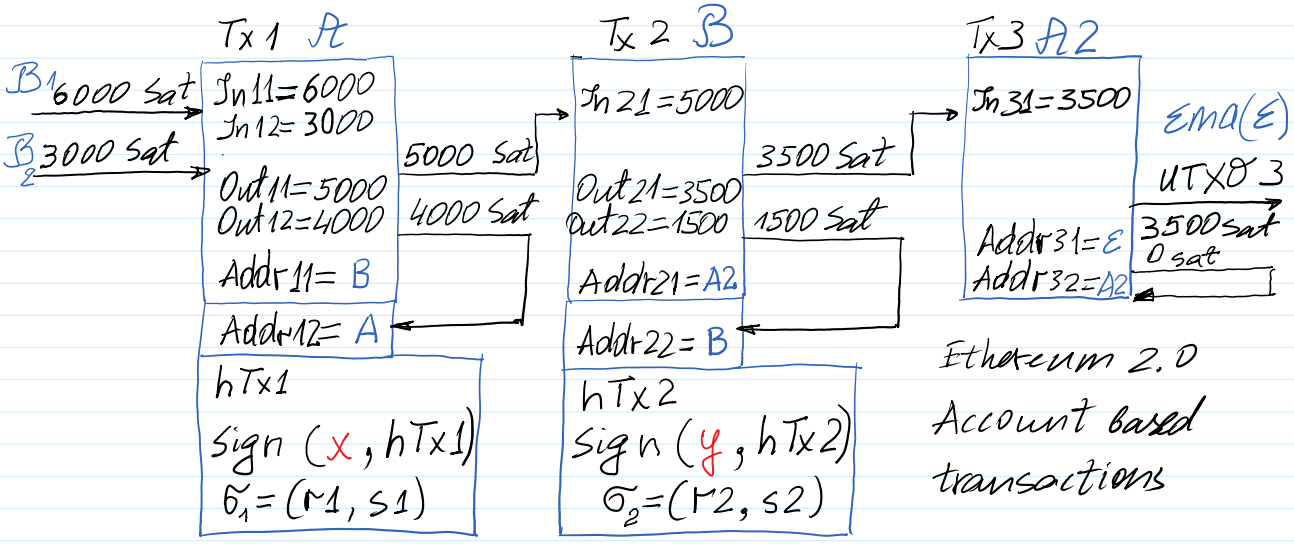
Egzaminas Pram. Pr. 20-237: Birželio 17 d. 10:50

Block structure - Unspent Transactio Output (UTxO) model



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

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

$Tx3 = '3 : In31 = 3500 || Out31 = 3500 || Out32 = 0 || Rec1 = E || Rec2 = A2'$

Transaction template:
Tx_N = 'Tx_N:In11=…||In12=…||Out11=…||Out12=…||Rec1=…||Rec2=…'

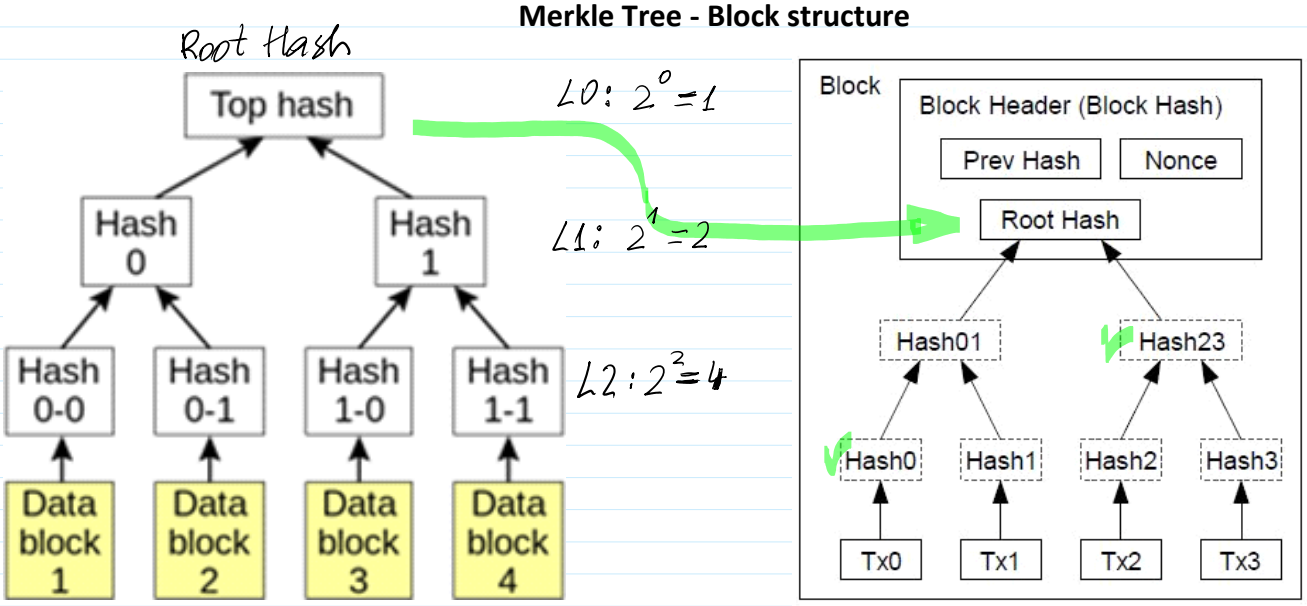
Transactions:
Tx_1 = 'Tx_1:In11=6000||In12=3000||Out11=5000||Out12=4000||Rec1=B||Rec2=A'
Tx_2='Tx_2:In21=5000||Out21=3500||Out22=1500||Rec1=A2||Rec2=B'
Tx_3='Tx_3:In31=3500||Out31=3500||Out32=0||Rec1=E||Rec2=A2'

