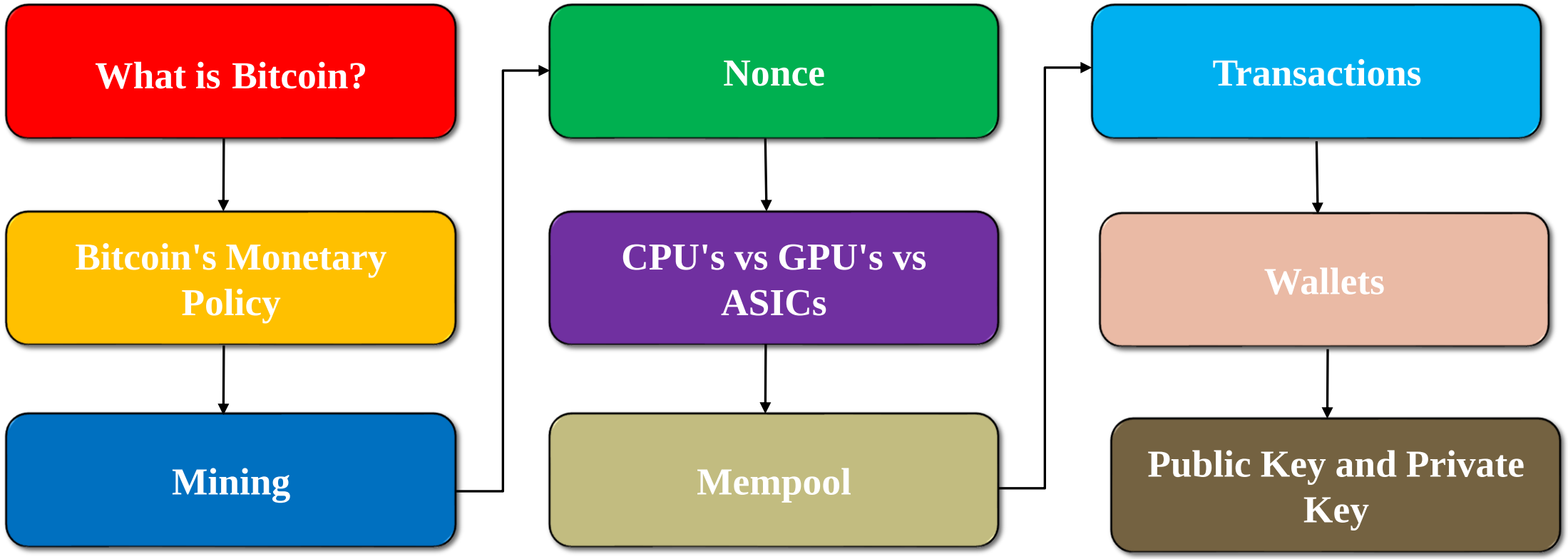
Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.

Cryptocurrency

Contents – Module B



CPUs Vs GPUs Vs ASICs

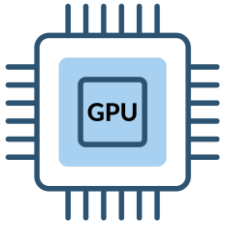
CPUs Vs GPUs Vs ASICs

- If one miner generates 5H/s and the second generates 10H/s
- The second miner has a higher chance of generating the hashes quickly and winning the reward
- Miner uses different technologies that generate different hashes per second
- At the start, people used CPUs (General purposes) for mining
- Then GPUs were used, as GPUs generate hashes much faster than CPUs
- GPU not specialized in generating hashes i.e., GPU can be used for gaming, etc.
- ASIC was introduced, specialized in generating hashes, and is capable of generating hashes much faster than GPUs
- The **latest Bitcoin ASIC miner (S19 Pro version)** can generate **110 TH/s**

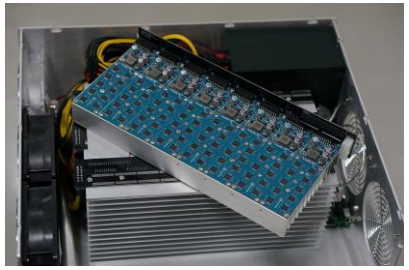
CPUs Vs GPUs Vs ASICs

CPU < 10 MH/s

GPU < 1 GH/s



ASIC > 1000 GH/s



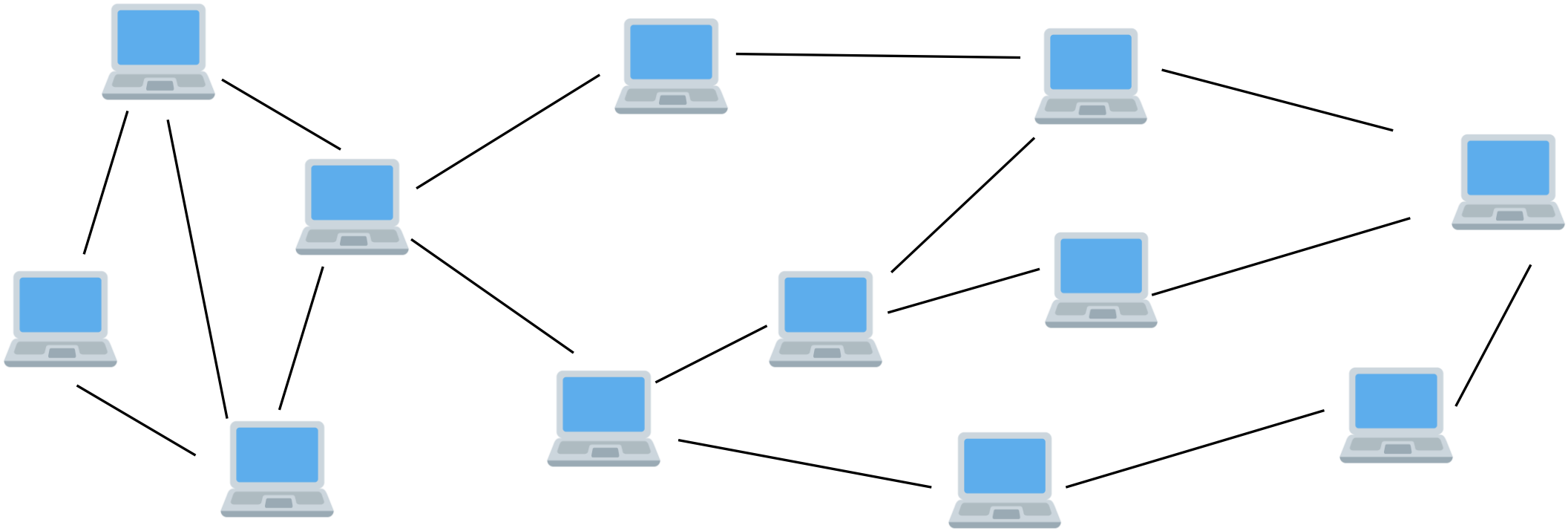
ASICs

Model	Release	Hashrate	Power	Noise	Algo	Profitability
Bitmain Antminer KS3 (8.3Th)	Aug 2023	8.3 Th/s	3188 W	75 db	KHeavyHash	$312.66 /day
Jasminer X16-P	Aug 2023	5.8 Gh/s	1900 W	75 db	EtHash	$4.58 /day
Bitmain Antminer K7 (63.5Th)	Jan 2023	63.5 Th/s	3080 W	75 db	Eaglesong	$3.50 /day
Bitmain Antminer L7 (9.5Gh)	Nov 2021	9.5 Gh/s	3425 W	75 db	Scrypt	$3.49 /day
Bitmain Antminer L7 (9.3Gh)	Feb 2022	9.3 Gh/s	3425 W	75 db	Scrypt	$3.20 /day
Bitmain Antminer L7 (9.16Gh)	Nov 2021	9.16 Gh/s	3425 W	75 db	Scrypt	$3.01 /day
Bitmain Antminer L7 (9.05Gh)	Feb 2022	9.05 Gh/s	3425 W	75 db	Scrypt	$2.85 /day

