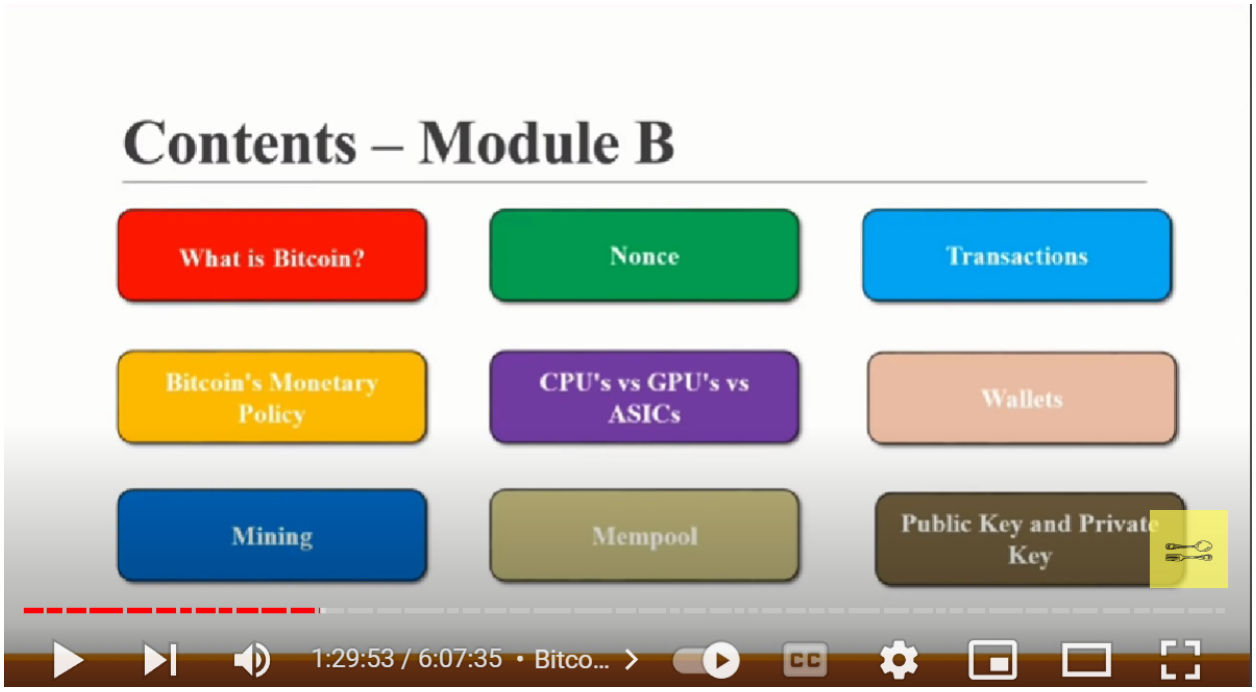
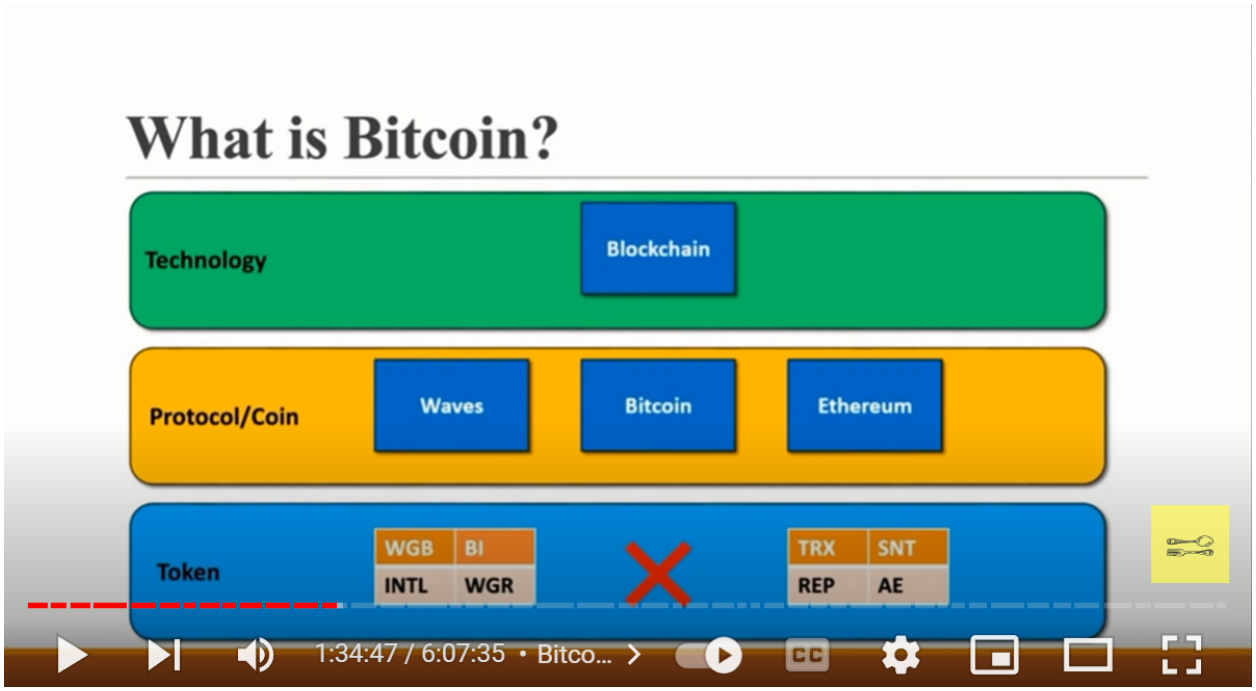
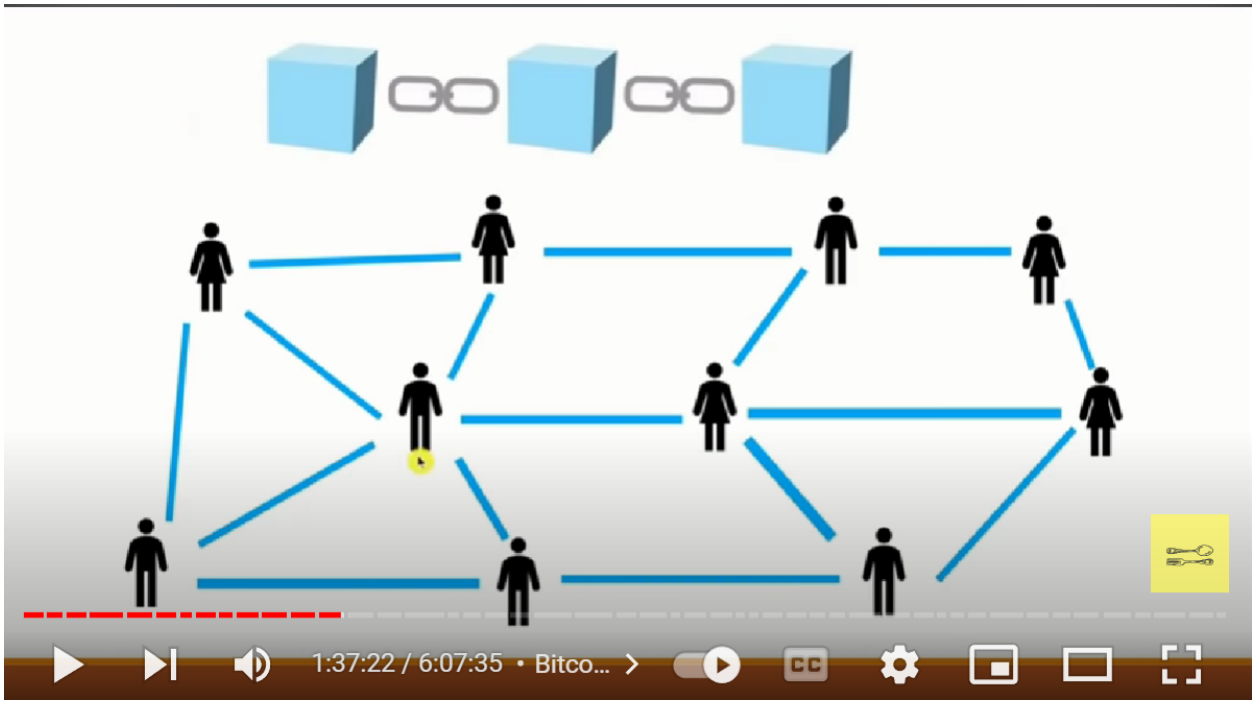
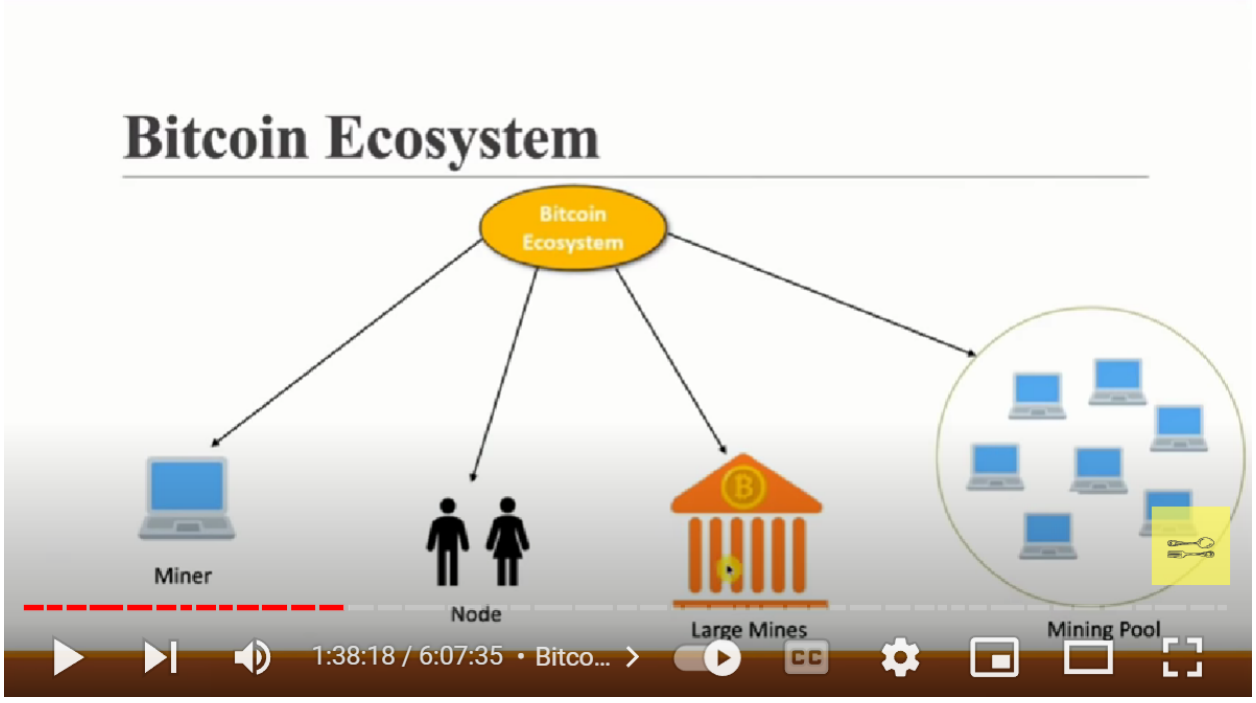
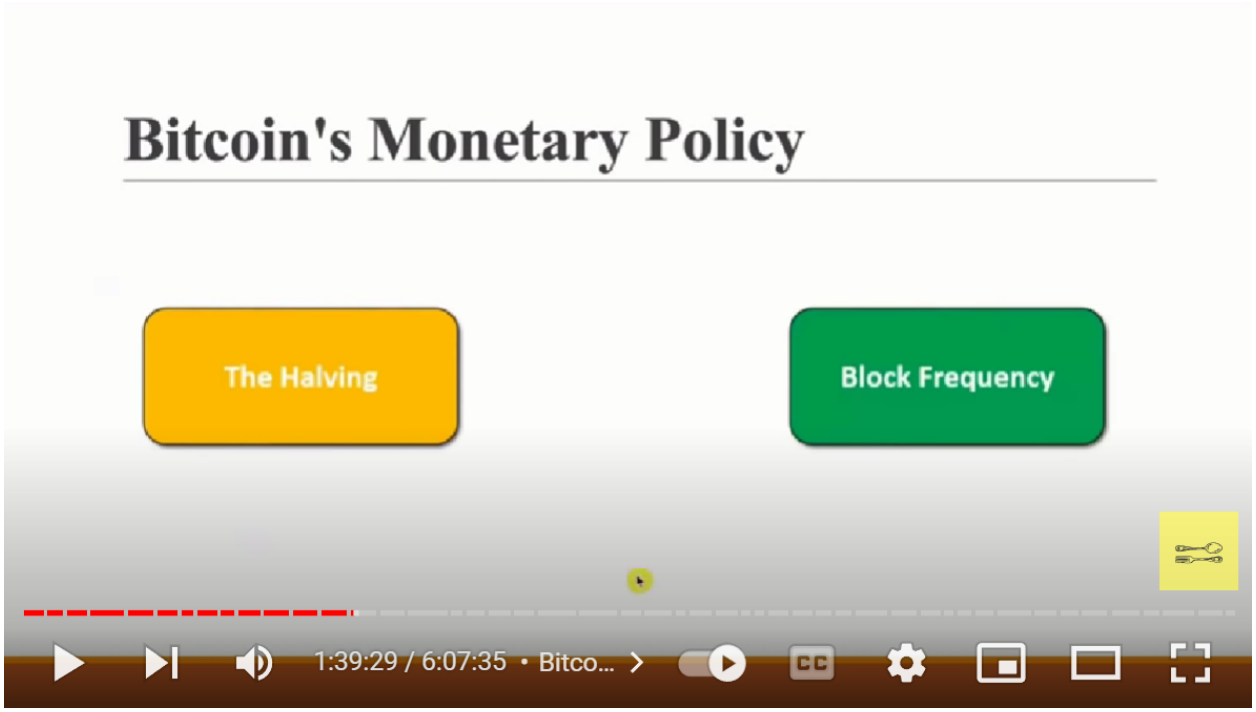
BLOCKCHAIN MODULE-B