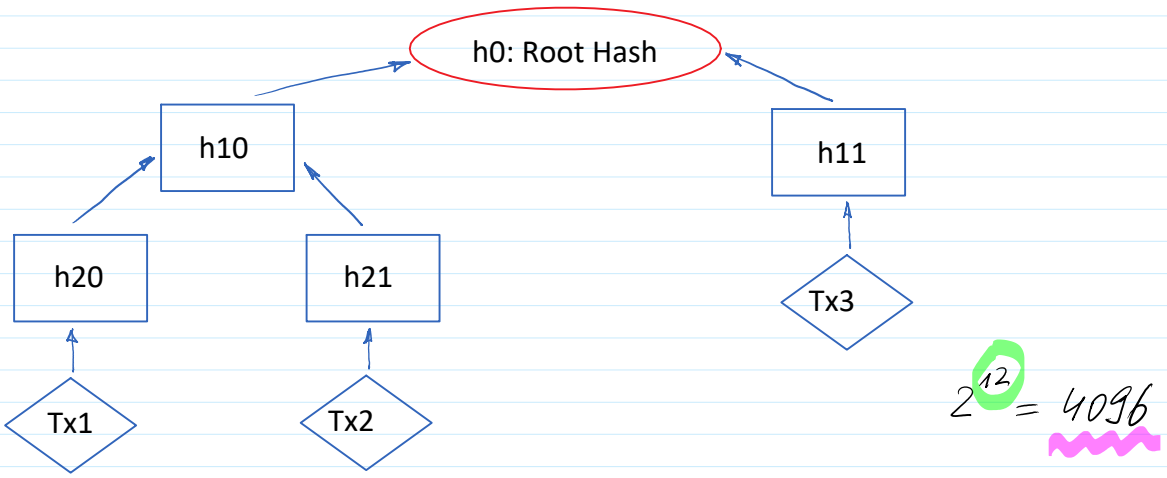
>> hTx_1=h28('Tx_1:In11=6000||In12=3000||Out11=5000||Out12=4000||Rec1=B||Rec2=A')
hTx_1 = 996BB7C
>> hTx_1=h28(Tx_1)
hTx_1 = 996BB7C

>> 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 - Block structure





>> h20=h28(hTx_1)
h20 = 996BB7C
>> h21=h28(hTx_2)
h21 = 977D75B
>> h11=h28(hTx_3)
h11 = 9201218

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

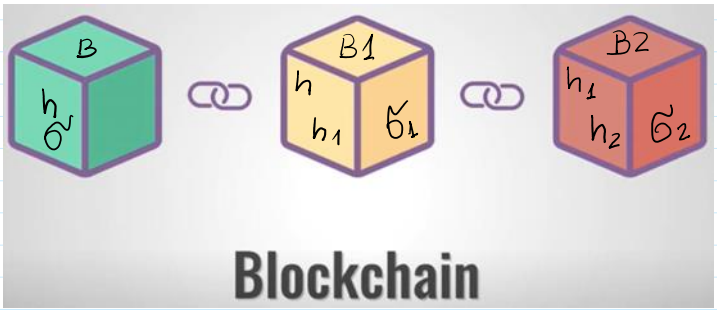
Root Hash: h0

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

Python : sha256

h20: 5B5412B
h21: D5C895A
h11: FEC59B7

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



Magic Number (4)	Block Size (4)
Version (4)	Previous Block Hash (32)
	sha 256 bits
	Merkle Root(32)
	Timestamp (4)
Difficulty Target (4)	Nonce (4)
Transaction Counter (Variable : 1-9)	
Transaction List (Variable : Upto 1 MB)	