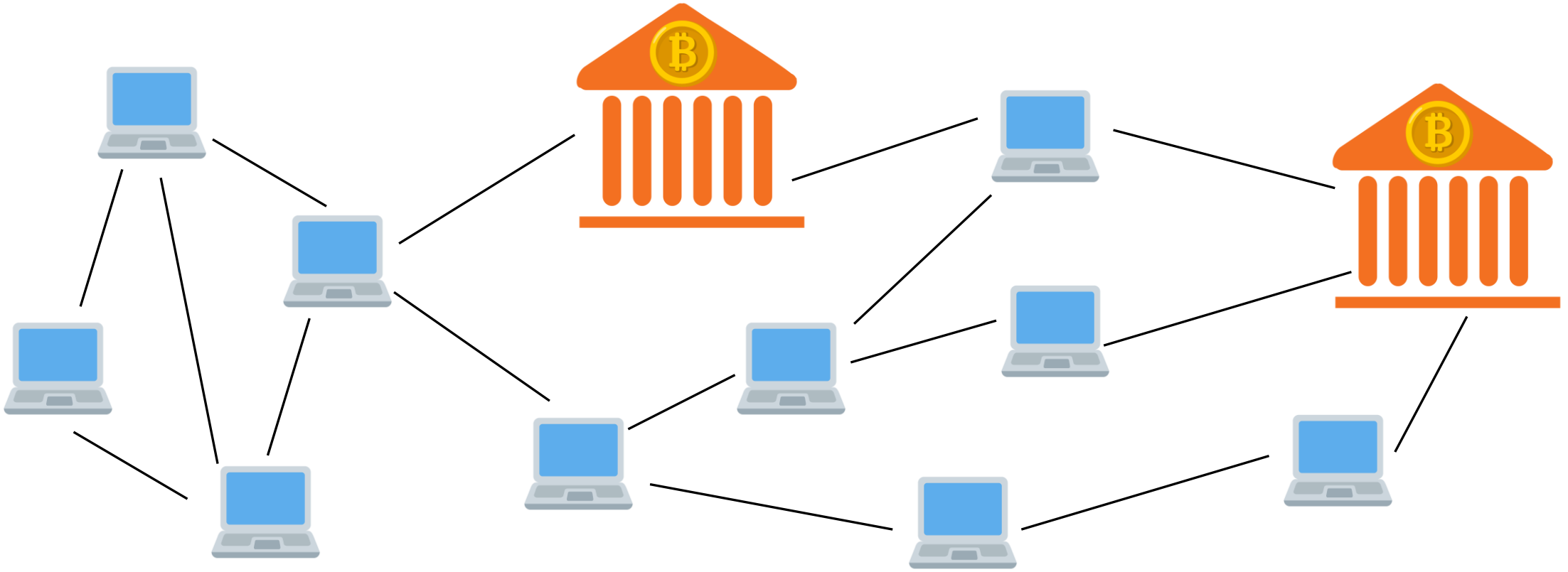
https://www.asicminervalue.com/

Mining Pool

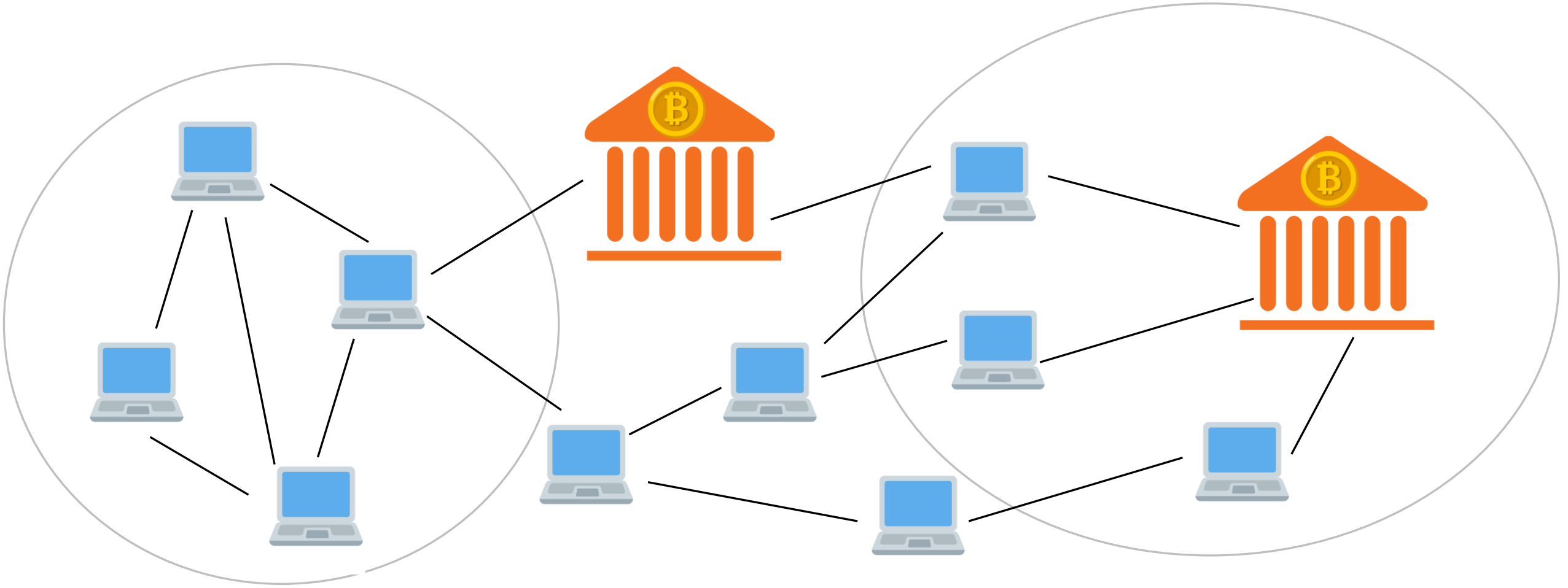
Mining Pools



Mining Pools



Mining Pools



Mining Pools

- A space that allows miners to work cooperatively to mine blocks
- Miner interacts with each other using different technologies
- If big miners join the network (Industries created), the chances for small miners to mine blocks decrease and thus exploited **(Elon Musk)**
- Therefore, mining pools are created, where small miners work jointly
- Rewards are distributed proportionately to the provided resources
- The software used for the mining pool ensures parallelism and miners work on different ranges