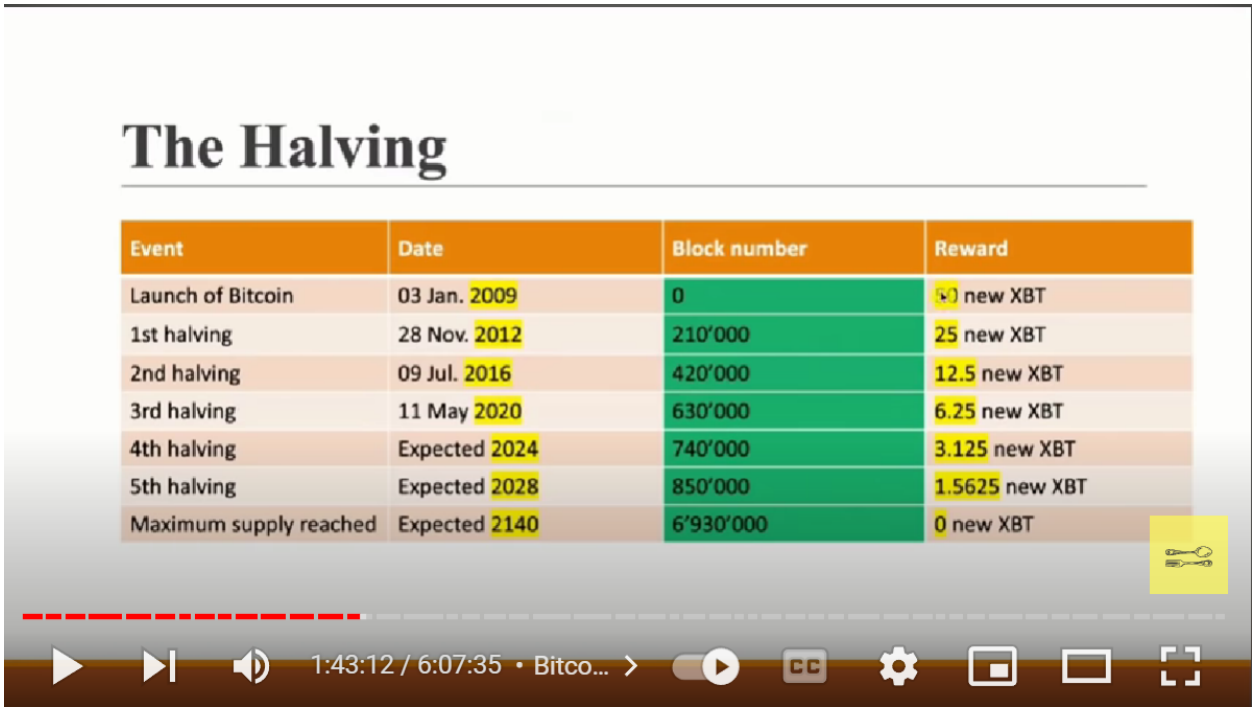


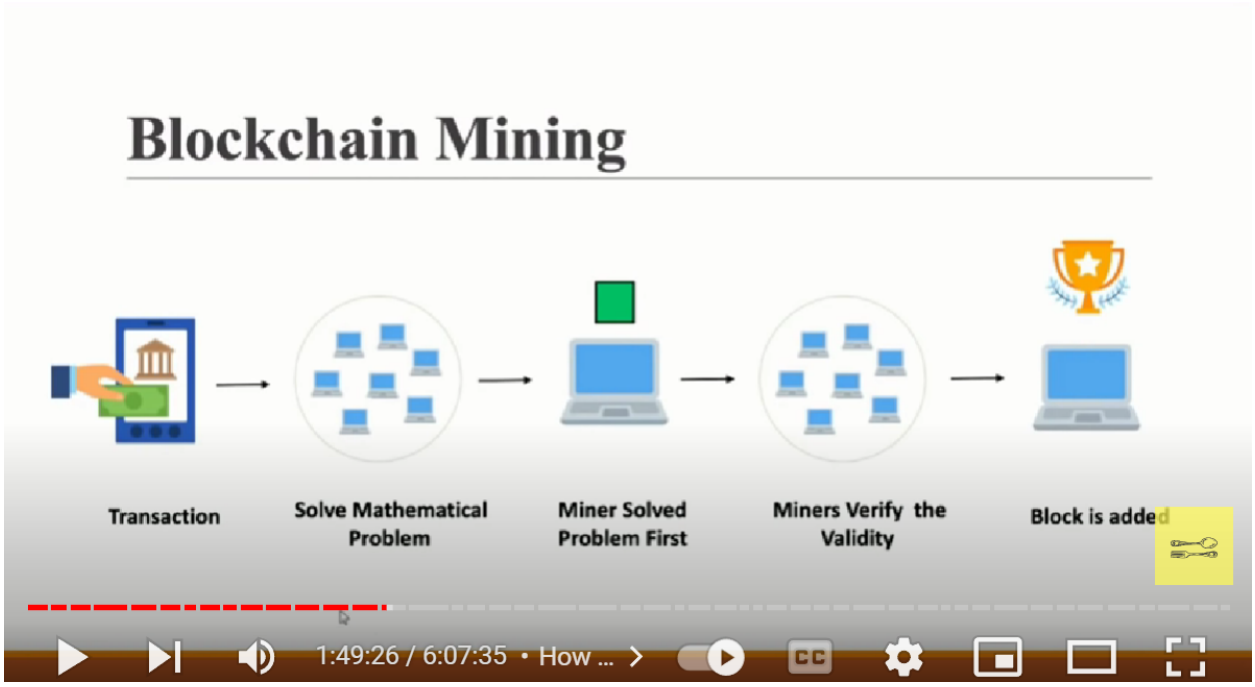


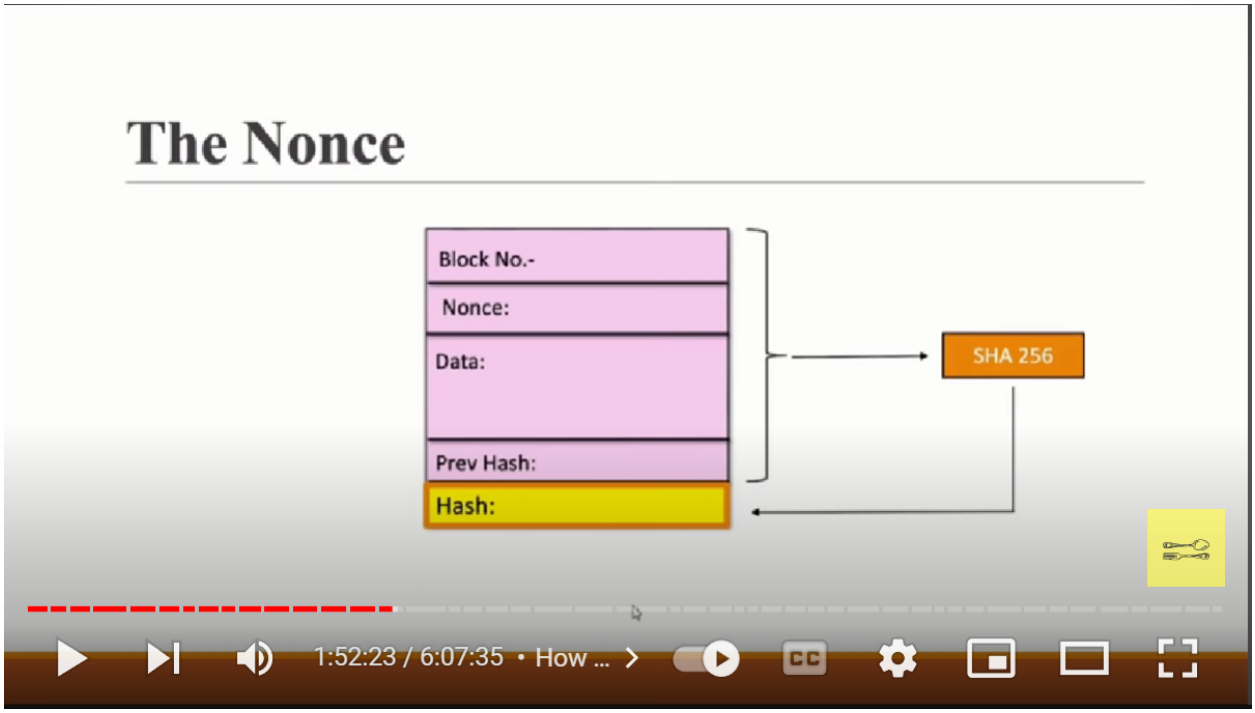

1:37:22 / 6:07:35 • Bitco...

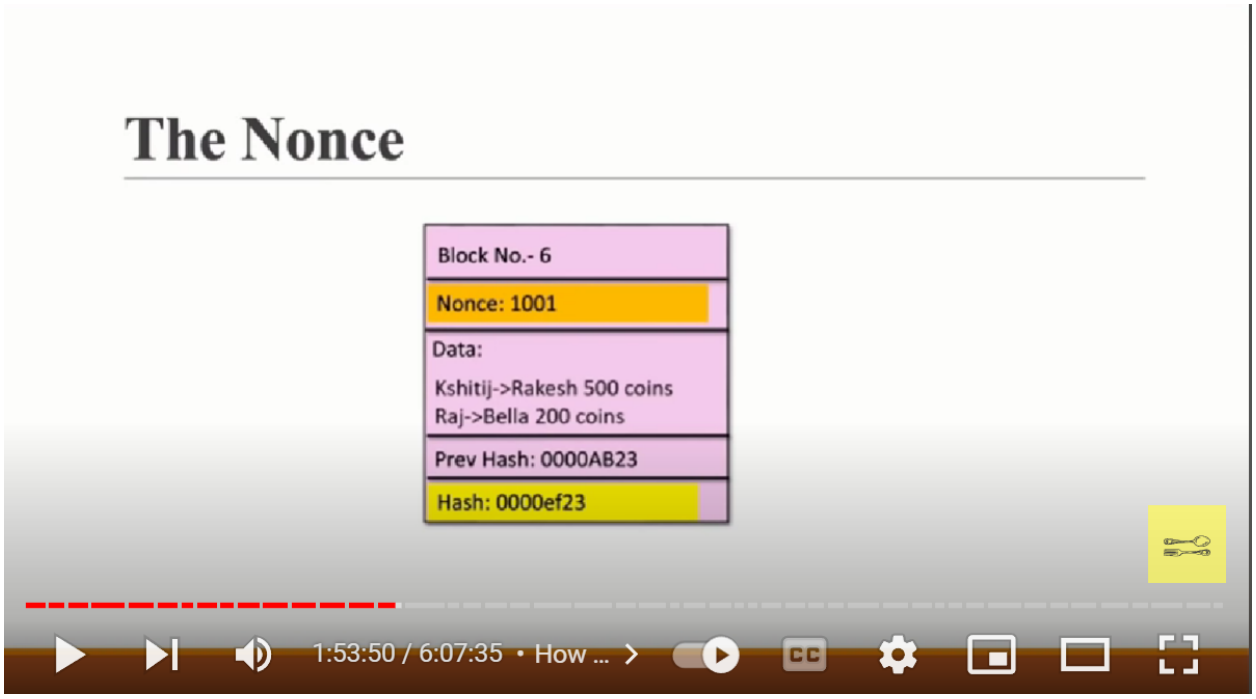

Bitcoin Ecosystem
Bitcoin Ecosystem
Miner
Node
Large Mines
Mining Pool
1:38:18 / 6:07:35 • Bitco...

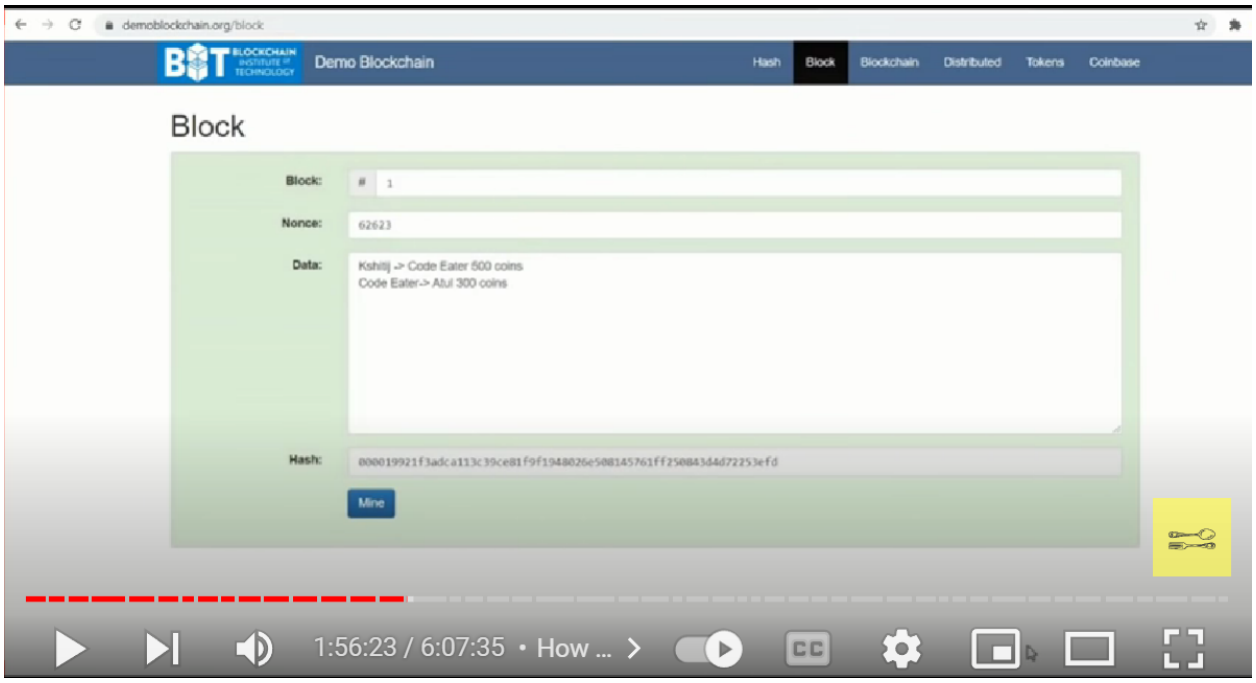

Bitcoin's Monetary Policy
The Halving
Block Frequency
1:39:29 / 6:07:35 • Bitco...

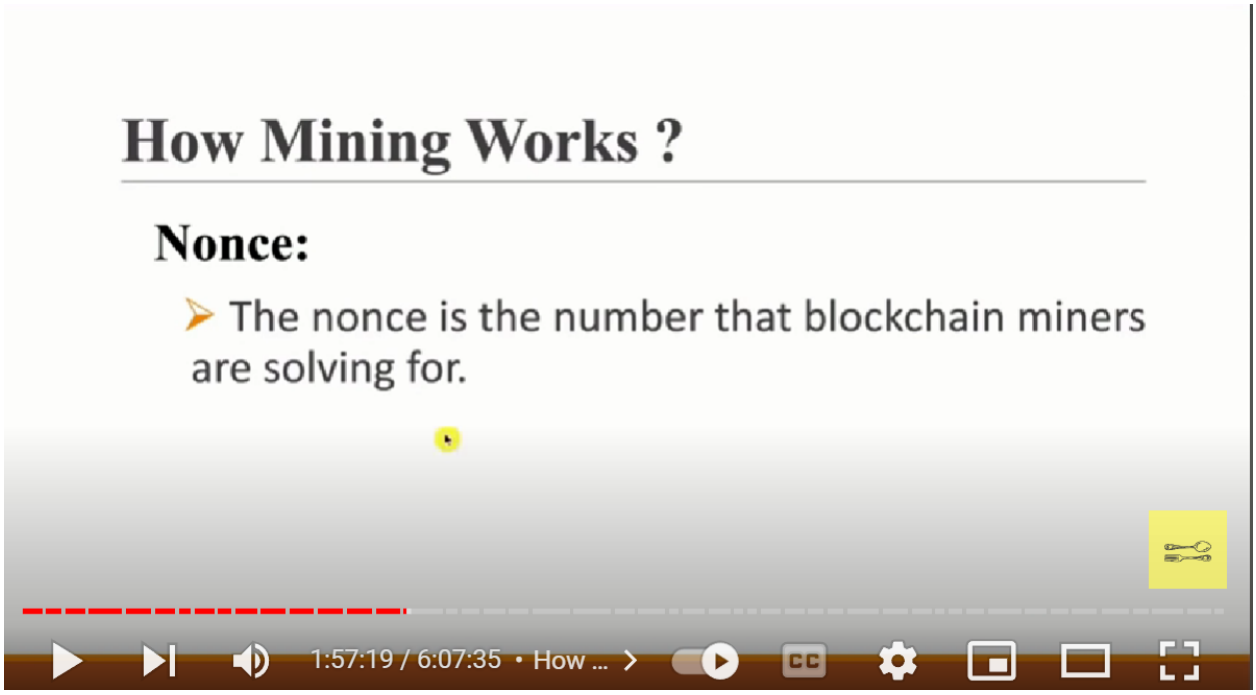

The Halving
Event
Date
Block number
Reward
Launch of Bitcoin
03 Jan. 2009
0
50 new XBT
1st halving
28 Nov. 2012
210'000
25 new XBT
2nd halving
09 Jul. 2016
420'000
12.5 new XBT
3rd halving
11 May 2020
630'000
6.25 new XBT
4th halving
Expected 2024
740'000
3.125 new XBT
5th halving
Expected 2028
850'000
1.5625 new XBT
Maximum supply reached
Expected 2140
6'930'000
0 new XBT
1:43:12 / 6:07:35 • Bitco...

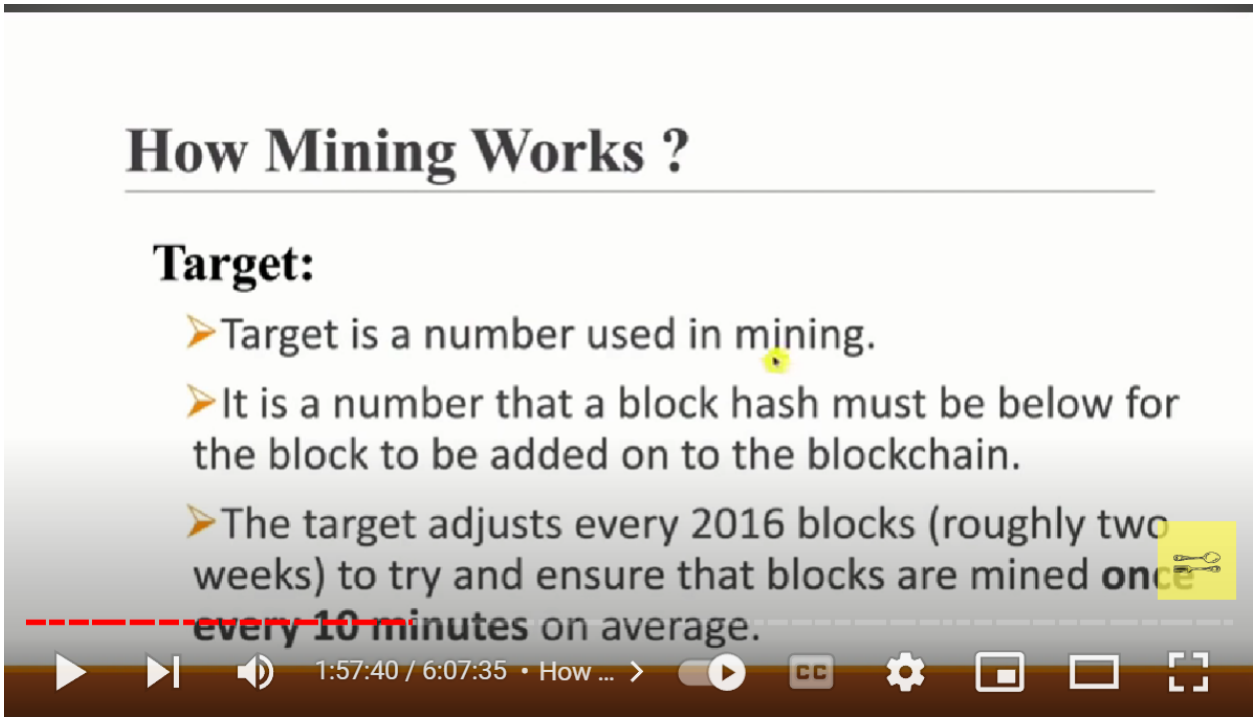

Blockchain Mining
Transaction
Solve Mathematical Problem
Miner Solved Problem First
Miners Verify the Validity
Block is added
1:49:26 / 6:07:35 • How ...


The Nonce
Block No.-
Nonce:
Data:
Prev Hash:
Hash:
SHA 256
1:52:23 / 6:07:35 • How ...

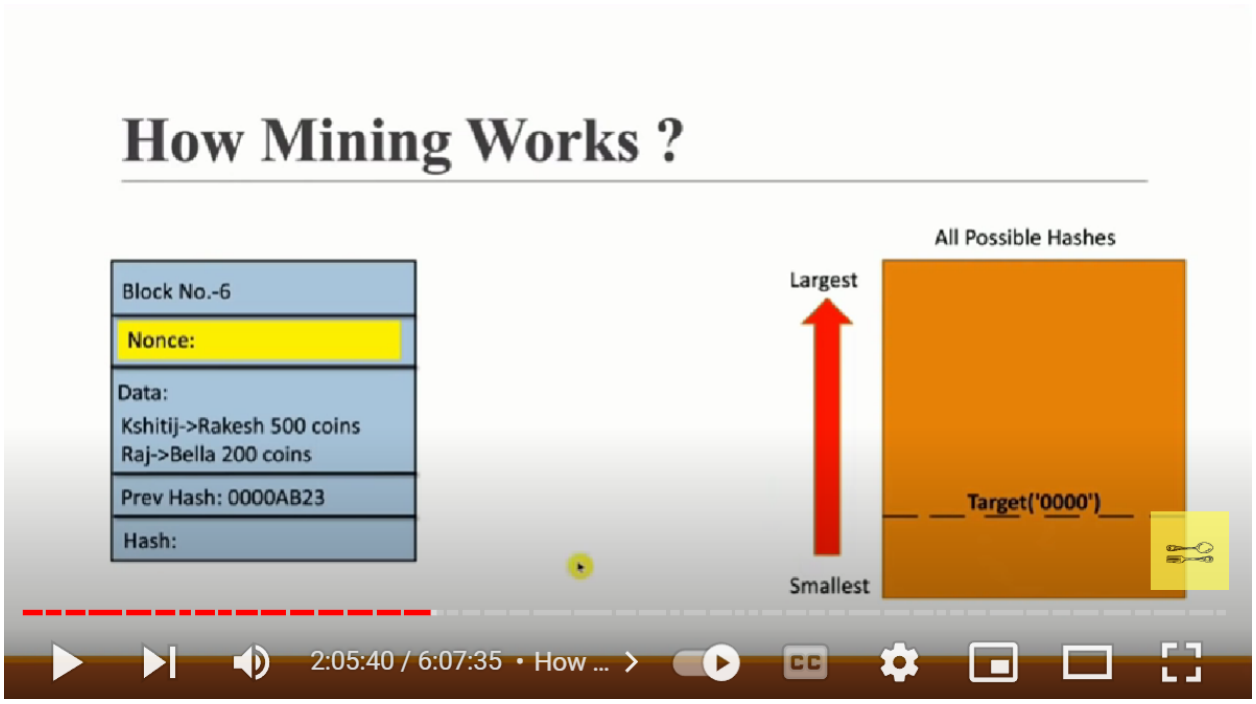

The Nonce
Block No.- 6
Nonce: 1001
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000ef23
1:53:50 / 6:07:35 • How ...