BLOCK HEADER

Block size = 4 Bytes
4 Bytes × 8 bits = 32 bits
Block have
$2^{32} - 1$ = 4294967295
In ASCII encoding
8 bits represents
1 symbol a, b, c, ... #
Block represents
536 870 912 symbols

Difficulty Target (DT): defines the complexity of block mining. In our simulation DT we will choose to find h-value of mining (mined block) having only 1 leading hexadecimal digit equal to 0_h.

h28('RootHash PrevHash 73732763 1') =

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

DT: to mine a block it is needed to find h-value having leading zero in hexadecimal format: C51E6DE 0XXXXXX

6 × 4 = 24 bits

F
1111

h-value is computed sm >> h28( ) → 7 hex numbers

What probability to mine a block? Number of 4 bits has $2^4 = 16$ values

0000	0001	0010	0011	...	1001	1010	1011	1100	1101	1110	1111
0	1	2	3		9	10 A	11 B	12 C	13 D	14 E	15 F

The number of possible h-values of 28 bits: 2^{28} >> 2^28 ans = 268 435 456

The number of adequate h-values: 2^{24} >> int64(2^24) ans = 16777216

$$Pr\{toMine\} = \frac{2^{24}}{2^{28}} = \frac{1}{2^4} = \frac{1}{16}$$

DT: two leading hex number = 00 00XXXXX

$5 \times 4 = 20$

The number of adequate h-values: 2^{20}

$$Pr\{to\,Mine\} = \frac{2^{20}}{2^{28}} = \frac{1}{2^8} = \frac{1}{256}$$

DT: two leading hex number = 000 000XXXX

$4 \times 4 = 16$

$$Pr\{to\,Mine\} = \frac{2^{16}}{2^{28}} = \frac{1}{2^{12}} = \frac{1}{4096}$$ >> 2^12 ans = 4096

$$Pr\{to\,Mine\} = \frac{1}{2^{28}} = \frac{1}{268\,435\,456}$$ >> 2^28 ans = 268 435 456

The probability to mine a block, e.g. in Bitcoin when DT: is to find SHA256 value having 18 leading zeroes

$1\,Eth = 10^{18}\,Wei$

```
>> sha256('RootHash PrevHash 737327631')
ans = F4AE534CD226FAF799 8C8424B348E020BA80639A687E93A0B8C5130EDC51E6DE
      000000000000000000 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

The number of possible h-values having 256 bits is 2^{256}.

The numbe of adequate h-values of SHA 256 is

$256 - 18 \cdot 4 = 256 - 72 = 184$ bits, that are represented 46 hex. num.

The number of adequate values is 2^{184}.

$$Prob\{to\,mine\} = \frac{2^{184}}{2^{256}} = 2^{184-256} = 2^{-72}$$

$2^{72} \sim 4\,GT = 4 \cdot 2^{30} \cdot 2^{40} = 2^2 \cdot 2^{30} \cdot 2^{40} = 2^{72}$.

$1\,K = 2^{10} = 1024$

$1\,M = 2^{20} = \ldots$

$1\,G = 2^{30} = \ldots$

$2^{72} \sim 4\,GT = 4 \cdot 2^{30} \cdot 2^{40} = 2^2 \cdot 2^{30} \cdot 2^{40} = 2^{72}$

$1M = 2^{20} = \ldots$

$1G = 2^{30} = \ldots$

$1T = 2^{40} = \ldots$

N = 4 722 366 482 869 645 213 696

Number of trials $N = 1T \cdot 1G \cdot 2^2 = 4 \cdot 2^{40} \cdot 2^{30}$

Total net capacity $Cap \sim 2000$ Th/sek

$$Time\ T = \frac{N}{Cap} = \frac{4 \cdot 2^{40} \cdot 2^{30}}{2000 \cdot 2^{40}} \simeq \frac{4 \cdot 2^{30}}{2^{11}} = 4 \cdot 2^{19}\ s$$

```
>> T=int64(4*2^19)
T = 2097152
>> Tval=T/3600
Tval = 583
>> Tdien=Tval/24
Tdien = 24
```

Private blockchain ⟷ Public blockchain

Monero blockchain: Transactions sums → confidential → verifiable

Sender, Receiver } → anonymous

How to realize confidential & verifiable transactions.