Mining Pools

Advantages of joining Mining Pools:

- Provide faster processing
- Cheaper, can provide a stable income
- If one is unaware of the mining, he pays small fees and joins the pool

Disadvantages of joining Mining Pools:

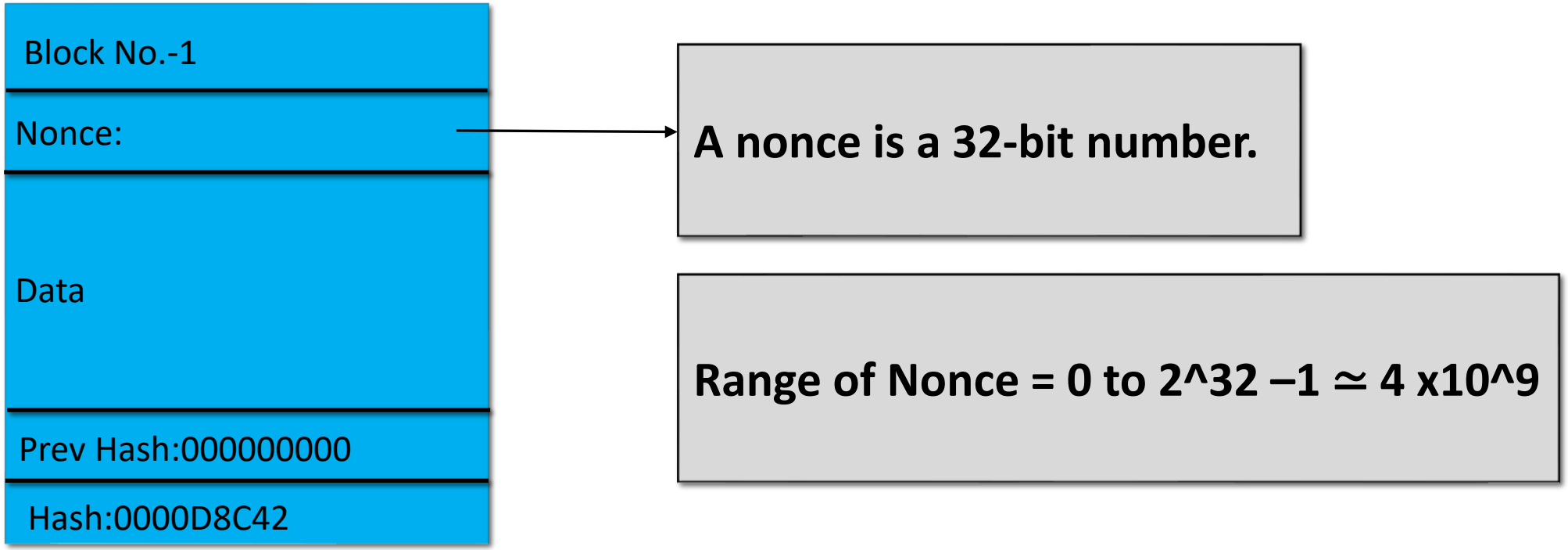
- Joining a very big pool gives a small portion of the reward
- Bigger pools get a high commission

Hash rate Distribution Demonstration

https://www.blockchain.com/charts/pools

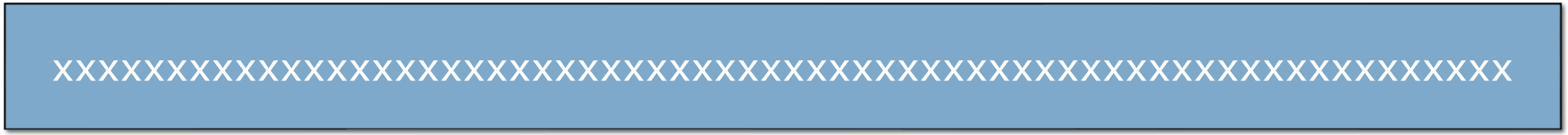
Nonce Range

Nonce Range


Block No.-1
Nonce:
Data
Prev Hash:000000000
Hash:0000D8C42
A nonce is a 32-bit number.
Range of Nonce = 0 to 2^32 –1 ≃ 4 x10^9

Nonce Range

SHA 256



Total number of possible hashes = 16 x 16 x.....16 = 16^64 ≃ 10^77

Nonce Range

- Nonce is a 32-bit number
- The total numbers of nonces are 2^32 ≃ 4 billion
- SHA-256 has 64 hexadecimal numbers each position has 16 possibilities
- The total number of hashes that can be generated from SHA-256 is

  16^64 ≃ 10^77

Nonce Range

Total hashes $\simeq 10^{77}$

Total number of Nonce that we can generate $\simeq 4 \times 10^{9}$

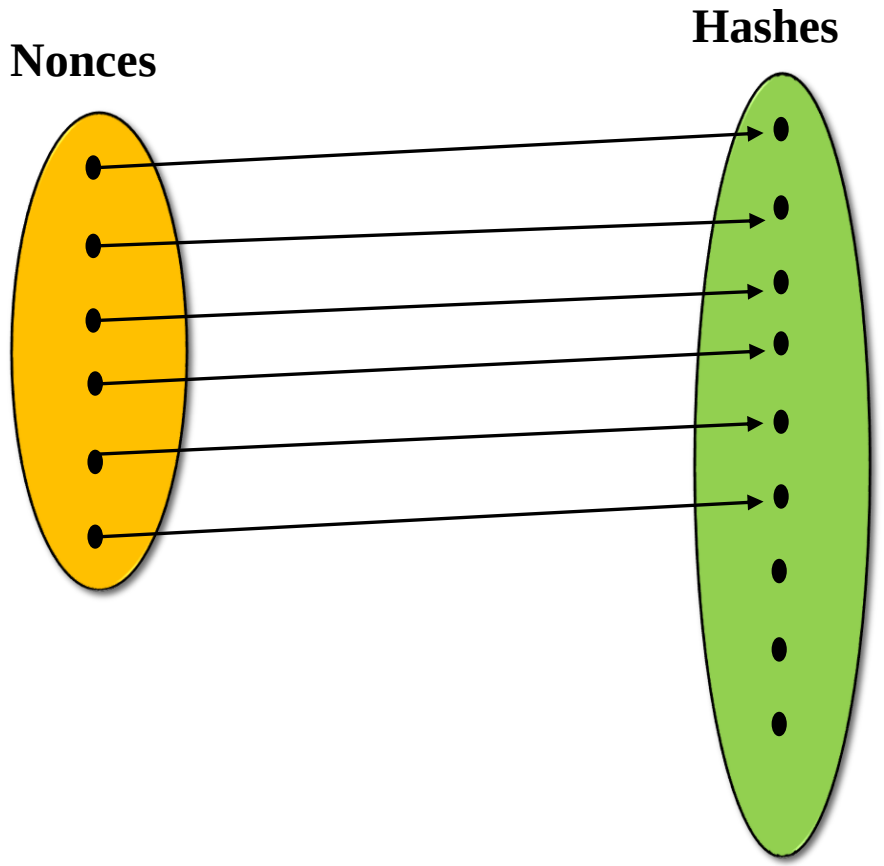
$10^{77} >>>>> 4 \times 10^{9}$

10^{77} is much greater than 4×10^{9}

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

Nonce Range

- Total Nonces ≃ 4 x10^9 on the left side
- Total hashes ≃ 10^77 on the right side
- Some parts of the hashes can be generated by a nonce
- A modest miner generates 10^8 H/s, then 4 billion nonces will be covered in 40 seconds.
- How to check the remaining hashes?



