = F163C4A8C3BCD99BB9C1B9DE0D3D22FAA00DBC54794A4C3292AC93E2E9C5C5DD
>> sha256('RootHash PrevHash 737327642')
ans = E1055CA9D8D248831CC5E8072E31CBAE2E501E8C95DDBD9D9656782786682763
.....
>> sha256('RootHash PrevHash 737327648')
ans = 01F9832B2431AFF9D2  219E446D613B8361B9903B4B02B8A63990C6B2209785A6
```

48
30
18 trials

$$Pr\,Mine = \frac{N.\ of\ all\ adequate\ values\ (NAV)}{N.\ of\ all\ possible\ values\ (NPV)}$$

64
− 18
46

Since number consisting of 64 hex digits consist of 256 bits

Then $NPV = 2^{256}$

Since number consisting of 63 hex digits consist of 252 bits

Then $NAV = 2^{252}$

$$Pr\,Mine = \frac{2^{252}}{2^{256}} = 2^{252-256} = 2^{-4} = \frac{1}{16}$$

Difficulty target : to mine a block it is needed to find a has consisting of 18 leading zeroes of hex digits.

Then NAV numb. consist of 46 hex digits consisting of 184 bits

$$Pr\,Mine = \frac{2^{184}}{2^{256}} = 2^{-72} = \frac{1}{2^{72}}$$

```
>> int64(2^72)
ans = 9 223 372 036 854 775 807
```