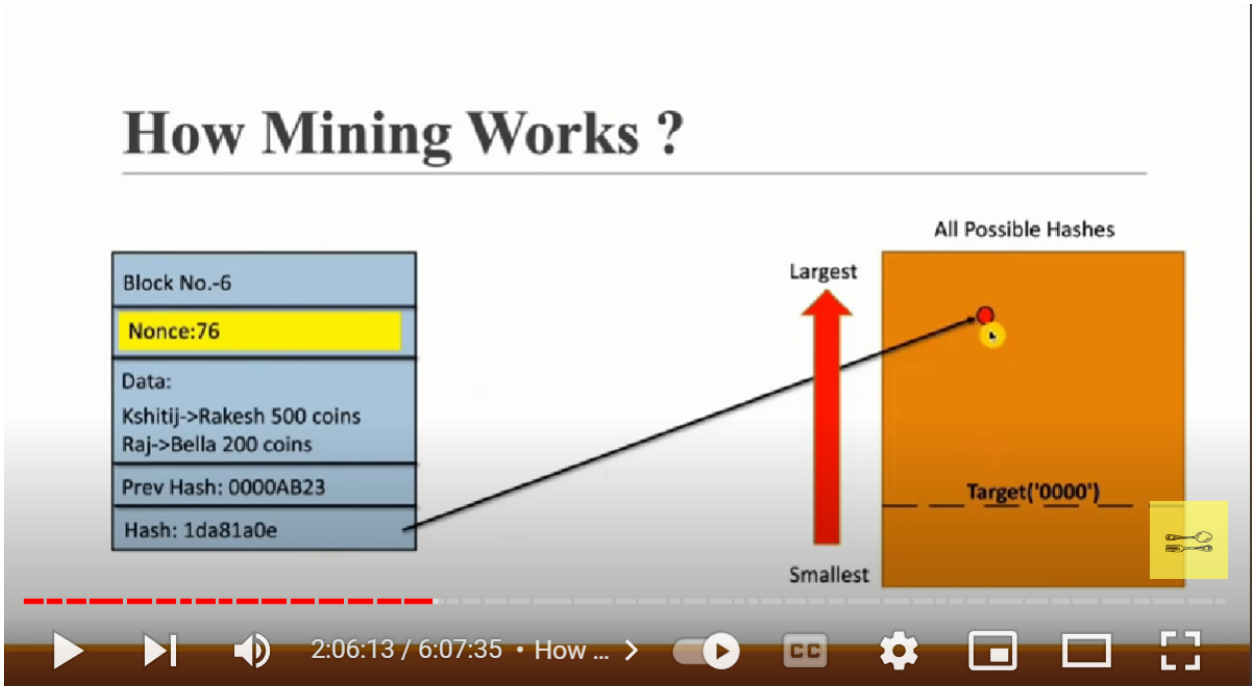

demoblockchain.org/block
Demo Blockchain
Hash
Block
Blockchain
Distributed
Tokens
Coinbase
Block
Block:
Nonce:
62623
Data:
Kshitij -> Code Eater 500 coins
Code Eater-> Atul 300 coins
Hash:
Mine
1:56:23 / 6:07:35 • How ...

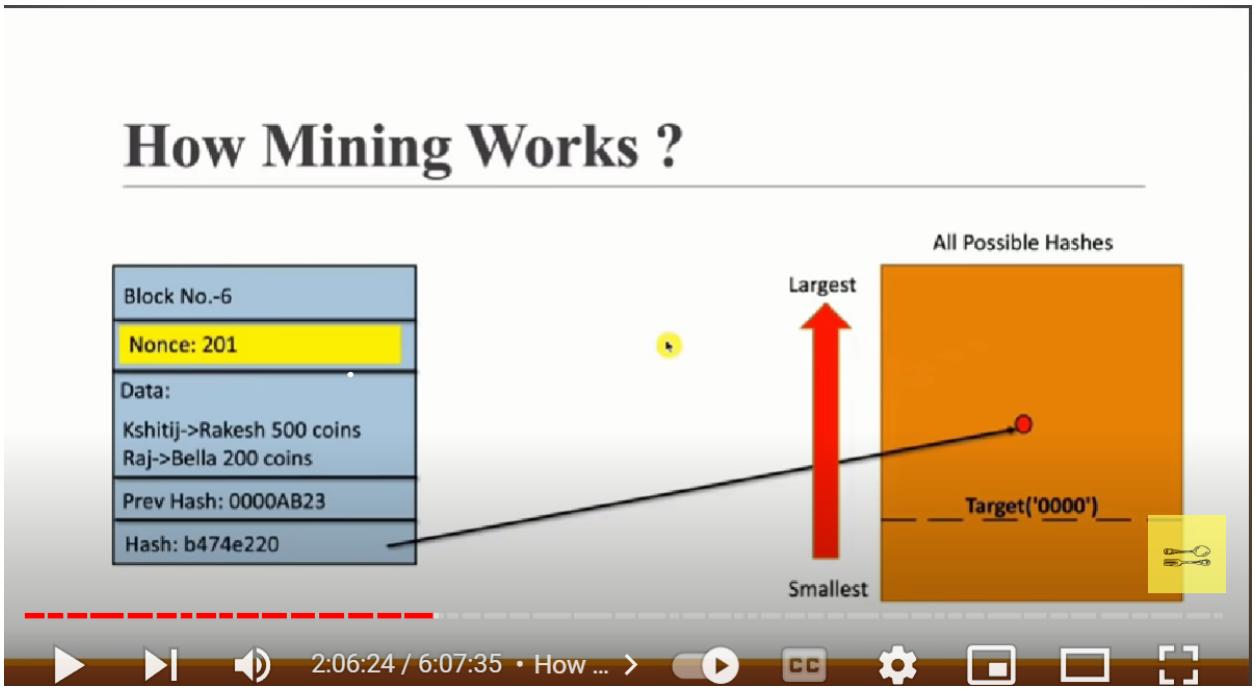

How Mining Works ?
Nonce:
The nonce is the number that blockchain miners are solving for.
1:57:19 / 6:07:35 • How ...

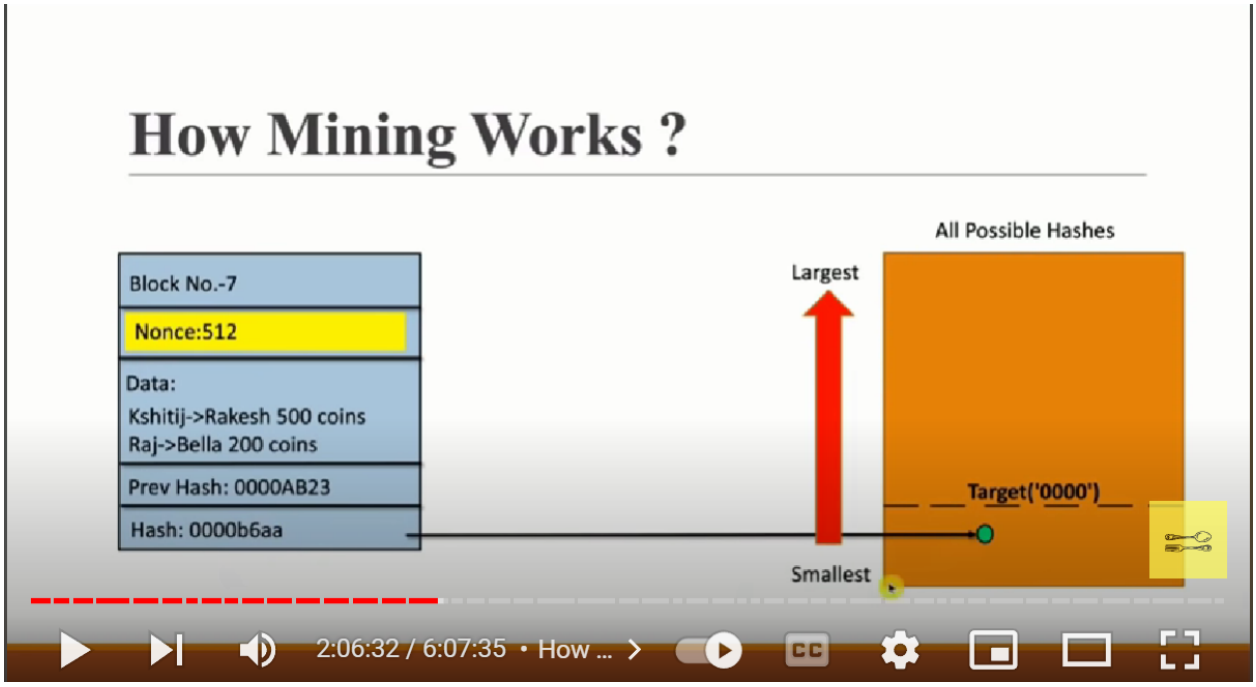

How Mining Works ?
Target:
Target is a number used in mining.
It is a number that a block hash must be below for the block to be added on to the blockchain.
The target adjusts every 2016 blocks (roughly two weeks) to try and ensure that blocks are mined once every 10 minutes on average.
1:57:40 / 6:07:35 • How ...

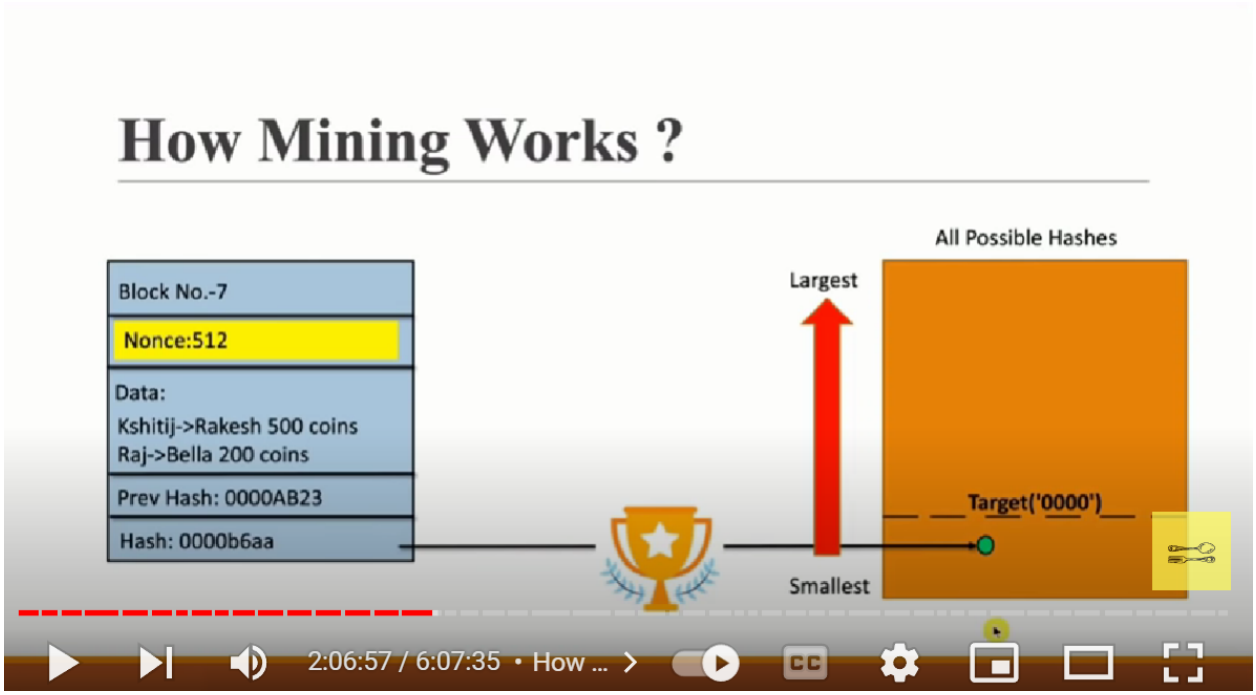

How Mining Works ?
d2fd3930d274b202fe8e7cb431e38a8b64ec396e15f5717e60493234b0de210a
52d095795c1dc87ff2f6b4d9b005a1fe2cfed01103763c9443f6d4496df8e800
0000005432d9f64f6e05c019f9302162100163b6cdba06bd72eee35cd19aebf
Smallest- 0000000.....0
Largest- fffffffffffff.....f
2:02:34 / 6:07:35 • How ...

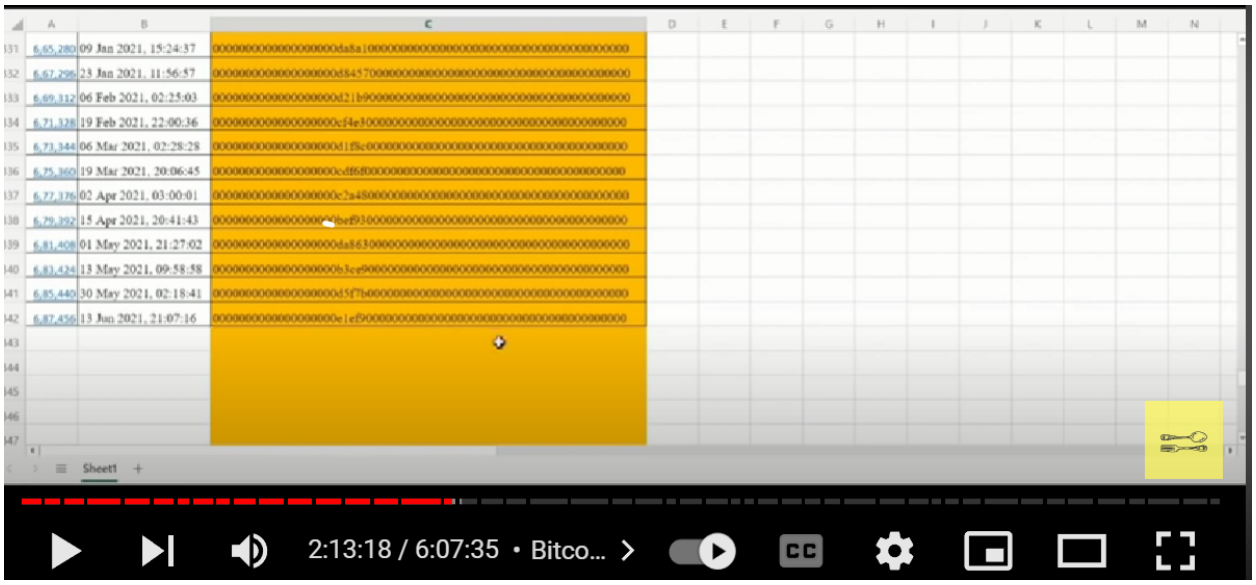

How Mining Works ?
Block No.-6
Nonce:
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash:
All Possible Hashes
Largest
Smallest
Target('0000')
2:05:40 / 6:07:35 • How ...

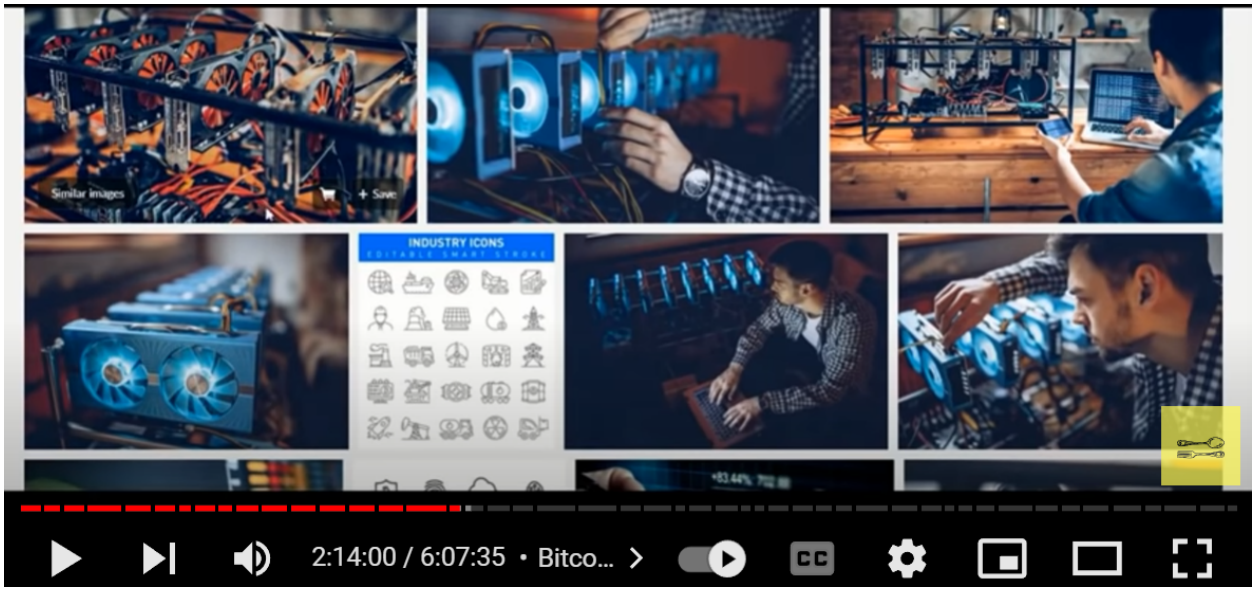

How Mining Works ?
All Possible Hashes
Block No.-6
Nonce:76
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 1da81a0e
Largest
Smallest
Target('0000')
2:06:13 / 6:07:35 • How ...

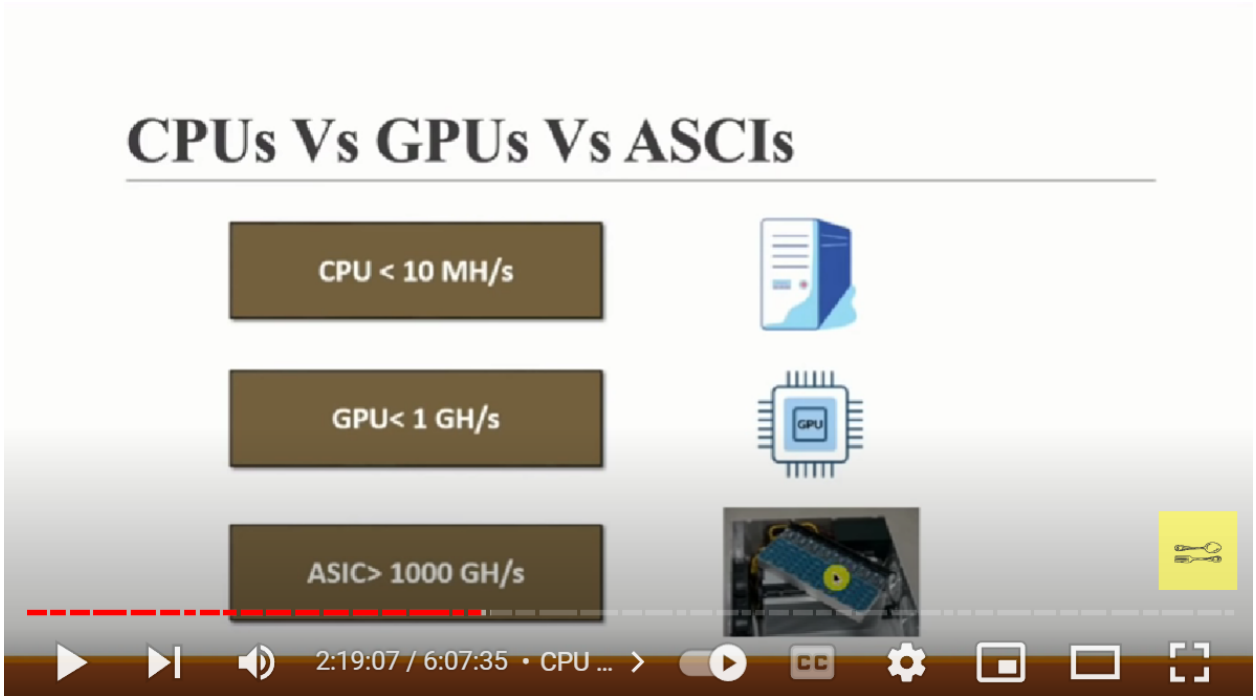

How Mining Works ?
All Possible Hashes
Block No.-6
Nonce: 201
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: b474e220
Largest
Smallest
Target('0000')
2:06:24 / 6:07:35 • How ...