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.

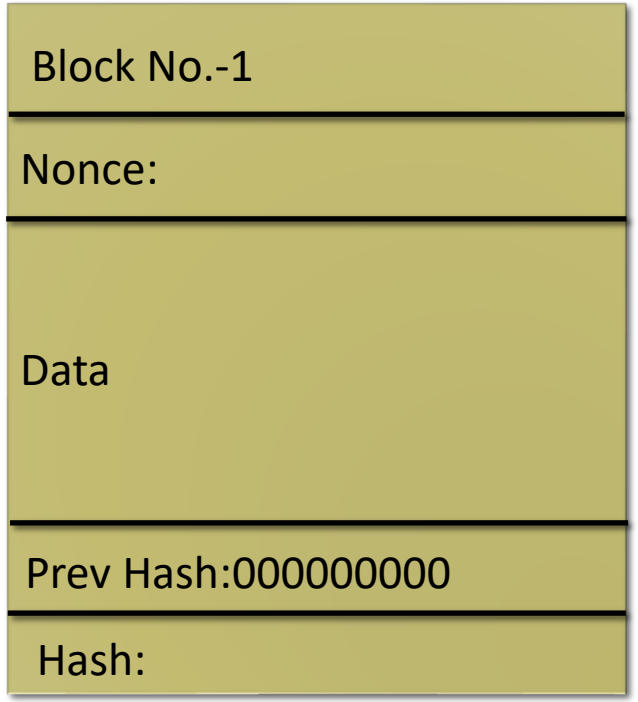
Q) So, what the miners do when all the nonce get exhausted and miners have not hit the target ?

Timestamp

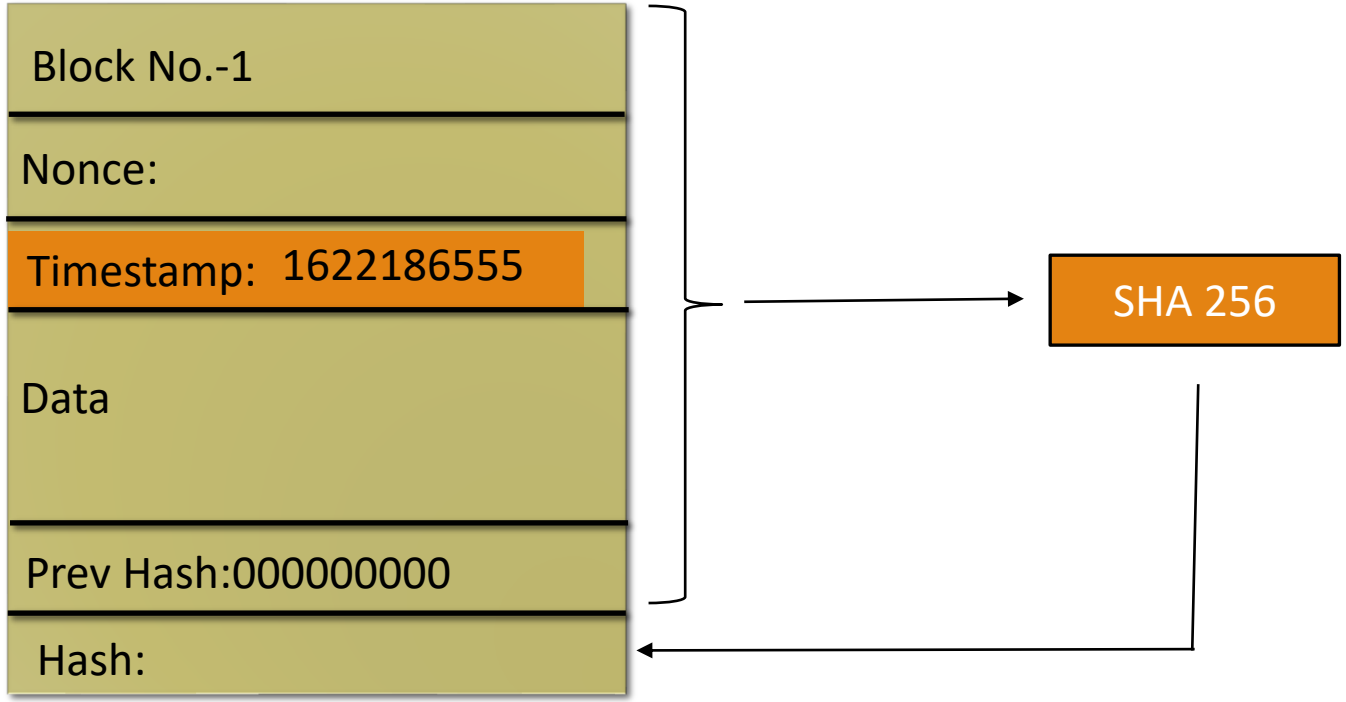
Timestamp

- The timestamp field is introduced to generate the remaining hashes.
- Timestamp is a Unix time, Unix time represents time in seconds, and it started when Unix was introduced on January 1, 1970.
- The hash is calculated for all the block fields including a timestamp
- Miner exhausts 0.1 billion nonces in 1 second, while the timestamp changes, and due to the avalanche effect, the new hashes will be drastically changed.

