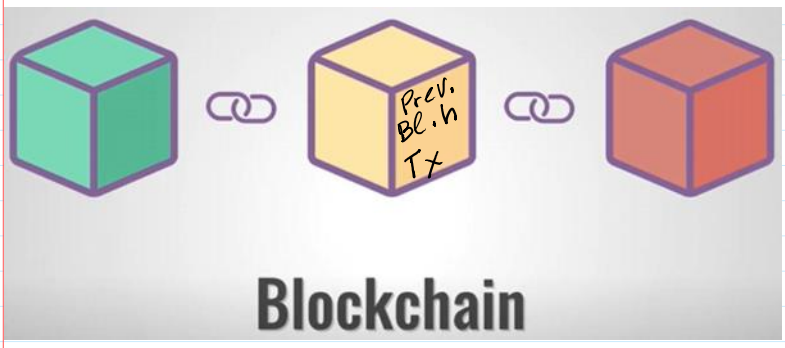
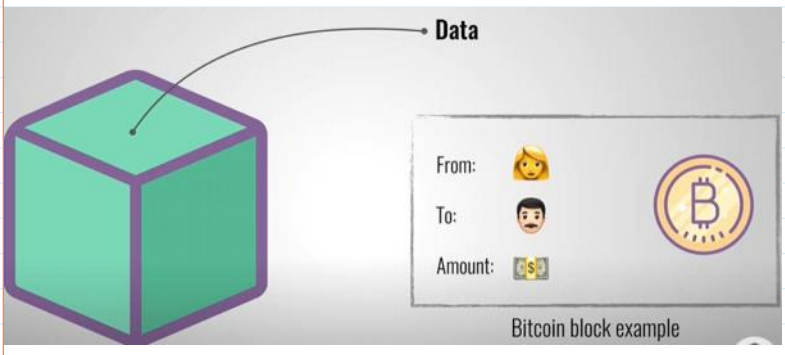


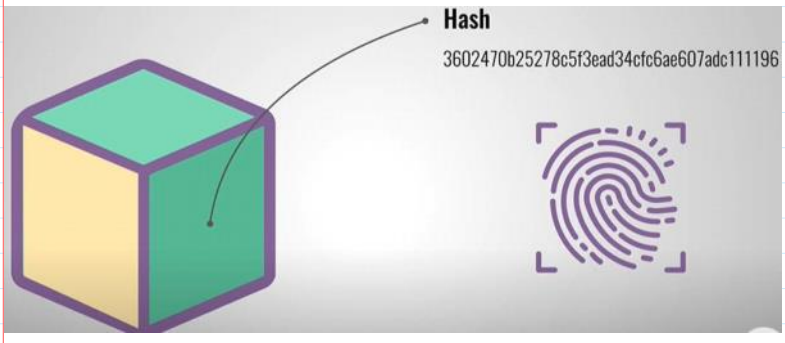
Last lecture on May 26 :
To present reports of course works