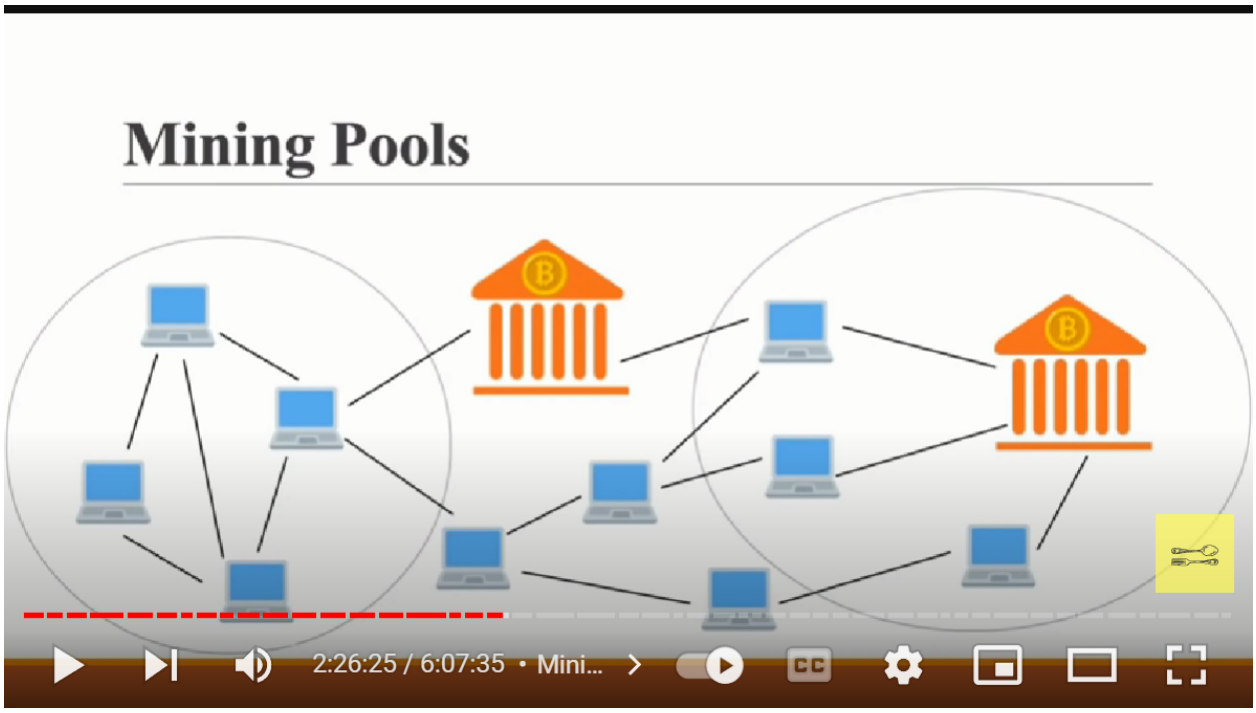

How Mining Works ?
All Possible Hashes
Block No.-7
Nonce:512
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000b6aa
Largest
Target('0000')
Smallest
2:06:32 / 6:07:35 • How ...

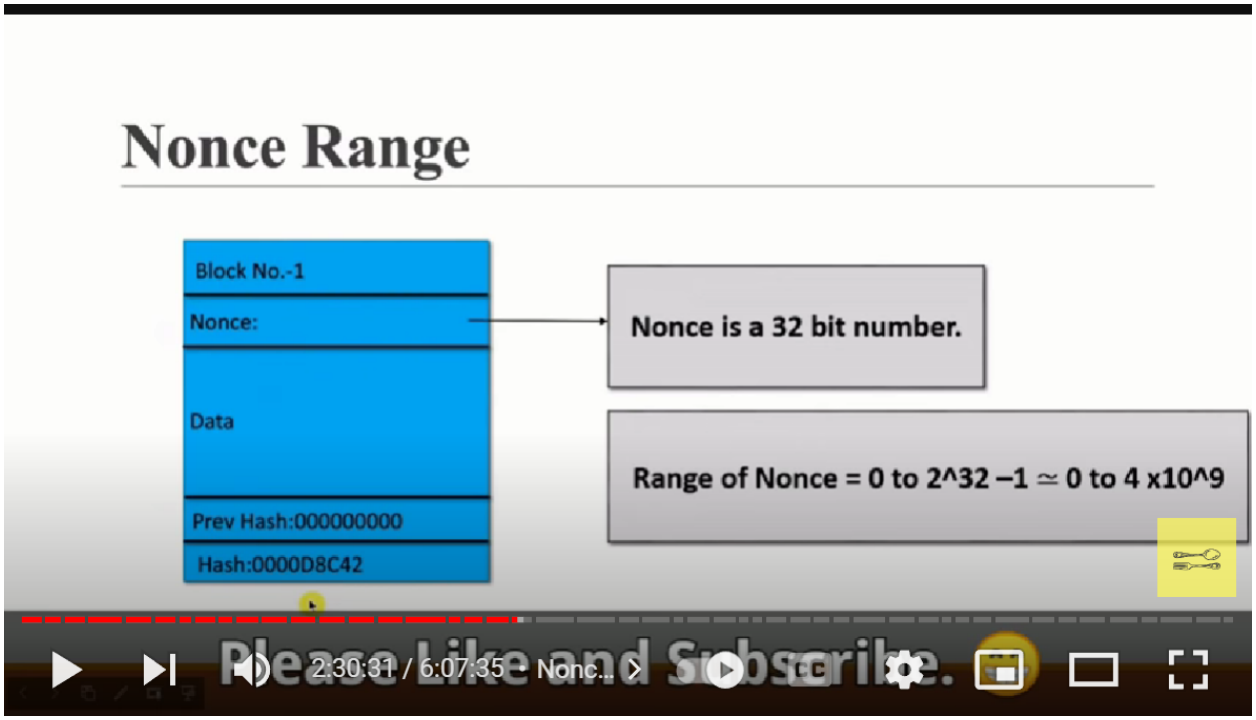

How Mining Works ?
All Possible Hashes
Block No.-7
Nonce:512
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000b6aa
Largest
Target('0000')
Smallest
2:06:57 / 6:07:35 • How ...

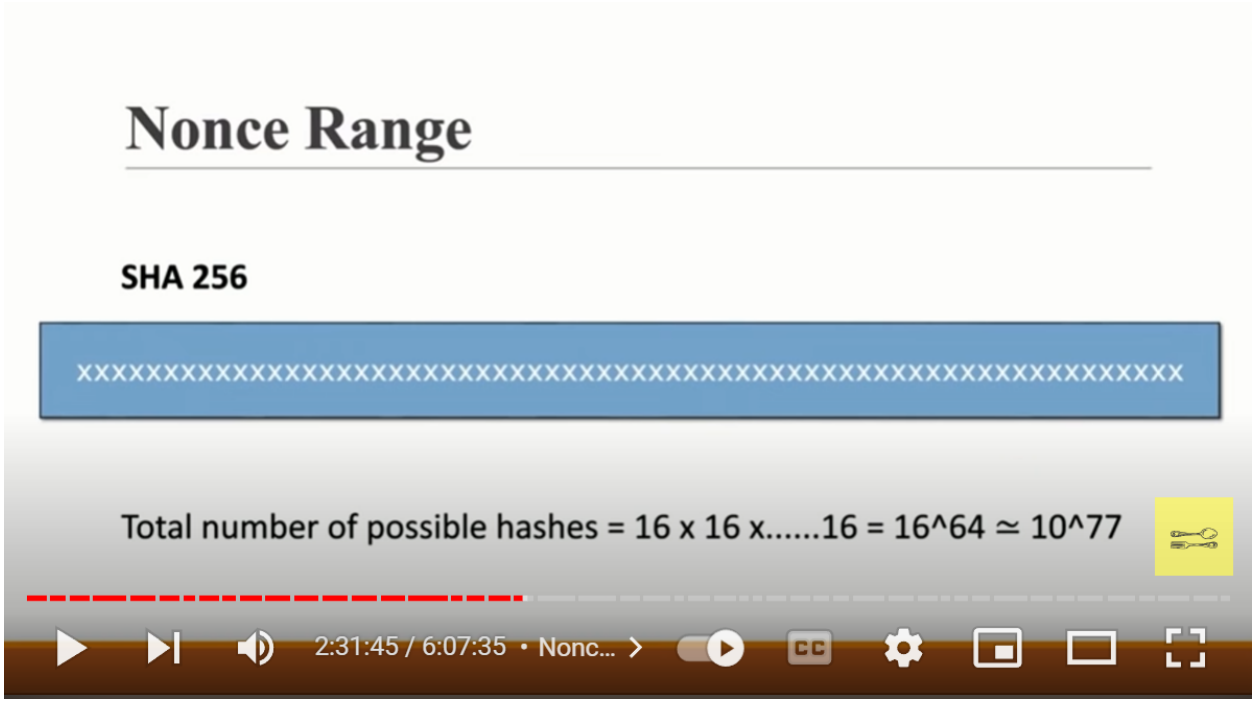

Sheet1
2:13:18 / 6:07:35 • Bitco...


Similar images
+ Save
INDUSTRY ICONS
2:14:00 / 6:07:35 • Bitco...


CPUs Vs GPUs Vs ASCIs
CPU < 10 MH/s
GPU< 1 GH/s
ASIC> 1000 GH/s
GPU
2:19:07 / 6:07:35 • CPU ...


Mining Pools
2:26:25 / 6:07:35 • Mini...


Nonce Range
Block No.-1
Nonce:
Data
Prev Hash:000000000
Hash:0000D8C42
Nonce is a 32 bit number.
Range of Nonce = 0 to 2^32 –1 ≃ 0 to 4 x10^9
2:30:31 / 6:07:35 • Nonc...
Please Like and Subscribe.


Nonce Range
SHA 256
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Total number of possible hashes = 16 x 16 x.....16 = 16^64 ≃ 10^77
2:31:45 / 6:07:35 • Nonc...

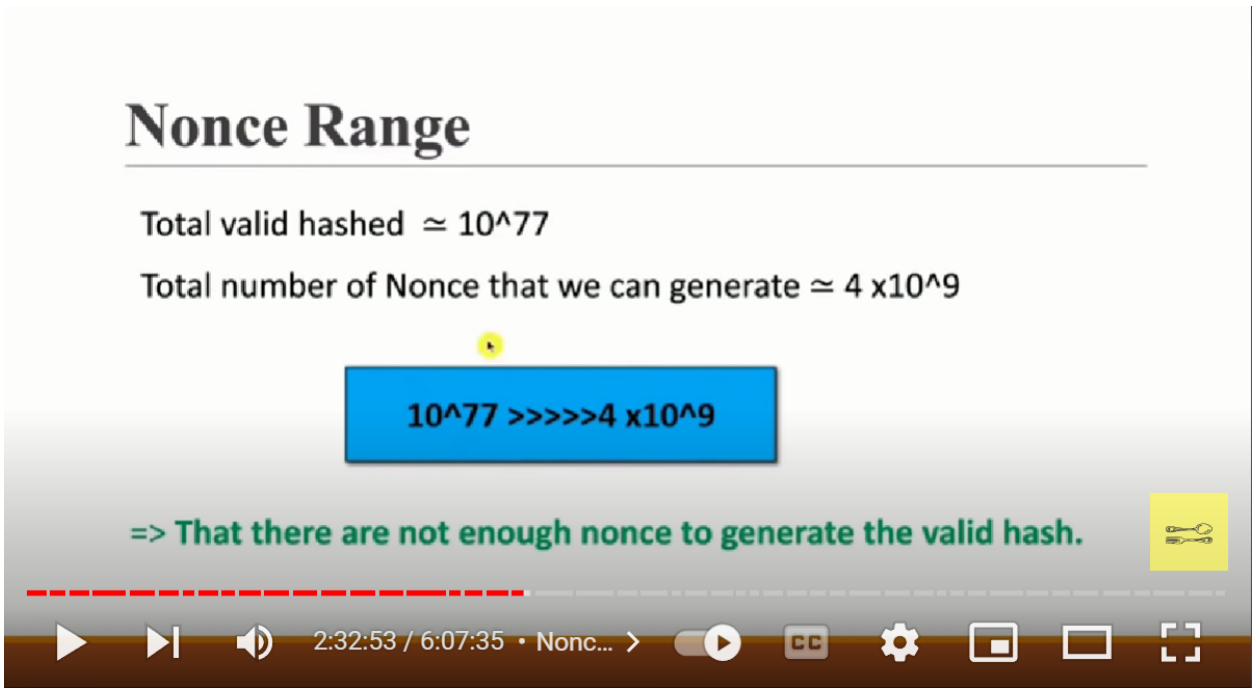
Nonce Range

Total valid hashed ≃ 10^77

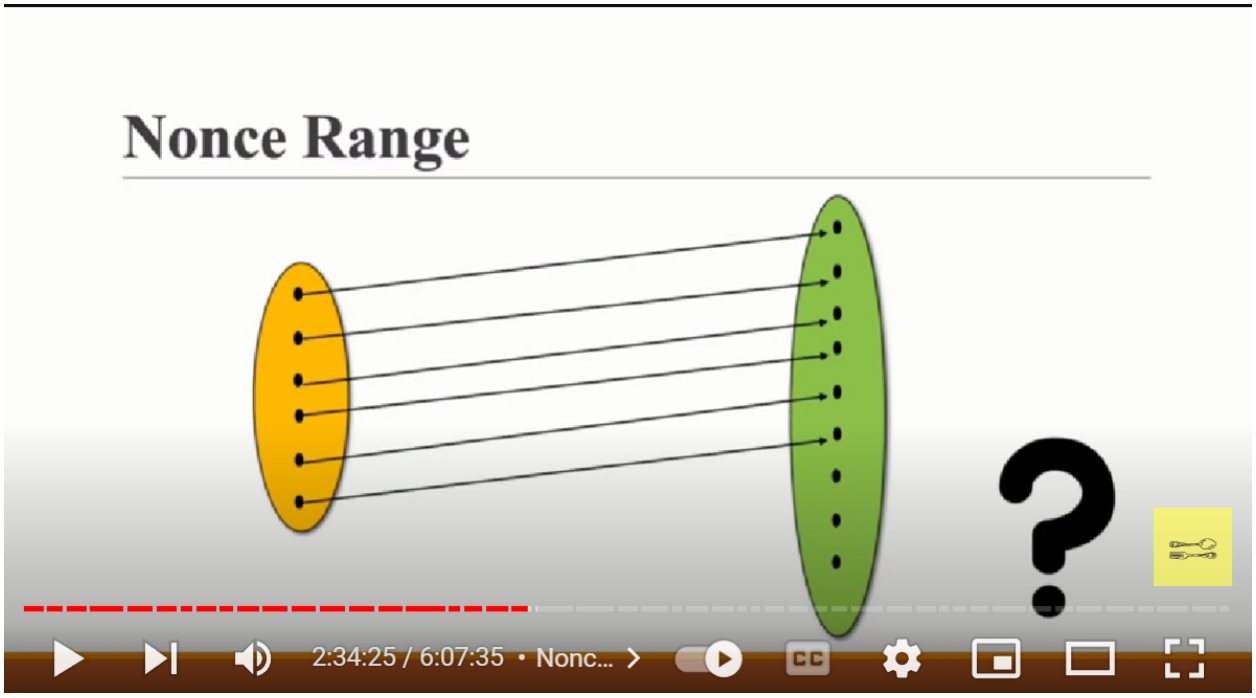
Total number of Nonce that we can generate ≃ 4 x10^9

10^77 >>>>>4 x10^9

=> That there are not enough nonce to generate the valid hash.