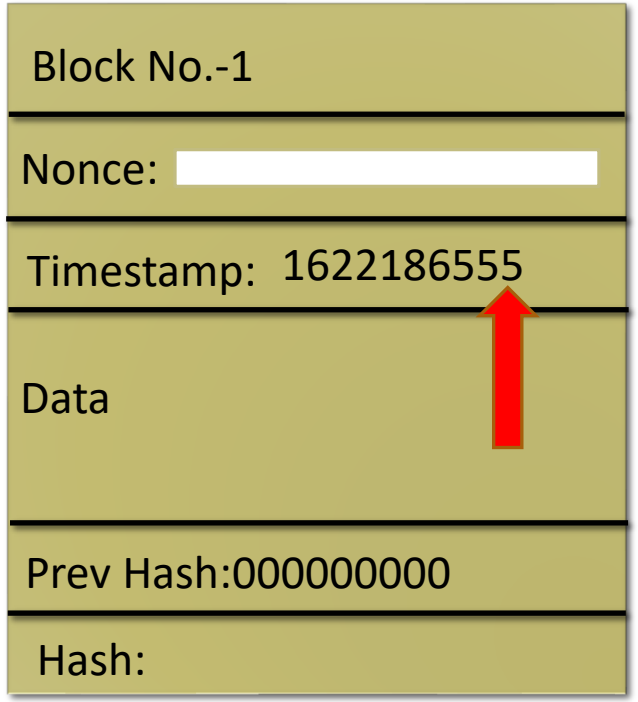
Timestamp



Timestamp


Block No.-1
Nonce:
Timestamp: 1622186555
Data
Prev Hash:000000000
Hash:
SHA 256

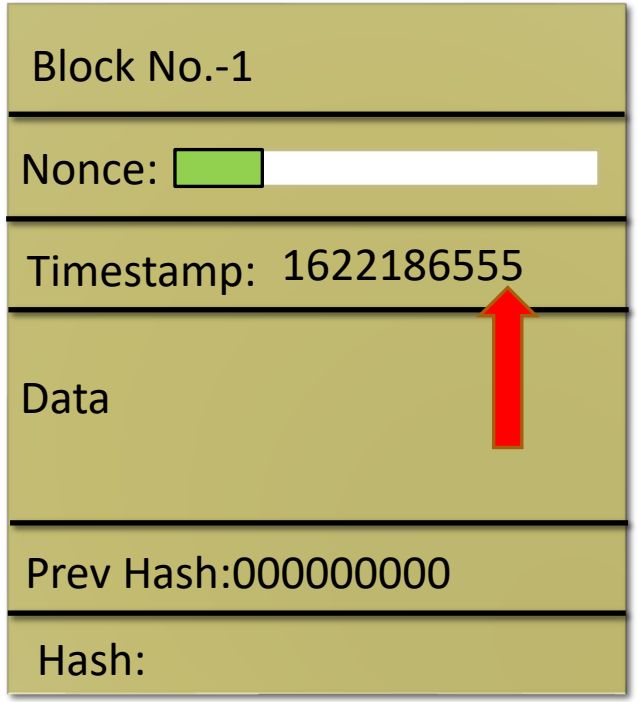
Timestamp



A miner exhaust **4 Billion nonce** in **40 sec**.

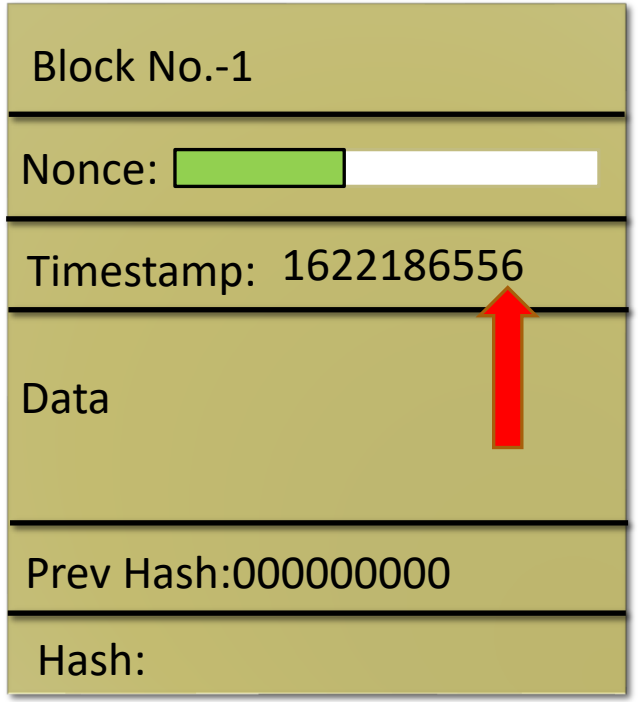
A miner will exhaust 0.1 **Billion nonce** in 1 **sec**.

Timestamp

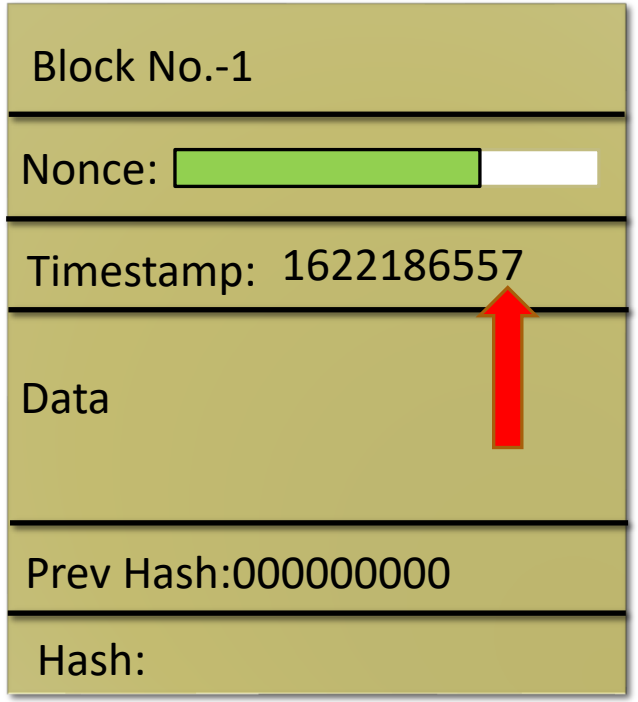


0.5 seconds

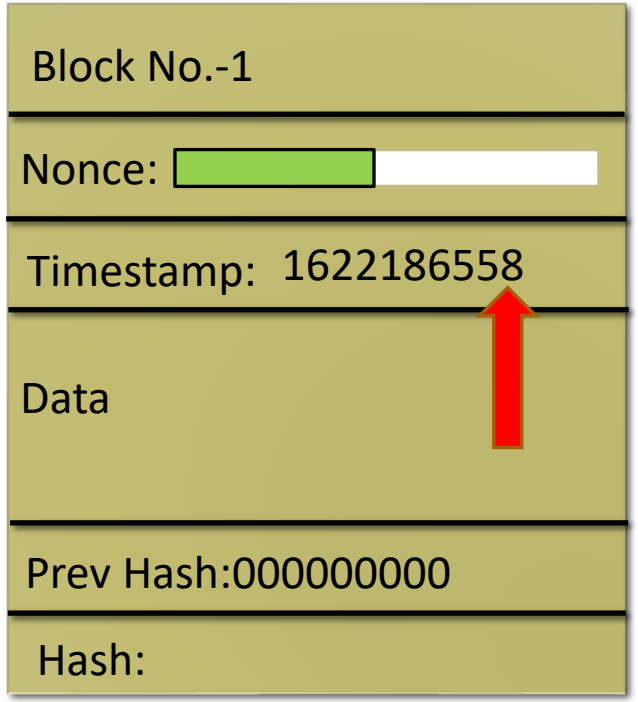
Timestamp


Block No.-1
Nonce:
Timestamp: 1622186556
Data
Prev Hash:000000000
Hash:

Timestamp


Block No.-1
Nonce:
Timestamp: 1622186557
Data
Prev Hash:000000000
Hash:

Timestamp


Block No.-1
Nonce:
Timestamp: 1622186558
Data
Prev Hash:000000000
Hash:

Timestamp

The current hashing rate is 230.88 EH/s equal to **230 million trillion H/s**

Hash rate demonstration

https://www.blockchain.com/charts/hash-rate

230 ignored

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

Now at this rate, before the timestamp changes, all the nonce will be exhausted

New complication arises

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

Mempool

Mempool

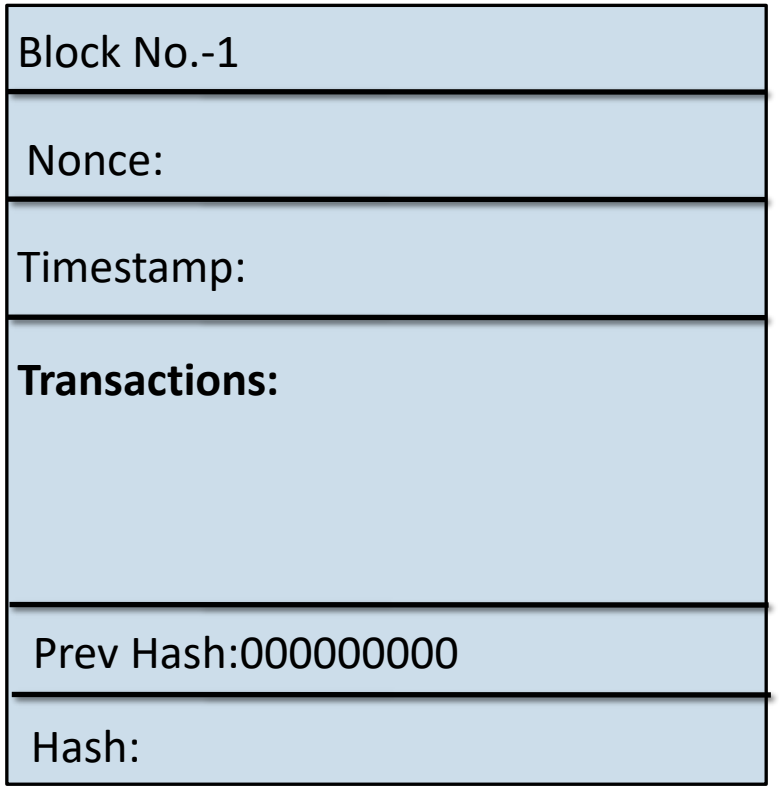
- Mempool is a place where all the unconfirmed transaction resides
- Mempool resides on every node just like blockchain resided on every node

  (Will be covered in detail later)
- Mempool will be used to utilize miners' resources effectively
- Mempool has thousands of unconfirmed transactions, miners get transactions from the pool
- After adding transactions, the miner starts mining to solve the mathematical problem

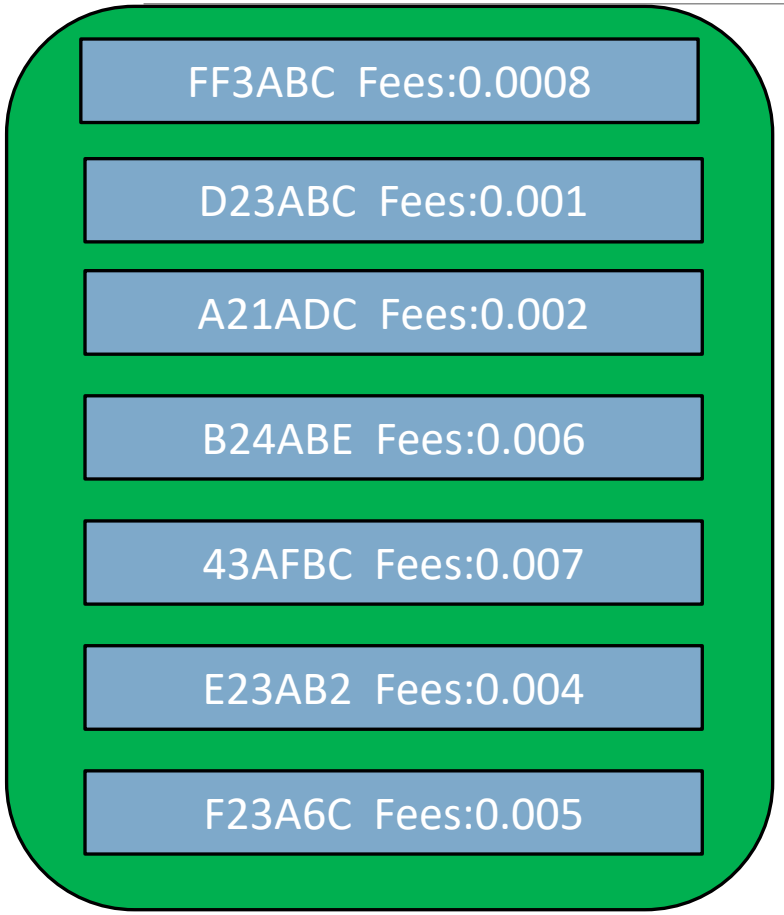
Mempool

- Miner exhausted all nonces in less than a second
- Timestamp is also not changed
- Still valid hash not computed
- Then, the Mempool transaction will be used for changing the hash
- If nonces are exhausted and the timestamp is not changed, the transaction picked will be changed
- Thus, using different transactions, the miner can reuse the nonce from the start

Mempool


Block No.-1
Nonce:
Timestamp:
Transactions:
Prev Hash:000000000
Hash:

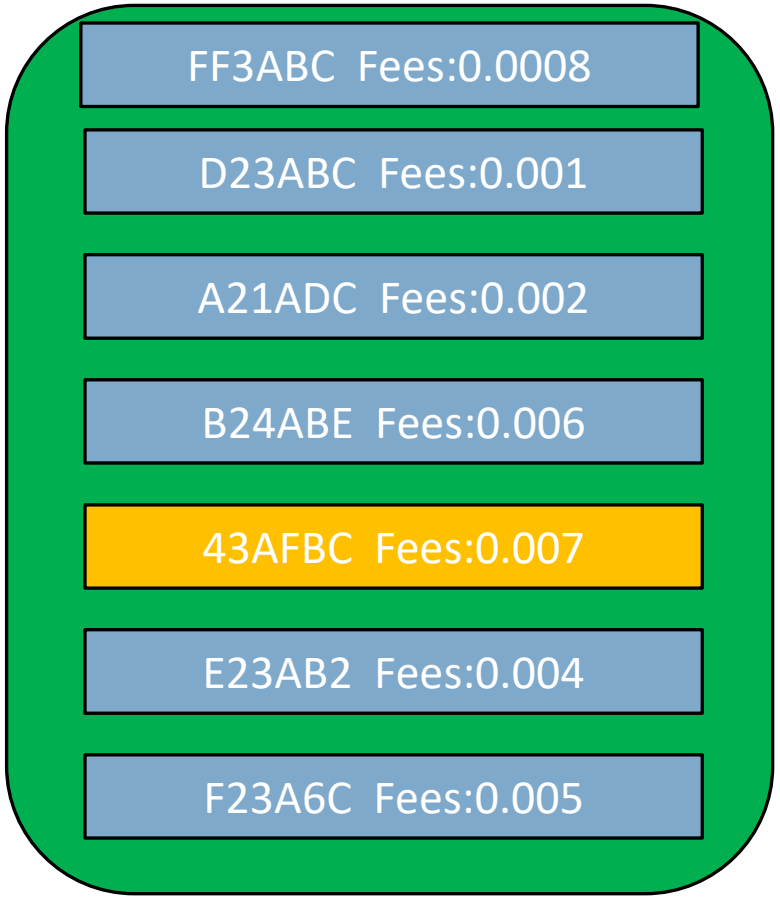
Mempool



Mempool

Block No.-1
Nonce:
Timestamp:
Transactions:
Prev Hash:000000000
Hash:

How actually mining of transaction takes place?