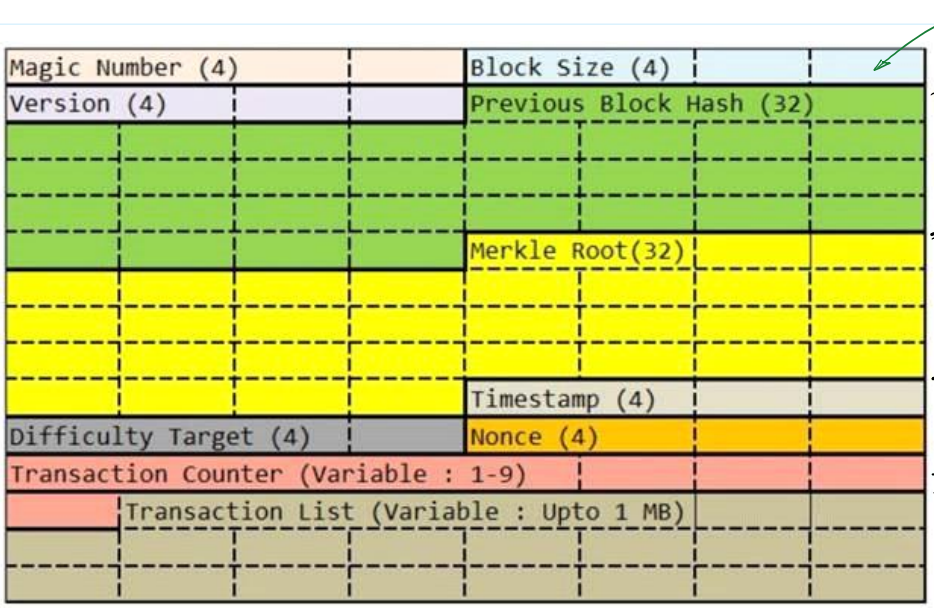
http://crypto.fmf.ktu.lt/xdownload/

- Example of CourseWork.7z



Proof of Work consensus princip.
↓
Block mining





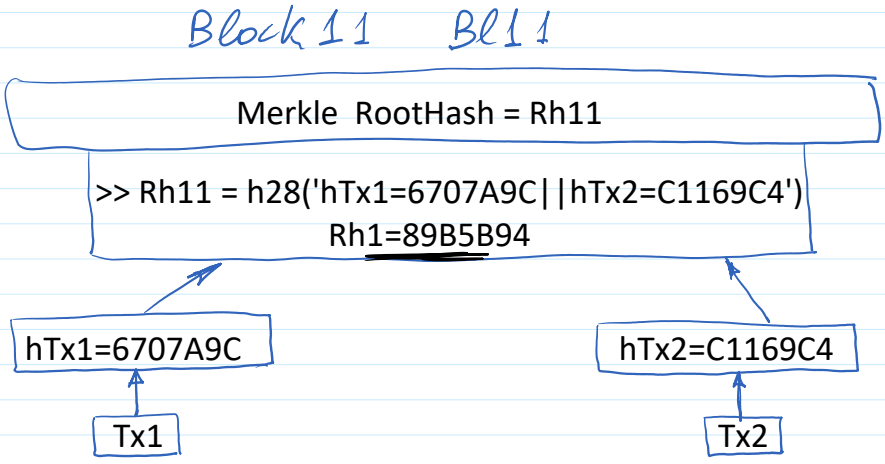
1 Byte

32 Bytes = 32 · 8 = 256 b
H-algor. SHA-256

h-value having
256 bit length

nonce = 1000
2000
3000

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



1. Difficulty Target DT: it is specified by the holder of cryptocurrency.
SHA-256 is used ⇒ 256 bits h-value of Bl11.
64 hexadecimal numbers.

In 2020 DT was determined as 18 leading zeroes in h-value of block to be mined

sha256

```
>> Bl11_00=sha256('Bl11:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=1000')
Bl11_00 = AAABD6D9FFB1DB2015C59106CE65B6E05C8ABE6D76BB661DAE1F737F6FF7B658
          000000000000000000HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
```

How many computations of h-values of block must be done to find h-value with 18 hexadecimal leading zeroes?
h-value of the block contains 256 bits;
the number of adequate h-values contains $256 - 18 \cdot 4 = 184$ bits.

$$Pr(\text{to mine a block}) = \frac{\text{adequate h-values}}{\text{total h-values}} = \frac{Ahv}{Thv}$$

$$\left.\begin{aligned} Ahv &= 2^{184} \\ Thv &= 2^{256} \end{aligned}\right\} \Rightarrow Pr = \frac{2^{184}}{2^{256}} = 2^{184-256} = 2^{-72} = \frac{1}{2^{72}}$$

$$2^{72} \sim 10^{21} = 1\,000\,000\,000\,000\,000\,000\,000$$

2. To mine a block miner must create a block by:

1.1. Including transactions into this block, say Bl11.

1.2. Composing Merkle Tree and computing Rh11.

1.3. Adding previous block h-value PrBlh.

1.4. To compute h-value of Bl11 by increasing nonce by 1 until h value hBl11 do not reach Difficulty Target DT.

Block11 PrBlh: PrBlh=0CAF06F

Rh: Rh=89B5B94

Tx1; hTx1=6707A9C

Tx2; hTx2=C1169C4

nonce: nonce=1000
nonce=2200
nonce=3050
.....