Nonce Range

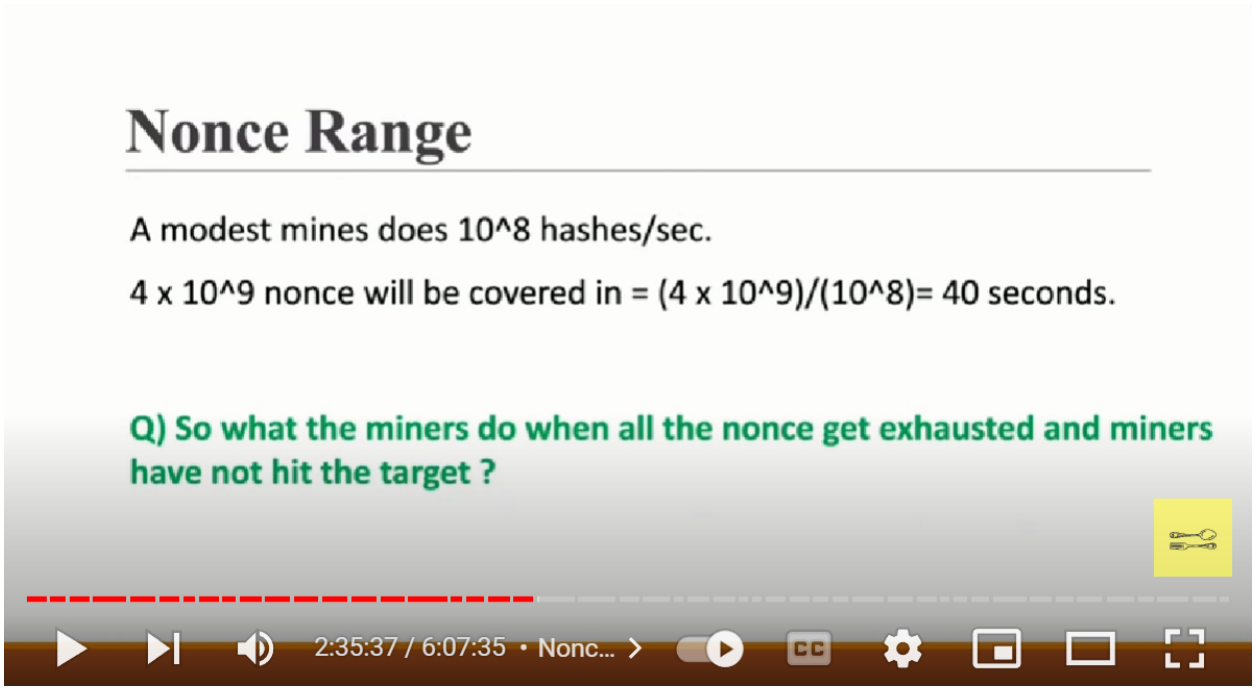


Nonce Range

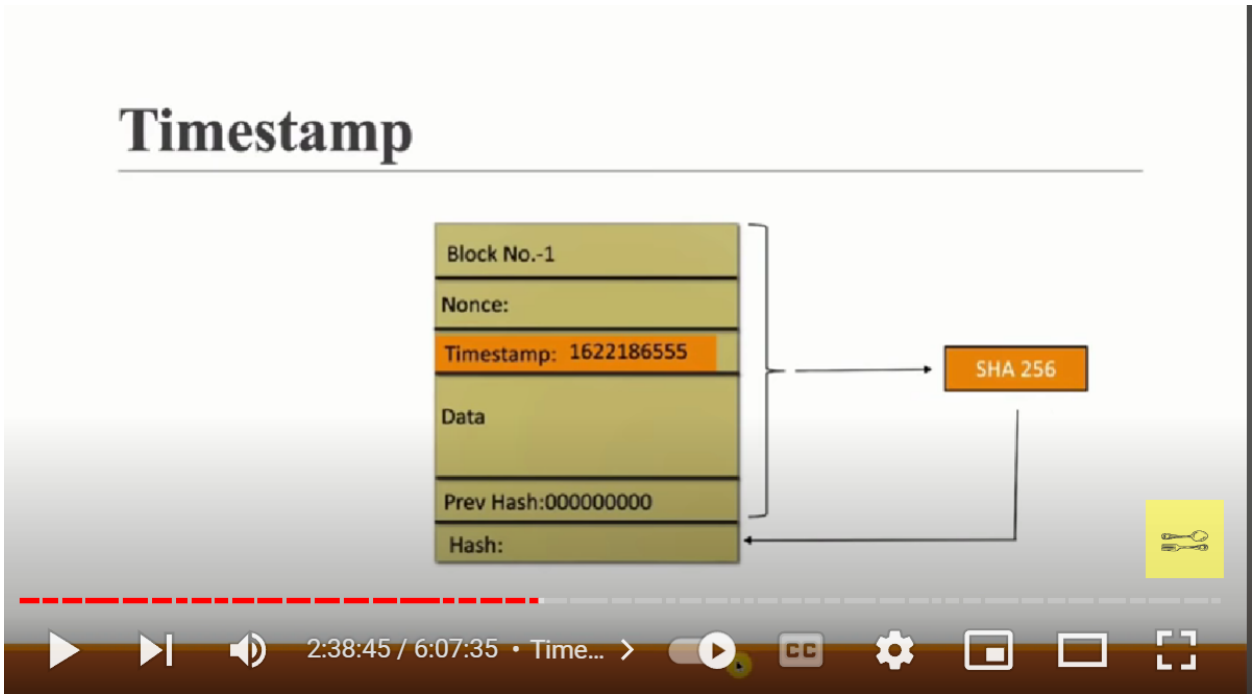
A modest mines does 10^8 hashes/sec.

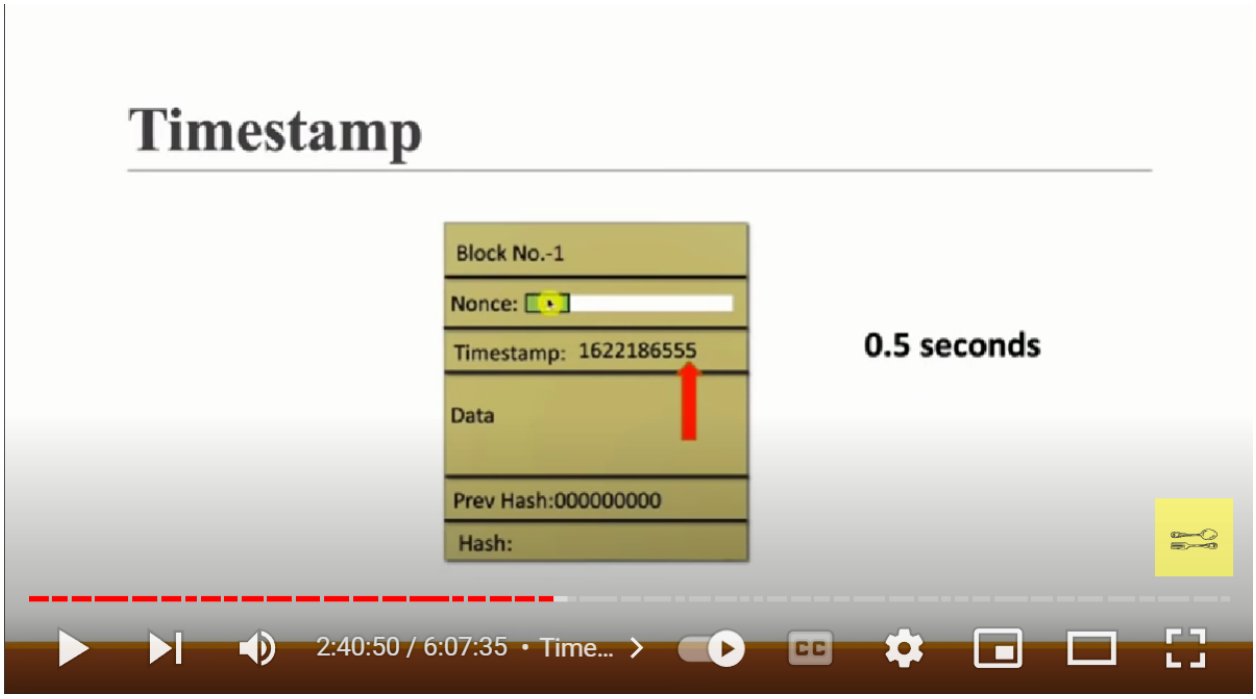
4 x 10^9 nonce will be covered in = (4 x 10^9)/(10^8)= 40 seconds.

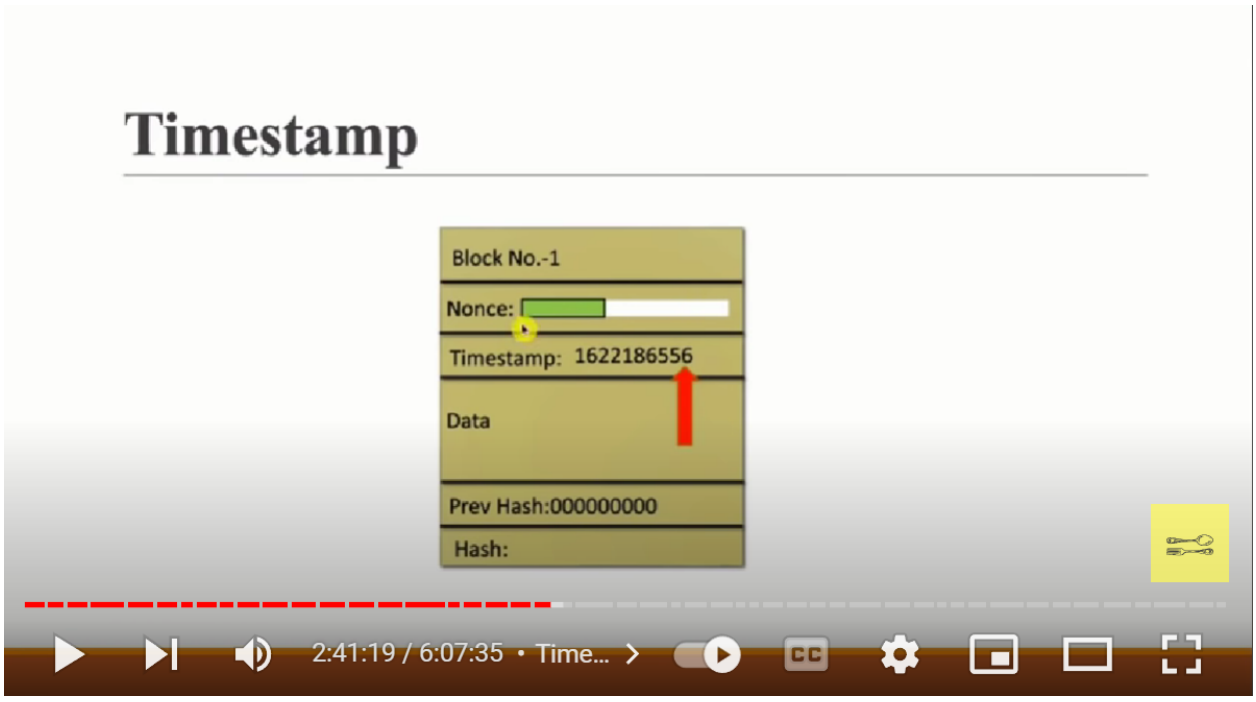
Q) So what the miners do when all the nonce get exhausted and miners have not hit the target ?

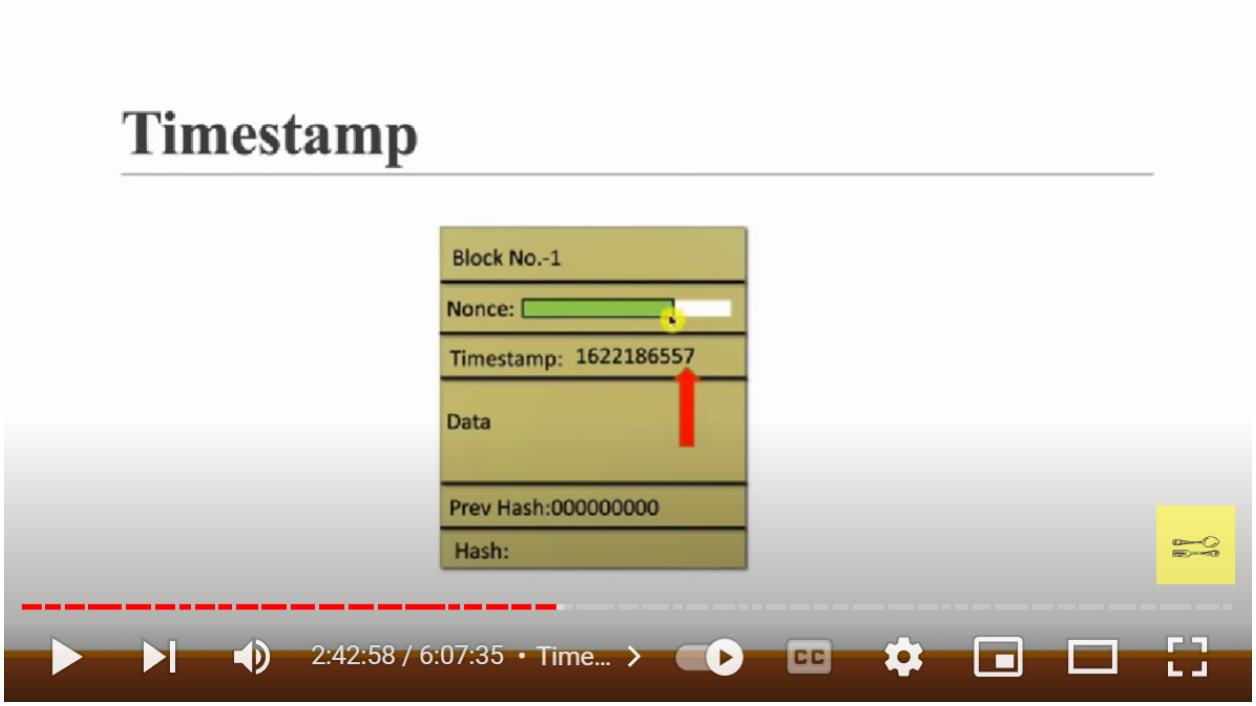


Timestamp




Timestamp
Block No.-1
Nonce:
Timestamp: 1622186555
Data
Prev Hash:000000000
Hash:
0.5 seconds
2:40:50 / 6:07:35 • Time...


Timestamp
Block No.-1
Nonce:
Timestamp: 1622186556
Data
Prev Hash:000000000
Hash:
2:41:19 / 6:07:35 • Time...


Timestamp
Block No.-1
Nonce:
Timestamp: 1622186557
Data
Prev Hash:000000000
Hash:
2:42:58 / 6:07:35 • Time...

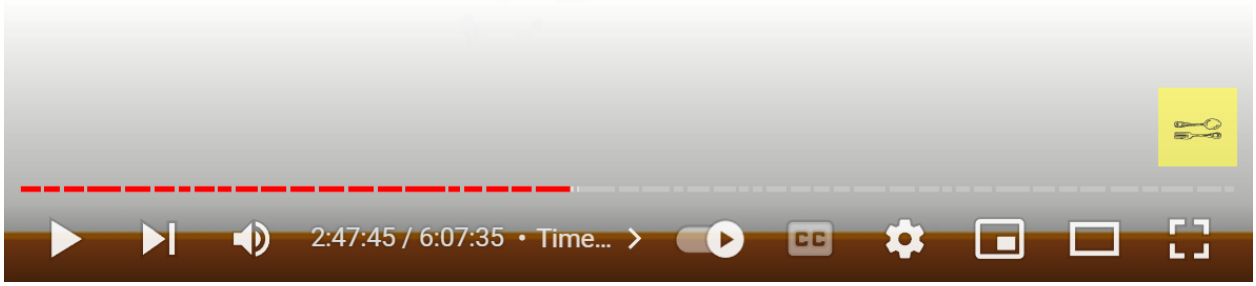

Timestamp
Current hashing rate is equal to 180 million trillion hashes/sec.
2:45:30 / 6:07:35 • Time...

Timestamp

Current hashing rate is equal to **180 million trillion hashes/sec**.

4 x 10^9 nonce will be covered in = (4 x 10^9)/(10^6 x10^12)= 4 x 10^-9 seconds.

4 x 10^-9 sec <<<<< 1 sec



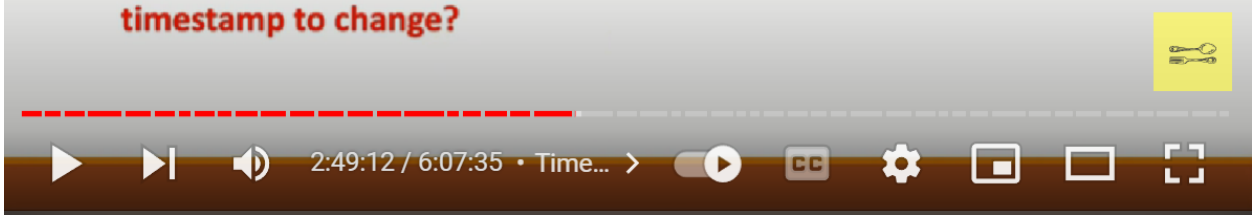
Timestamp

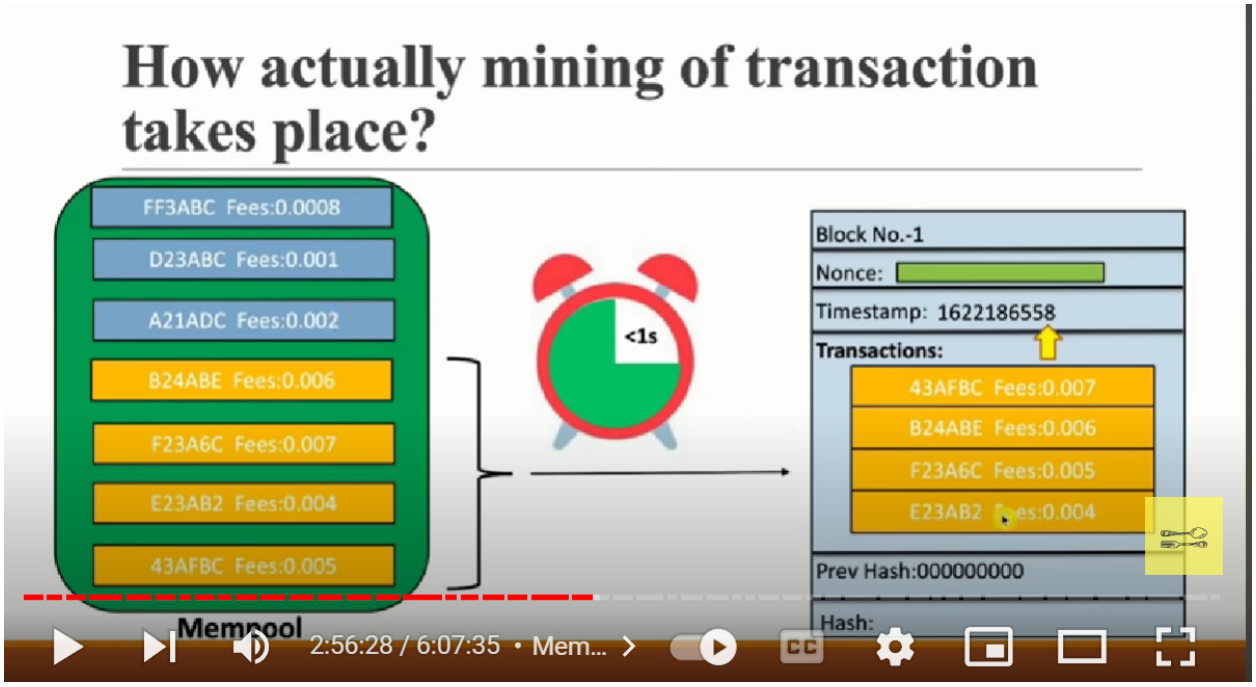
Current hashing rate is equal to **180 million trillion hashes/sec**.

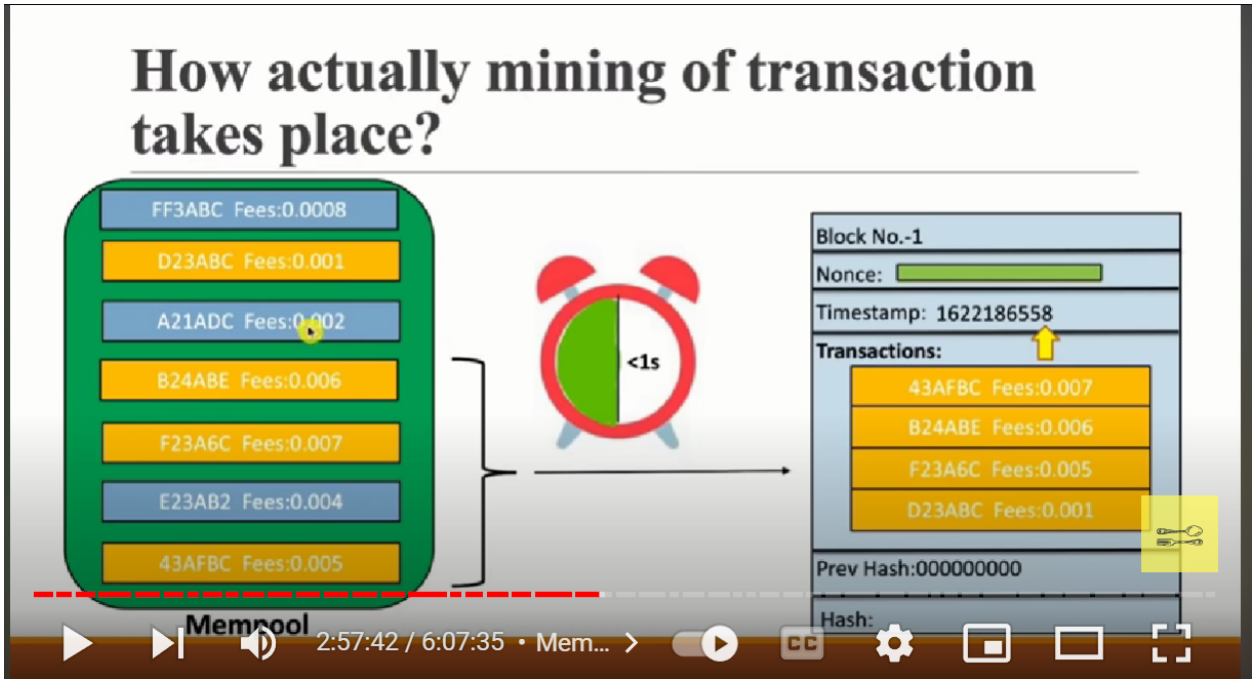
4 x 10^9 nonce will be covered in = (4 x 10^9)/(10^6 x10^12)= 4 x 10^-9 seconds.