Mempool

Block No.-1

Nonce:

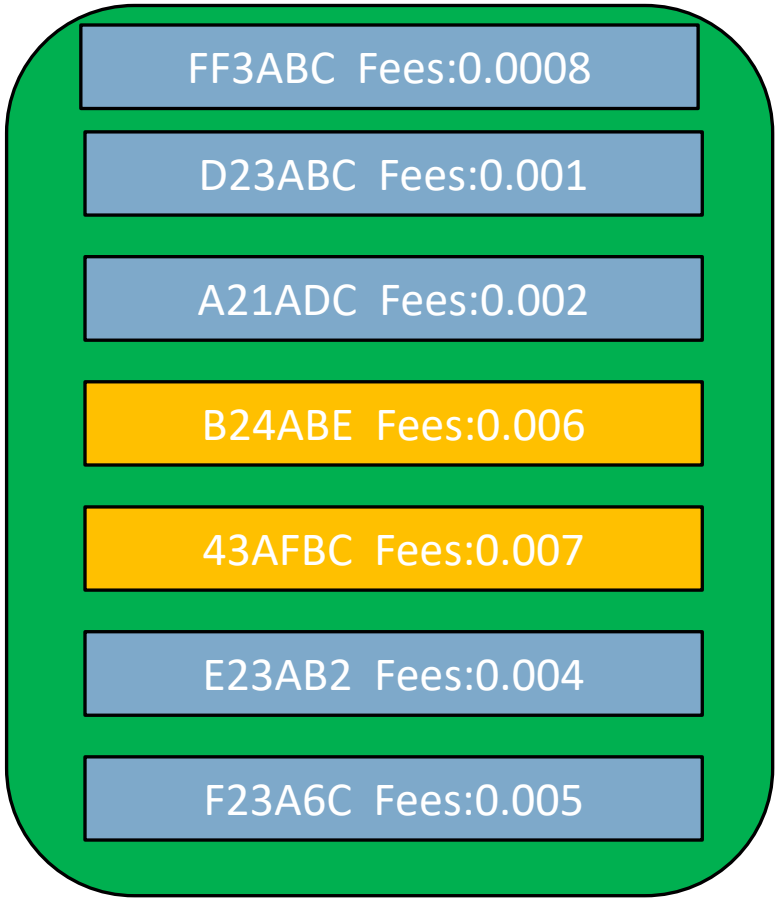
Timestamp:

Transactions:

Prev Hash:000000000

Hash:

How actually mining of transaction takes place?



Mempool

Block No.-1

Nonce:

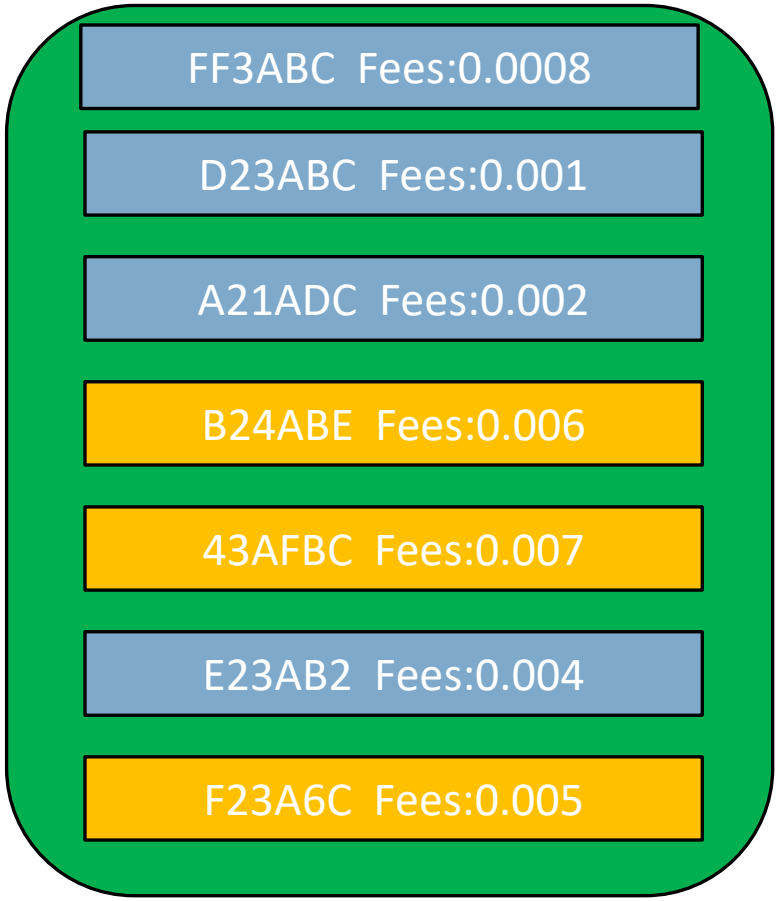
Timestamp:

Transactions:

Prev Hash:000000000

Hash:

How actually mining of transaction takes place?



Mempool

Block No.-1

Nonce:

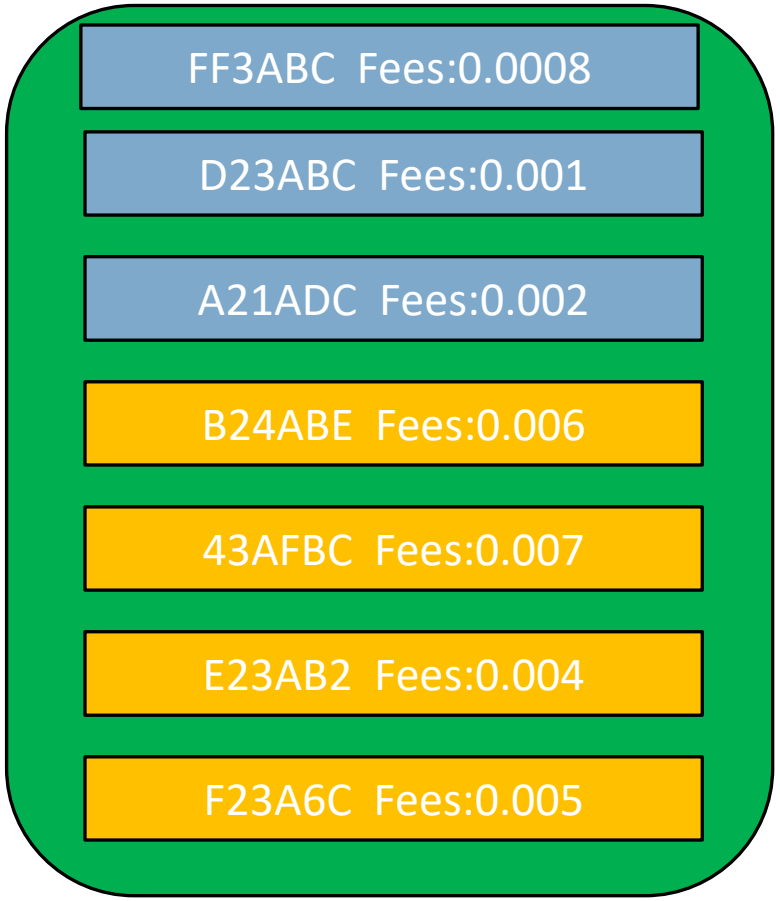
Timestamp:

Transactions:

Prev Hash:000000000

Hash:

How actually mining of transaction takes place?