Bl11 = 'Bl11: PrBlh=... || Rh11=... || Tx1=... || Tx2=... || nonce=1000'

```
>> Bl11_00=h28('Bl11:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=1000')
Bl1_00 = D99C1E7

>> Bl11_18=h28('Bl11:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=2018')
Bl11_18 = 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
```

DT in our simulation with 28 bits of block's h-value

Then block's h-value contains 28 bits → 7 hexadecimal numbers

DT is one leading hexadecimal number in h-value.

Bl11_18 = **06B0772**

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:

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

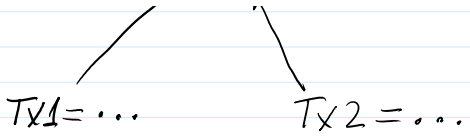
Exercises

PrBlh = 0CAF06F

EP Eimutis Papinigis	hTx1=6707A9D||hTx2=C1169C5||nonce=1000	Bl1	Rh1
GR Gvidas Rimeikis	hTx1=6707A9E||hTx2=C1169C6||nonce=2000	Bl2	Rh2
MM Malik Momodu	hTx1=6707A9F||hTx2=C1169C7||nonce=3000	Bl3	Rh3
NS Nedas Sirvidas	hTx1=6707A91||hTx2=C1169C8||nonce=4000	Bl4	Rh4
ZH zeid hamzeh	hTx1=7707A9D||hTx2=D1169C5||nonce=5000	Bl5	Rh5

Compute root h-values

RH1 = h28('hTx1=6707A9E||Tx2=C1169C6')



>> Rh1=**h28**('hTx1=6707A9D||hTx2=C1169C5')
Rh1 = 9F9E017

>> Bl11_00=**h28**('Bl11:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=1000')
Bl1_00 = D99C1E7

>> Bl5=h28('Bl11:PrBlh=0CAF06F||Rh=89B5B94||hTx1=6707A9C||hTx2=C1169C4||nonce=5000')

EP Eimutis Papinigis	Bl1=h28('Bl11:PrBlh=0CAF06F||Rh=9F9E017||hTx1=6707A9D||hTx2=C1169C5 ||NONCE=1009') Bl1 = **0F253CF**
GR Gvidas Rimeikis	Bl2=h28('Bl2:PrBlh=0CAF06F||Rh=F6211DD||hTx1=6707A9E||hTx2=C1169C6 ||NONCE=2012') Bl2 = **00082BC**
MM Malik Momodu	
NS Nedas Sirvidas	Bl4=h28('Bl11:PrBlh=0CAF06F||Rh=963762D||hTx1=6707A91||hTx2=C1169C8 ||nonce=4012') Bl4 = **069216F**
ZH zeid hamzeh	

Bl5=h28('hTx1=7707A9D||hTx2=D1169C5||NONCE=5040')
Bl5 = BF6777D
>> Bl5=h28('hTx1=7707A9D||hTx2=D1169C5||NONCE=5052')
Bl5 = 00493CB

>> Bl5=h28('Bl1:PrBlh=0CAF06F||Rh=33E139E||hTx1=6707A9E||hTx2=C1169C6||NONCE=5011')
Bl5 = **0890312** works for Zeid

The probability to mine a block with 3 leading hex numb.:

P=(3e2)=Adequate h-values = Ahv

$$Pr(3\,l.z.) = \frac{\text{Adequate h-values}}{\text{Total h-values}} = \frac{AhV}{ThV}$$

$ThV = 2^{28}$; $|AhV| = 28 - 3 \cdot 4 = 28 - 12 = 16$ bits.

$AhV = 2^{16}$

$$Pr(3\,l.z.) = \frac{2^{16}}{2^{28}} = 2^{16-28} = 2^{-12} = 1/2^{12}$$

$2^{12} = 4096$: $Pr = \frac{1}{4096}$

$$Pr(All\ z.) = \frac{1}{2^{28}} = 1/268\,435\,456$$

Mining Pools: DT → 3 leading zeroes (l.z.)

Eimutis	1 l.z.	←	128 points
Gvidas	3 l.z.	←	$4096 - 2 \cdot 128 = 3840$ point
Nedas	1 l.z.	←	128 points