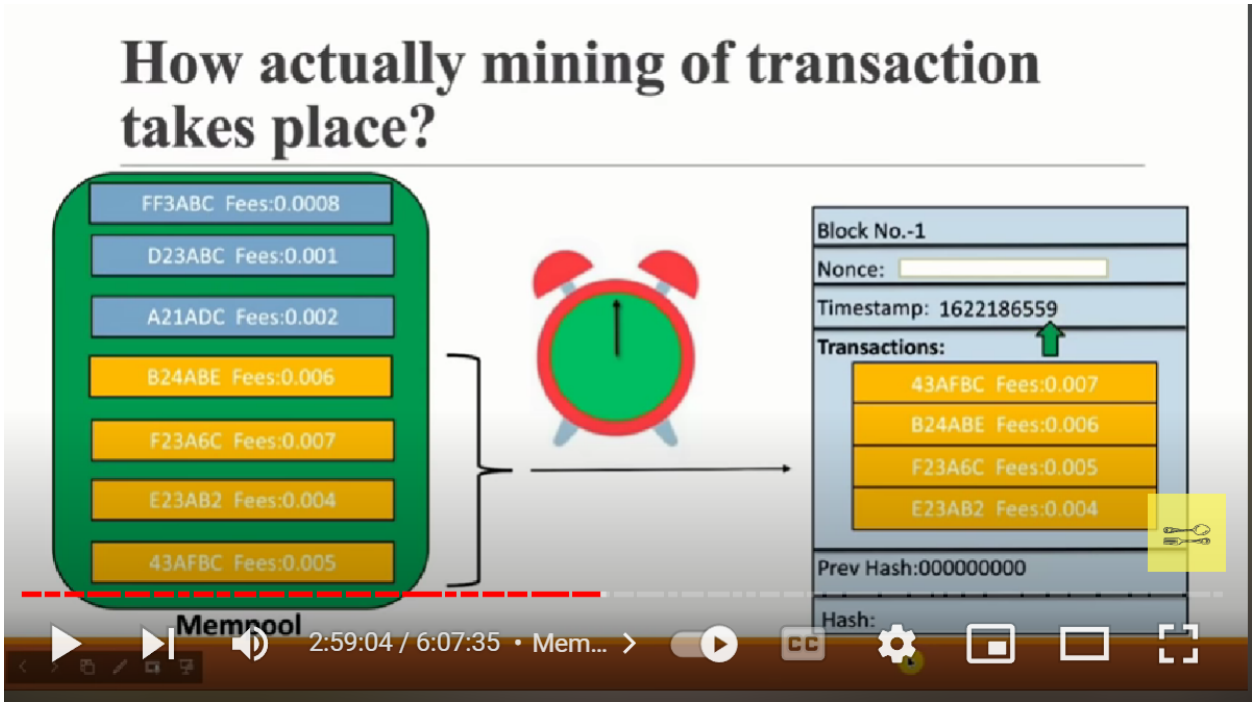
4 x 10^-9 sec <<<<< 1 sec

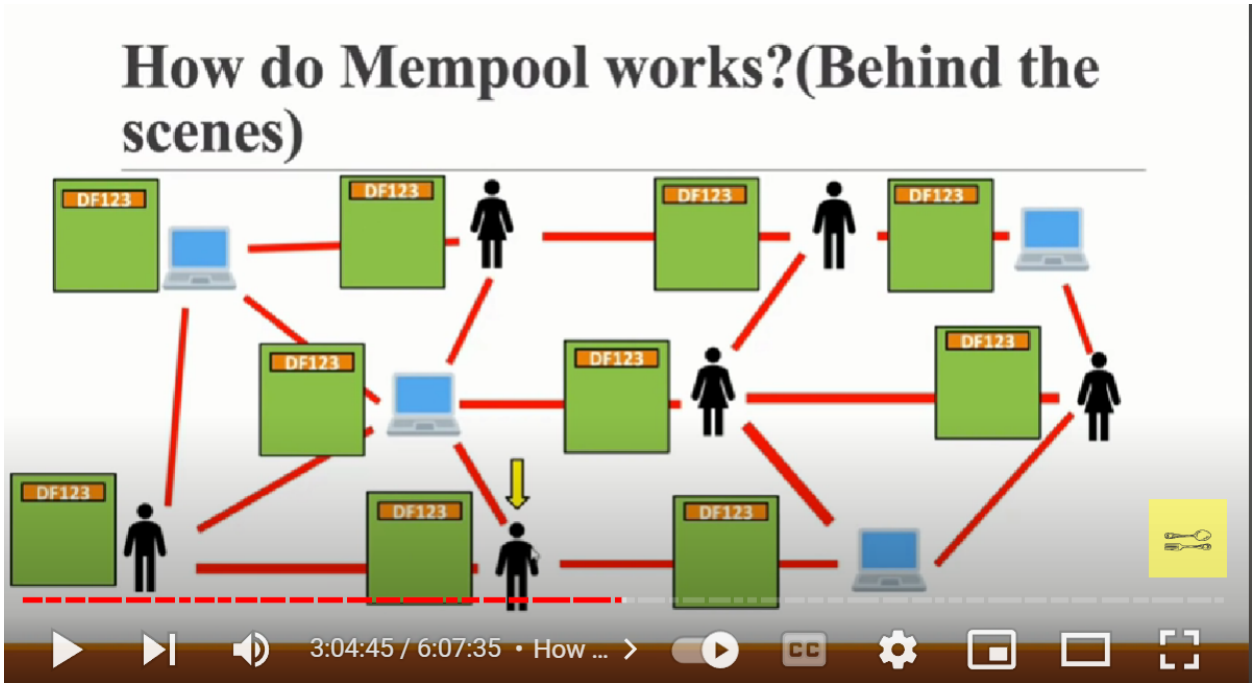
Q)What should the miners do in idle time? Should they wait for timestamp to change?

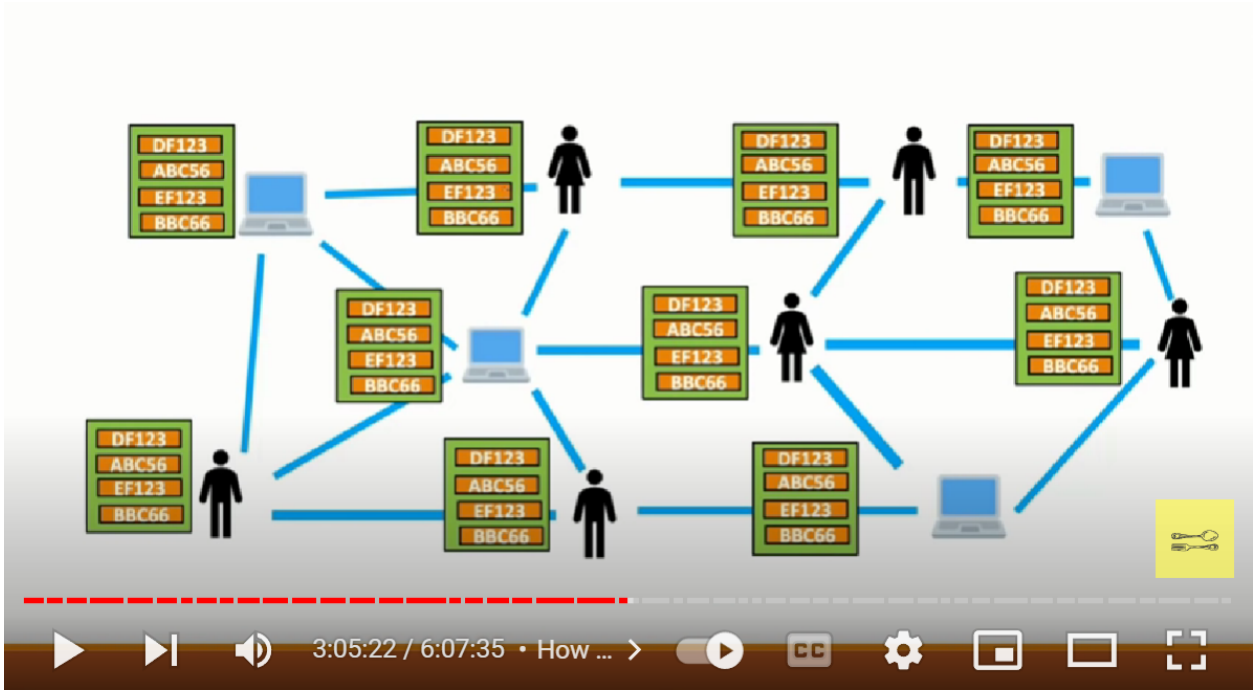


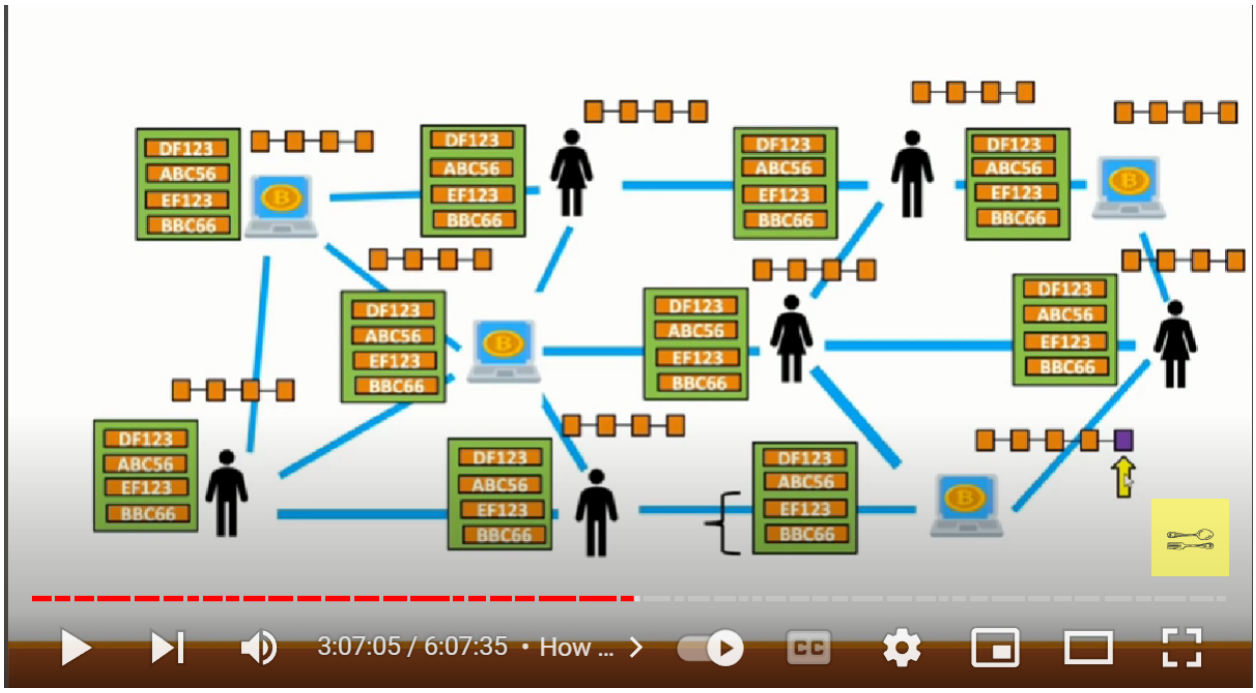

How actually mining of transaction takes place?
FF3ABC Fees:0.0008
D23ABC Fees:0.001
A21ADC Fees:0.002
B24ABE Fees:0.006
F23A6C Fees:0.007
E23AB2 Fees:0.004
43AFBC Fees:0.005
Mempool
<1s
Block No.-1
Nonce:
Timestamp: 1622186558
Transactions:
43AFBC Fees:0.007
B24ABE Fees:0.006
F23A6C Fees:0.005
E23AB2 Fees:0.004
Prev Hash:000000000
Hash:
2:56:28 / 6:07:35 • Mem...

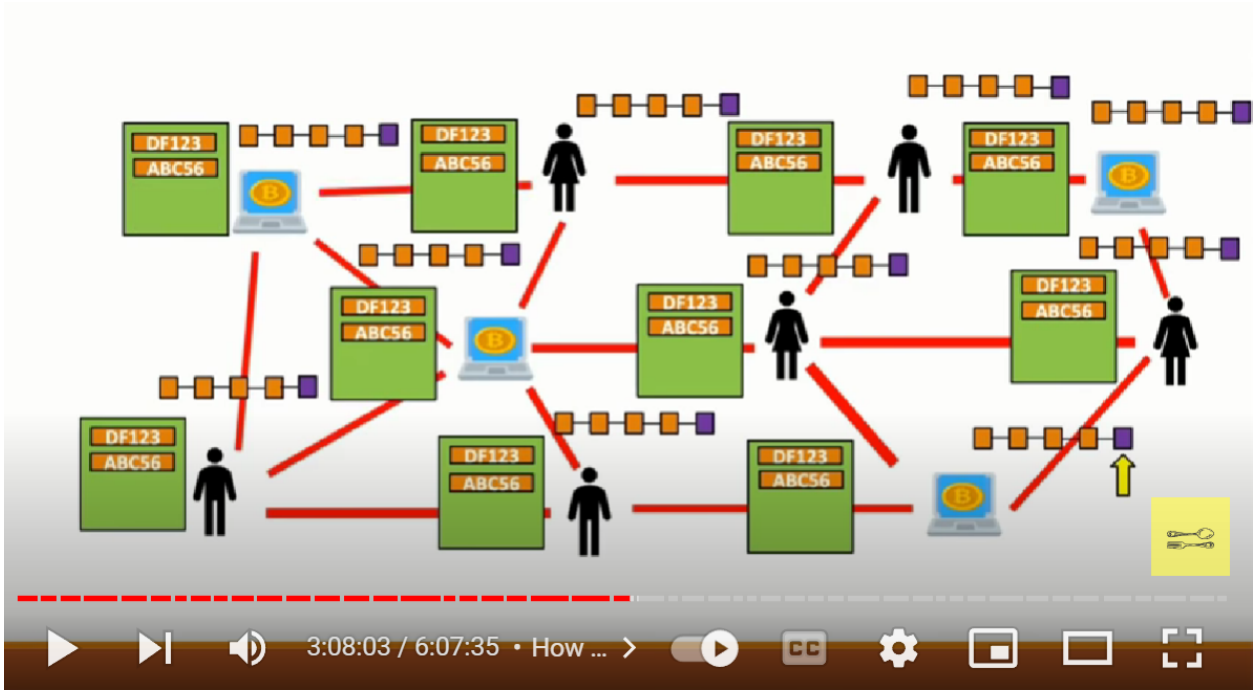

How actually mining of transaction takes place?
FF3ABC Fees:0.0008
D23ABC Fees:0.001
A21ADC Fees:0.002
B24ABE Fees:0.006
F23A6C Fees:0.007
E23AB2 Fees:0.004
43AFBC Fees:0.005
Mempool
<1s
Block No.-1
Nonce:
Timestamp: 1622186558
Transactions:
43AFBC Fees:0.007
B24ABE Fees:0.006
F23A6C Fees:0.005
D23ABC Fees:0.001
Prev Hash:000000000
Hash:
2:57:42 / 6:07:35 • Mem...

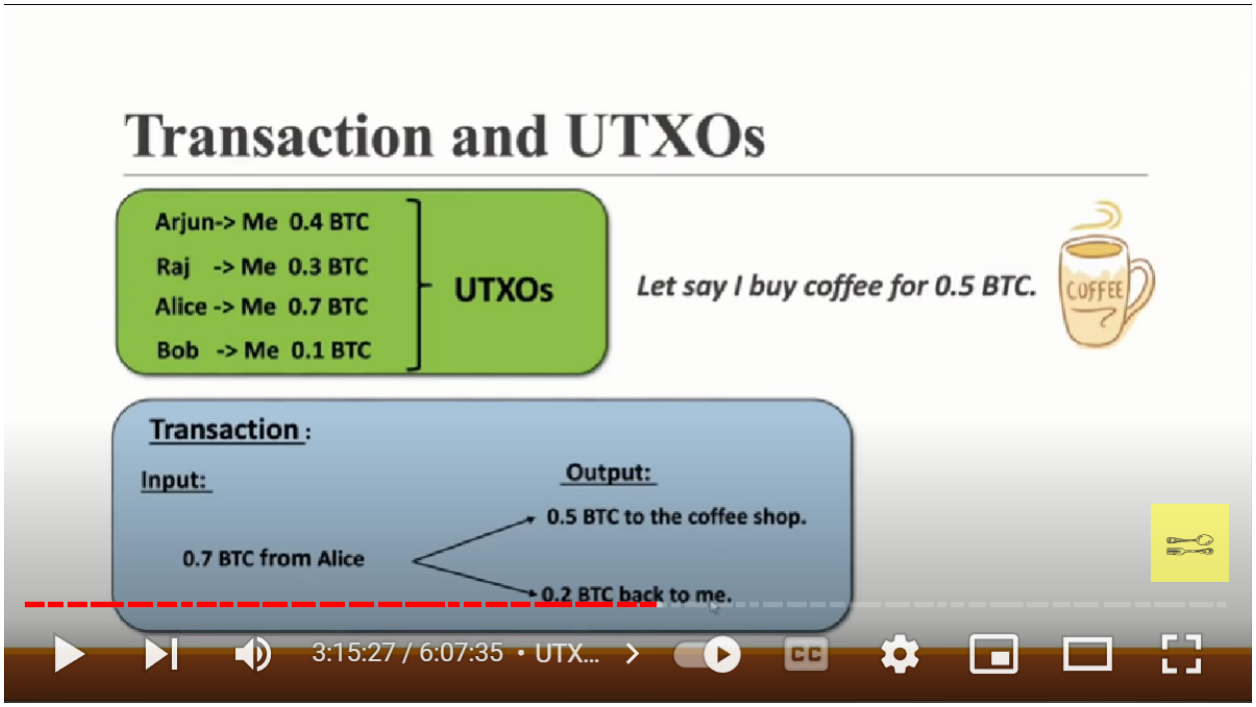

How actually mining of transaction takes place?
FF3ABC Fees:0.0008
D23ABC Fees:0.001
A21ADC Fees:0.002
B24ABE Fees:0.006
F23A6C Fees:0.007
E23AB2 Fees:0.004
43AFBC Fees:0.005
Mempool
Block No.-1
Nonce:
Timestamp: 1622186559
Transactions:
43AFBC Fees:0.007
B24ABE Fees:0.006
F23A6C Fees:0.005
E23AB2 Fees:0.004
Prev Hash:000000000
Hash:
2:59:04 / 6:07:35 • Mem...

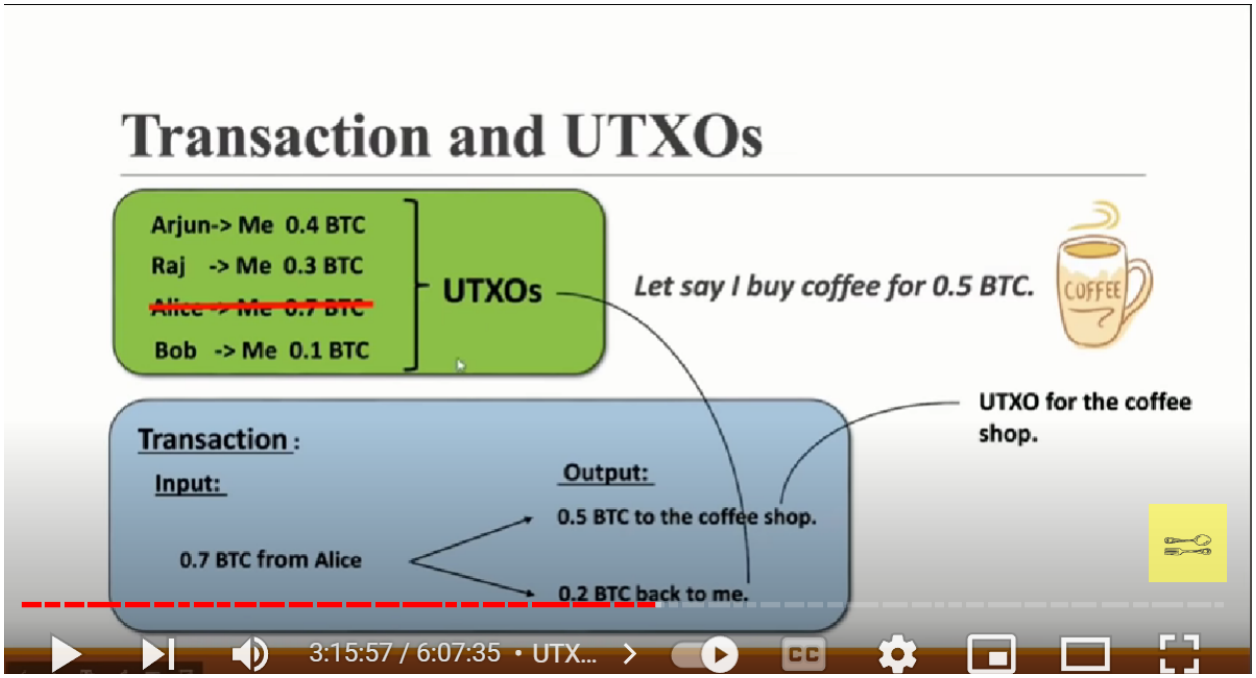

How do Mempool works?(Behind the scenes)
DF123
3:04:45 / 6:07:35 • How ...

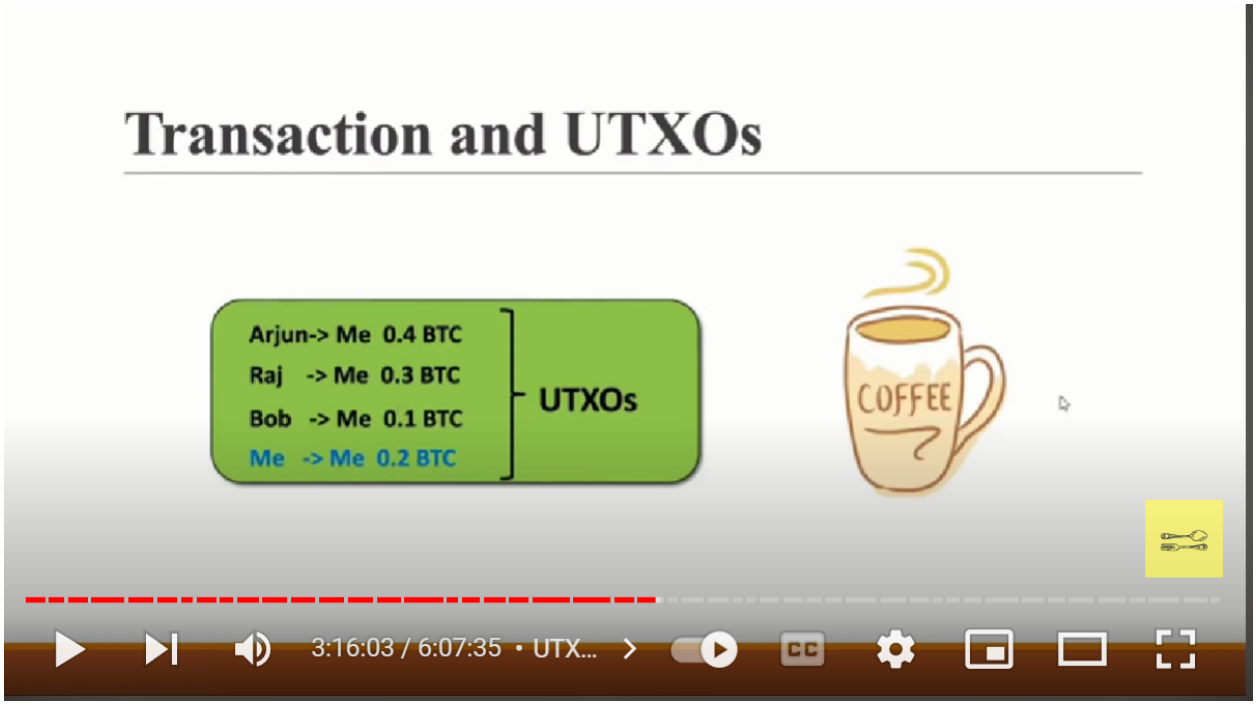

DF123
ABC56
EF123
BBC66
3:05:22 / 6:07:35 • How ...

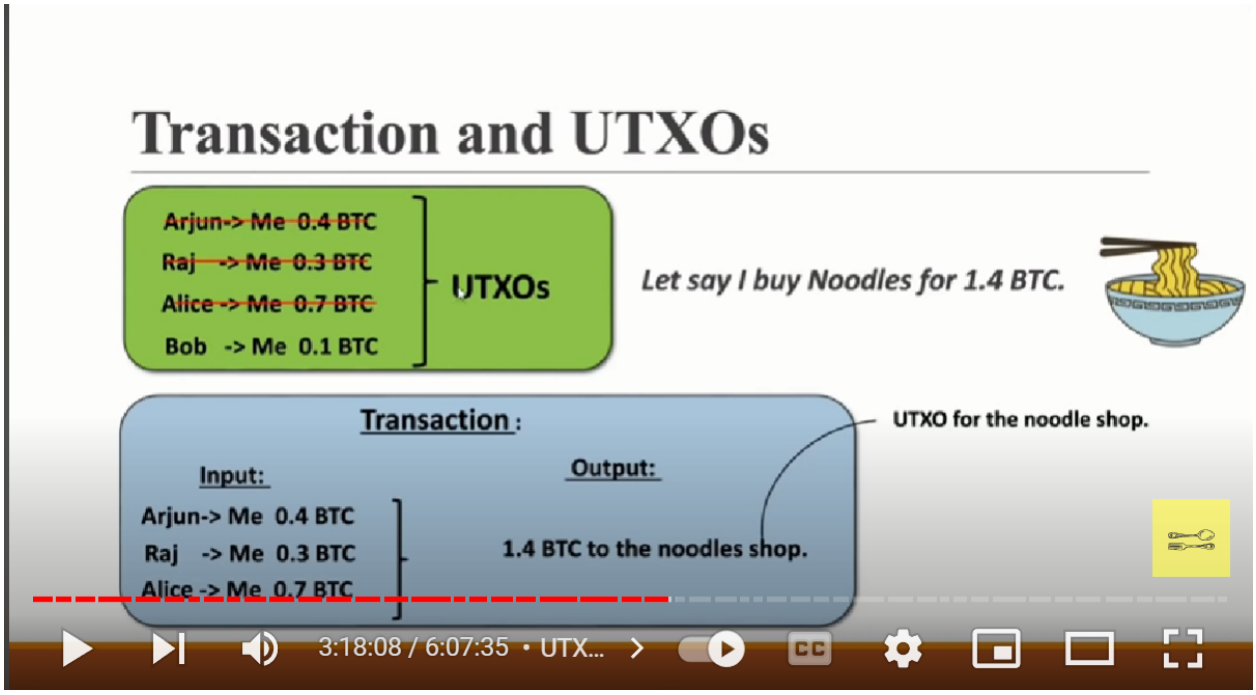

DF123
ABC56
EF123
BBC66
3:07:05 / 6:07:35 • How ...

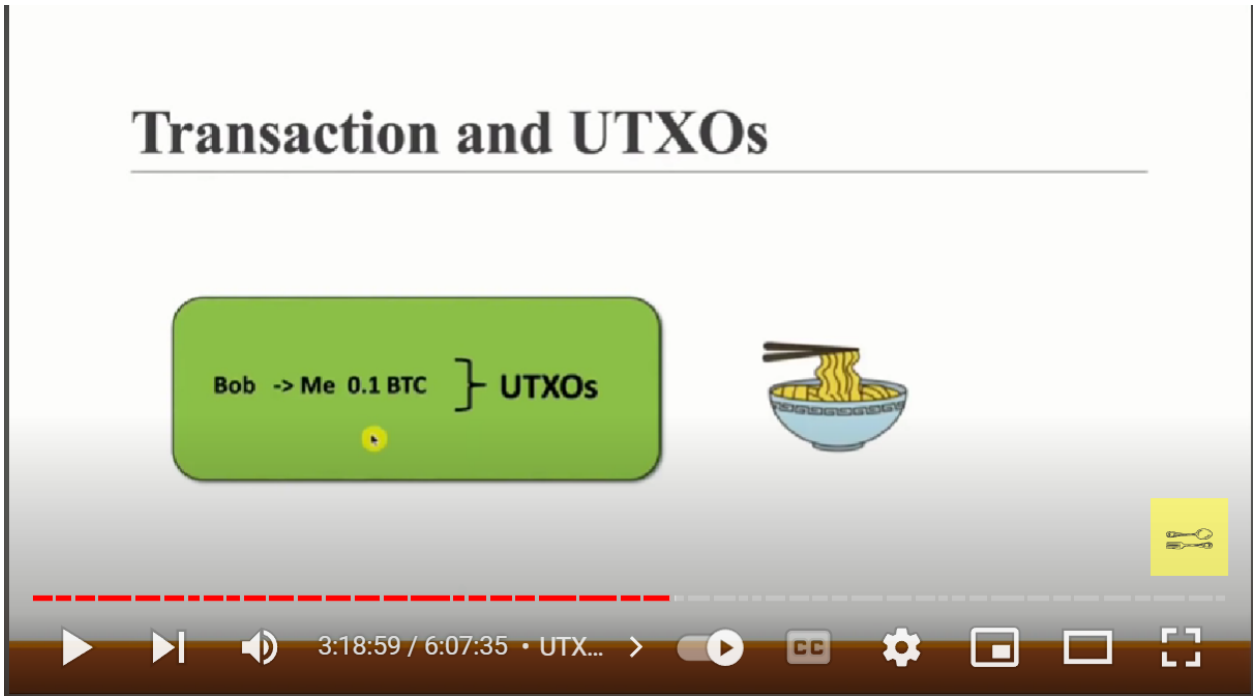

DF123
ABC56
3:08:03 / 6:07:35 • How ...

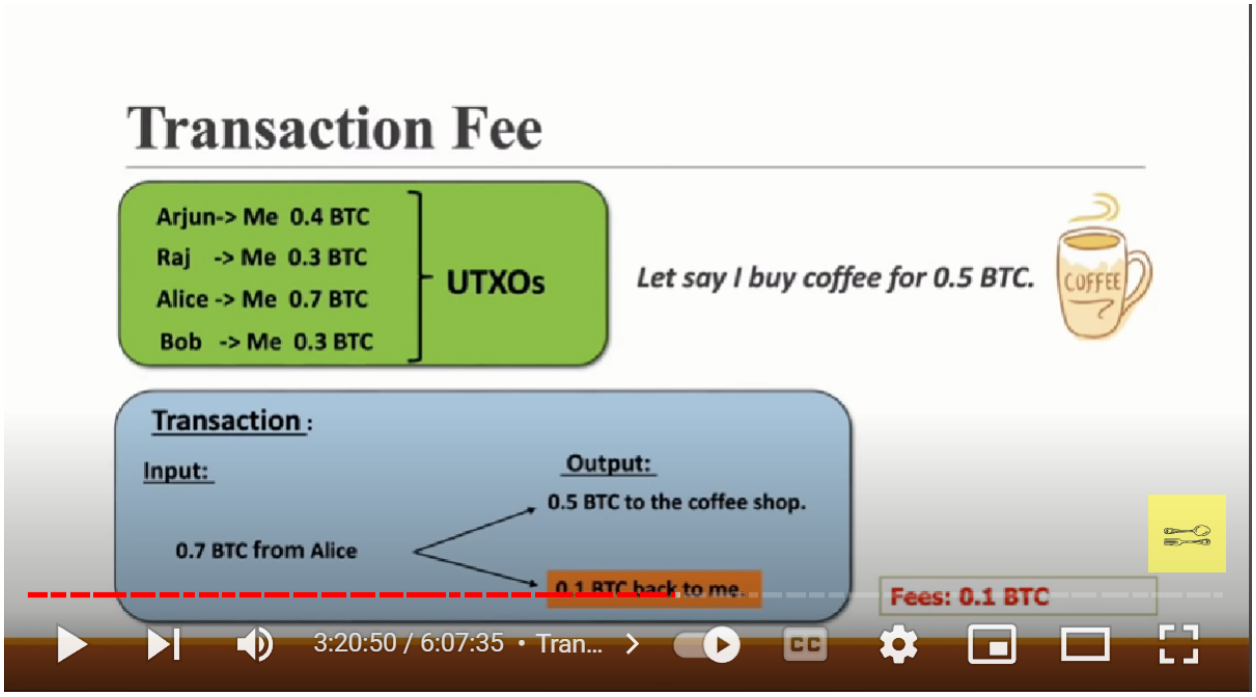

Transaction and UTXOs
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
UTXOs
Let say I buy coffee for 0.5 BTC.
COFFEE
Transaction :
Input:
Output:
0.7 BTC from Alice
0.5 BTC to the coffee shop.
0.2 BTC back to me.
3:15:27 / 6:07:35 • UTX...

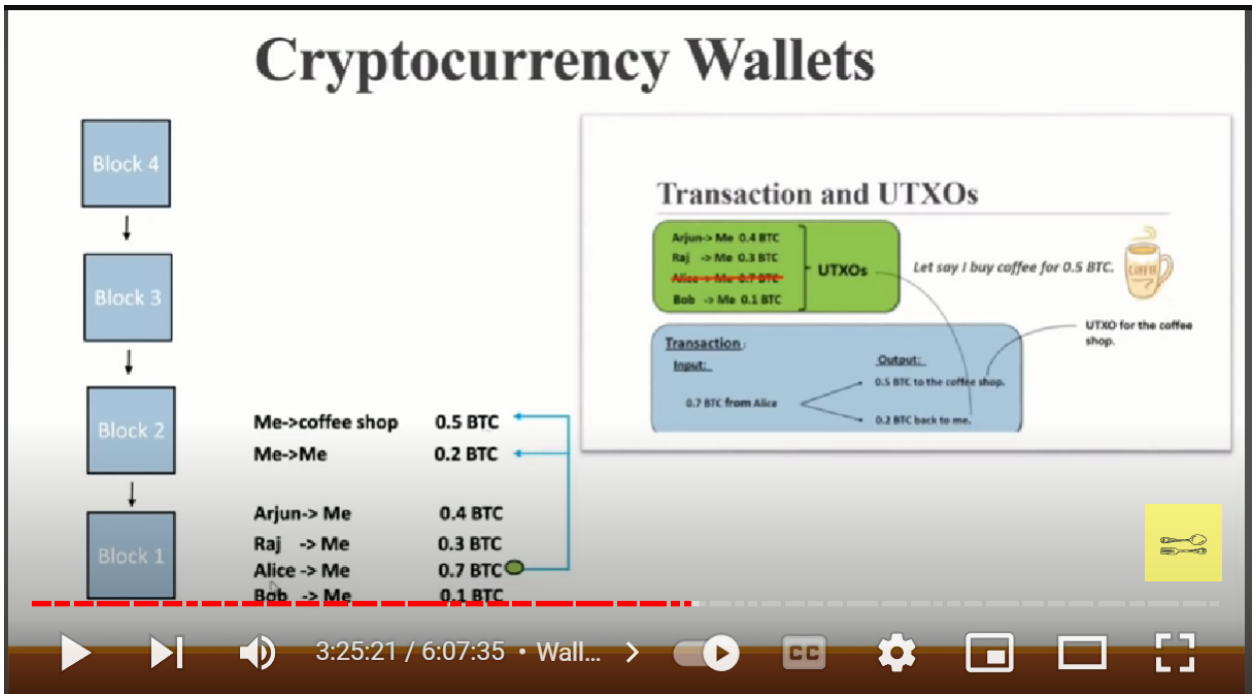

Transaction and UTXOs
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
UTXOs
Let say I buy coffee for 0.5 BTC.
COFFEE
Transaction :
Input:
0.7 BTC from Alice
Output:
0.5 BTC to the coffee shop.
0.2 BTC back to me.
UTXO for the coffee shop.
3:15:57 / 6:07:35 • UTX...

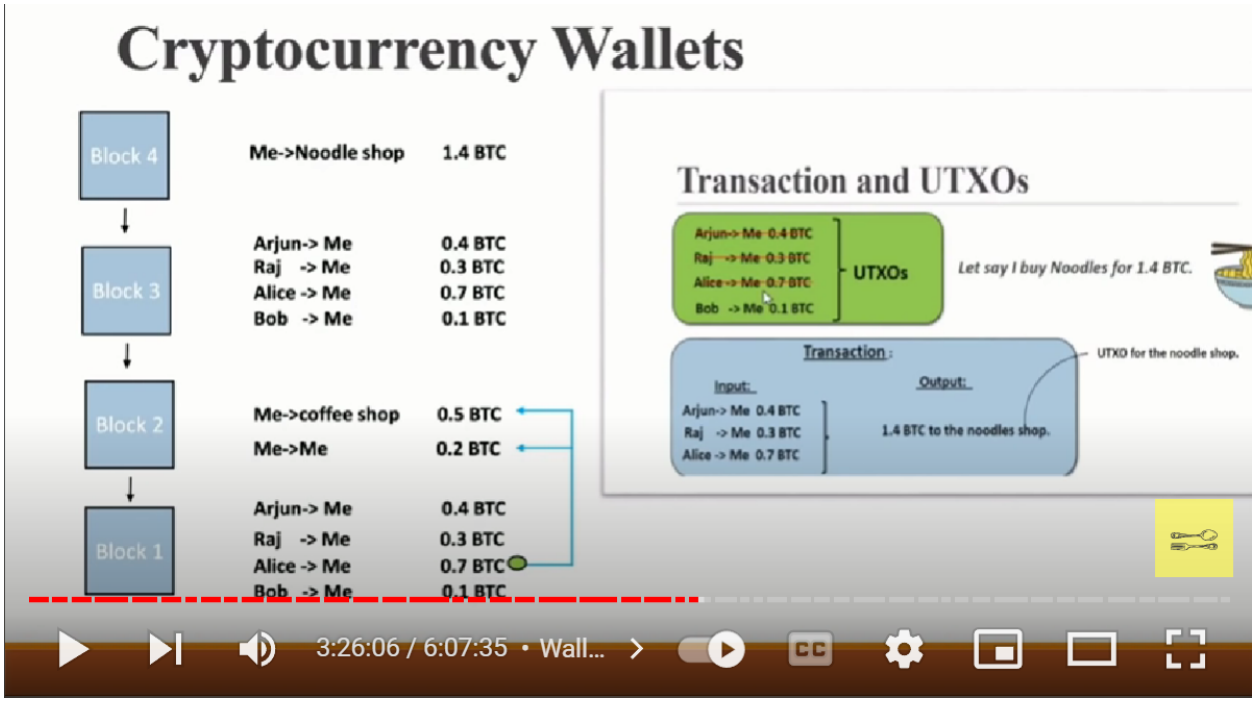

Transaction and UTXOs
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Bob -> Me 0.1 BTC
Me -> Me 0.2 BTC
UTXOs
COFFEE
3:16:03 / 6:07:35 • UTX...

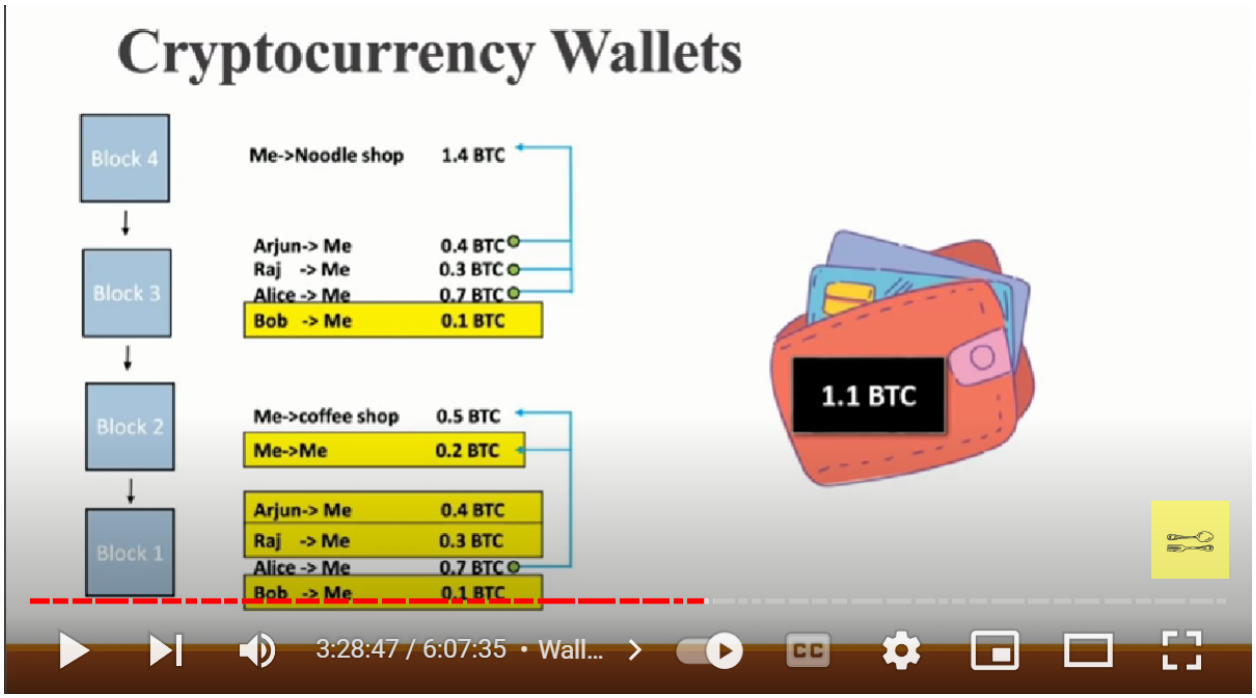

Transaction and UTXOs
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
UTXOs
Let say I buy Noodles for 1.4 BTC.
Transaction :
Input:
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Output:
1.4 BTC to the noodles shop.
UTXO for the noodle shop.
3:18:08 / 6:07:35 • UTX...

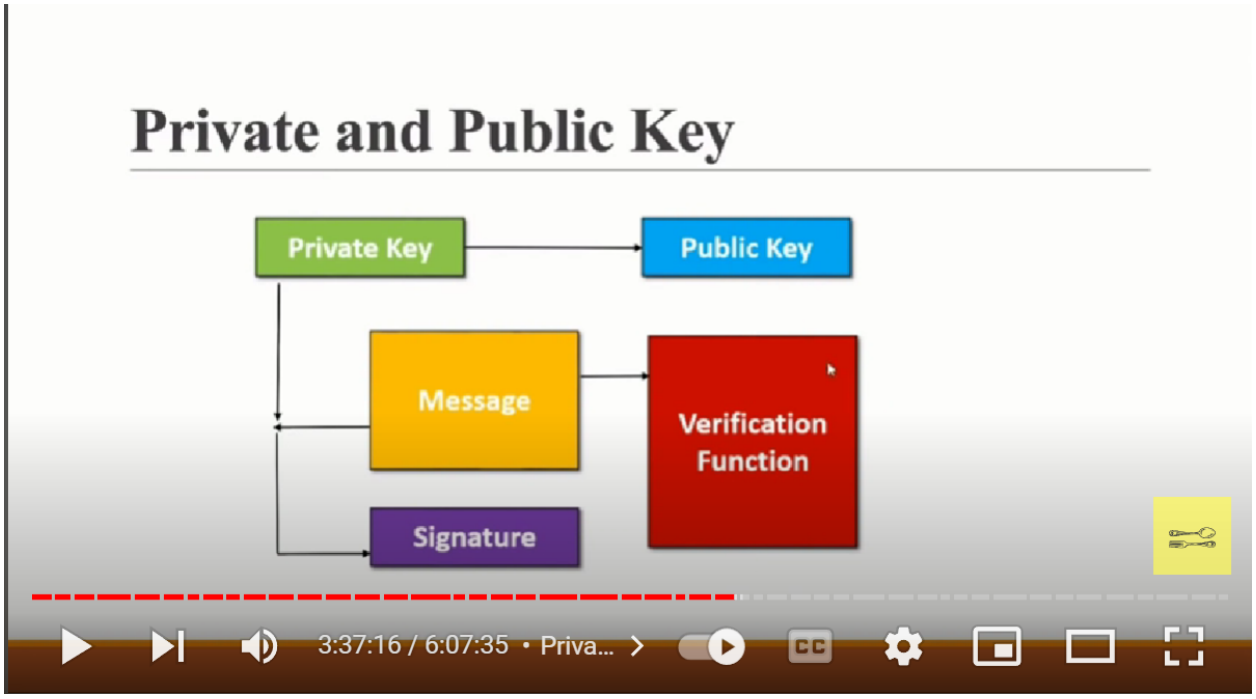

Transaction and UTXOs
Bob -> Me 0.1 BTC
UTXOs
3:18:59 / 6:07:35 • UTX...

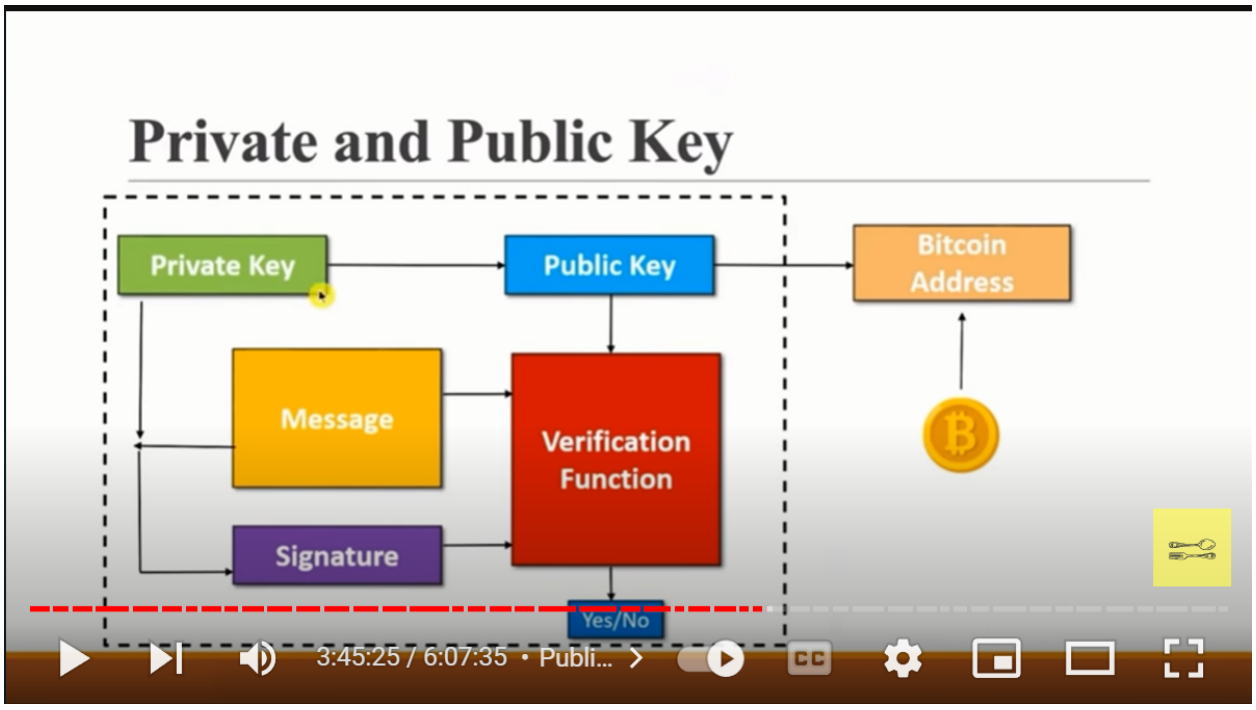

Transaction Fee
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.3 BTC
UTXOs
Let say I buy coffee for 0.5 BTC.
COFFEE
Transaction :
Input:
0.7 BTC from Alice
Output:
0.5 BTC to the coffee shop.
0.1 BTC back to me.
Fees: 0.1 BTC
3:20:50 / 6:07:35 • Tran...

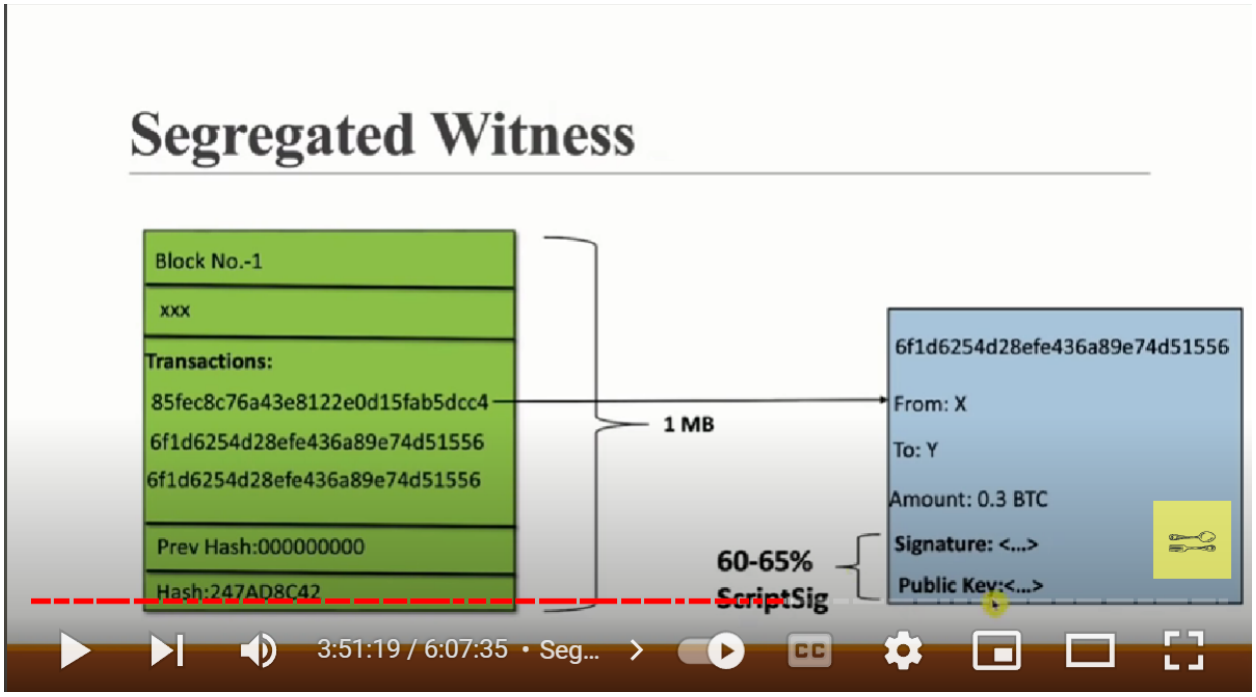

Cryptocurrency Wallets
Block 4
Block 3
Block 2
Block 1
Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
Transaction and UTXOs
UTXOs
Let say I buy coffee for 0.5 BTC.
Transaction :
Input:
Output:
0.7 BTC from Alice
0.5 BTC to the coffee shop.
0.2 BTC back to me.
UTXO for the coffee shop.
3:25:21 / 6:07:35 • Wall...

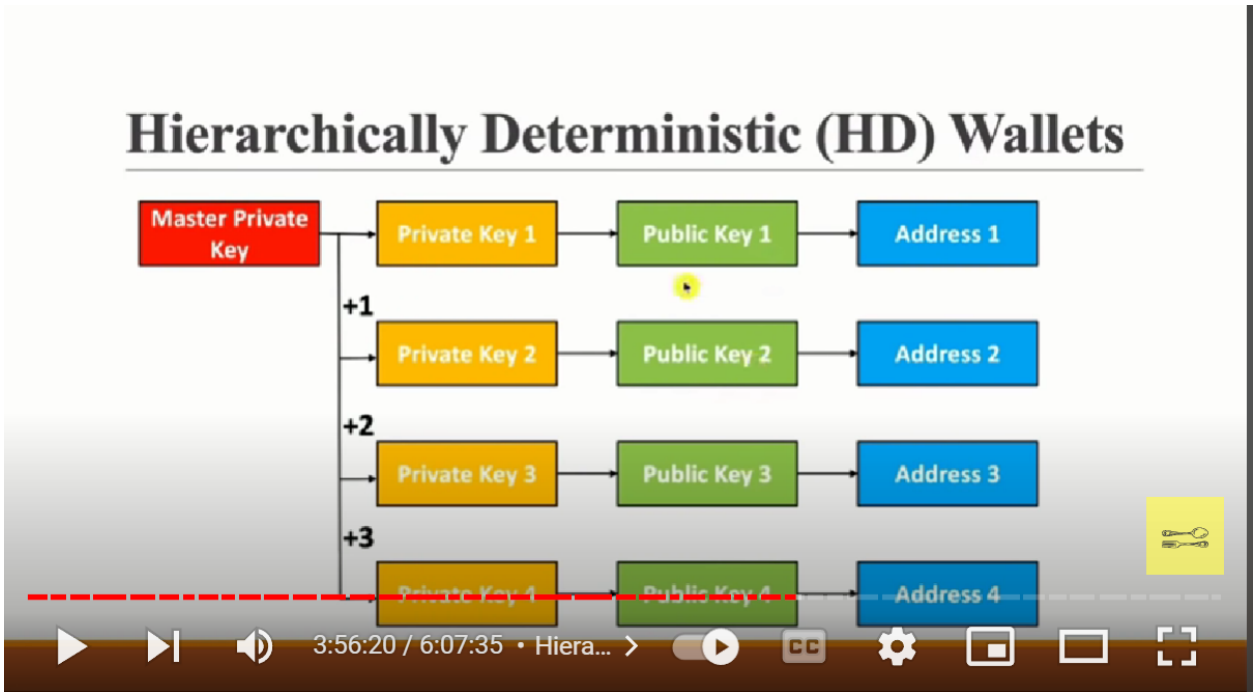

Cryptocurrency Wallets
Block 4
Me->Noodle shop 1.4 BTC
Block 3
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
Block 2
Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC
Block 1
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
Transaction and UTXOs
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
UTXOs
Let say I buy Noodles for 1.4 BTC.
Transaction :
Input:
Output:
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
1.4 BTC to the noodles shop.
UTXO for the noodle shop.
3:26:06 / 6:07:35 • Wall...


Cryptocurrency Wallets
Block 4
Me->Noodle shop 1.4 BTC
Block 3
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
Block 2
Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC
Block 1
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC
1.1 BTC
3:28:47 / 6:07:35 • Wall...


Private and Public Key
Private Key
Public Key
Message
Verification Function
Signature
3:37:16 / 6:07:35 • Priva...


Private and Public Key
Private Key
Public Key
Bitcoin Address
Message
Verification Function
Signature
Yes/No
3:45:25 / 6:07:35 • Publi...


Segregated Witness
Block No.-1
xxx
Transactions:
85fec8c76a43e8122e0d15fab5dcc4
6f1d6254d28efe436a89e74d51556
6f1d6254d28efe436a89e74d51556
Prev Hash:000000000
Hash:247AD8C42
1 MB
6f1d6254d28efe436a89e74d51556
From: X
To: Y
Amount: 0.3 BTC
Signature: <...>
Public Key:<...>
60-65%
ScriptSig
3:51:19 / 6:07:35 • Seg...


Hierarchically Deterministic (HD) Wallets
Master Private Key
Private Key 1
Public Key 1
Address 1
+1
Private Key 2
Public Key 2
Address 2
+2
Private Key 3
Public Key 3
Address 3
+3
Address 4
3:56:20 / 6:07:35 • Hiera...