Mempool

Block No.-1

Nonce:

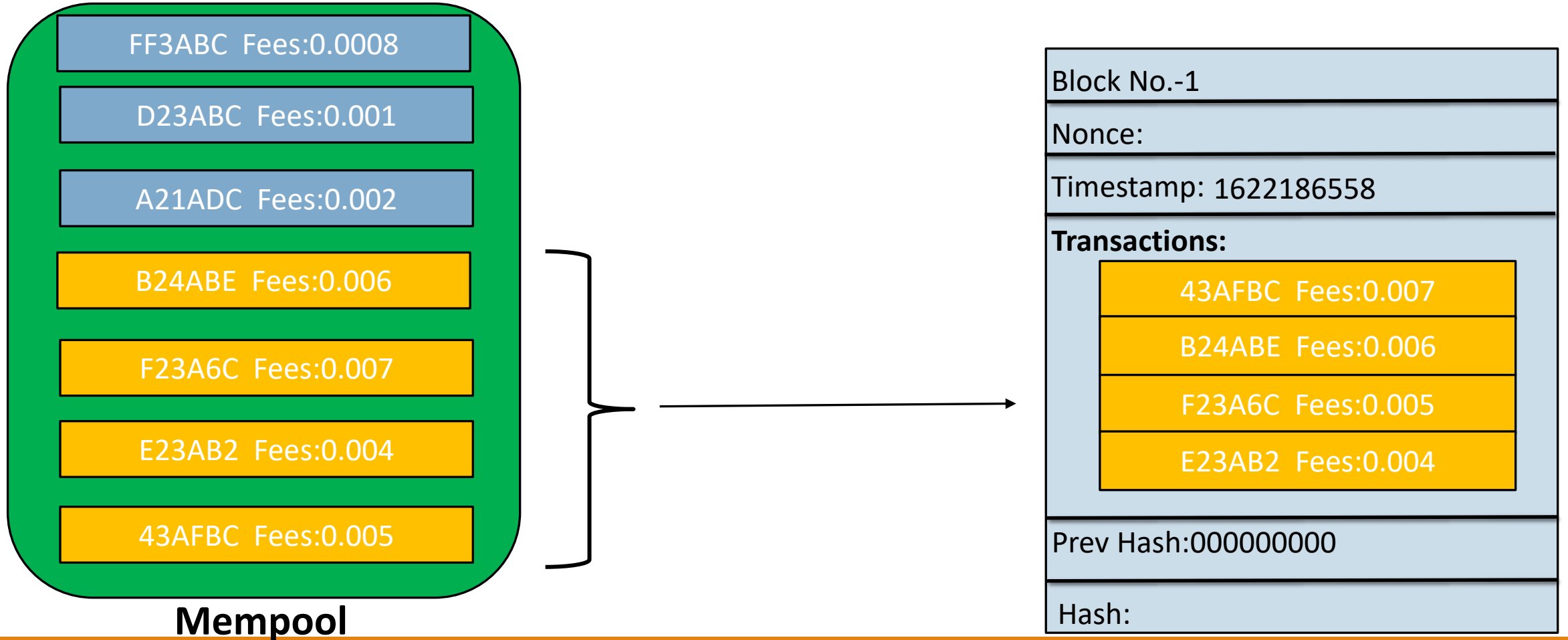
Timestamp:

Transactions:

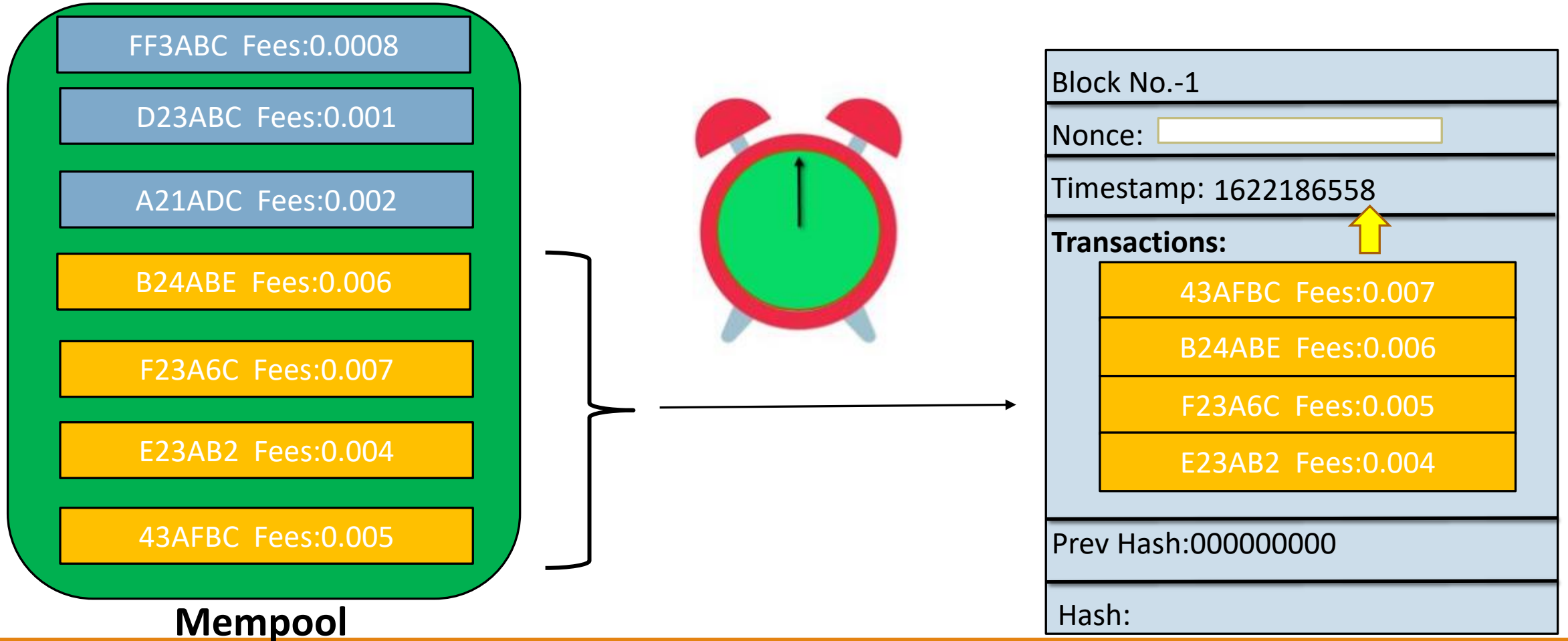
Prev Hash:000000000

Hash:

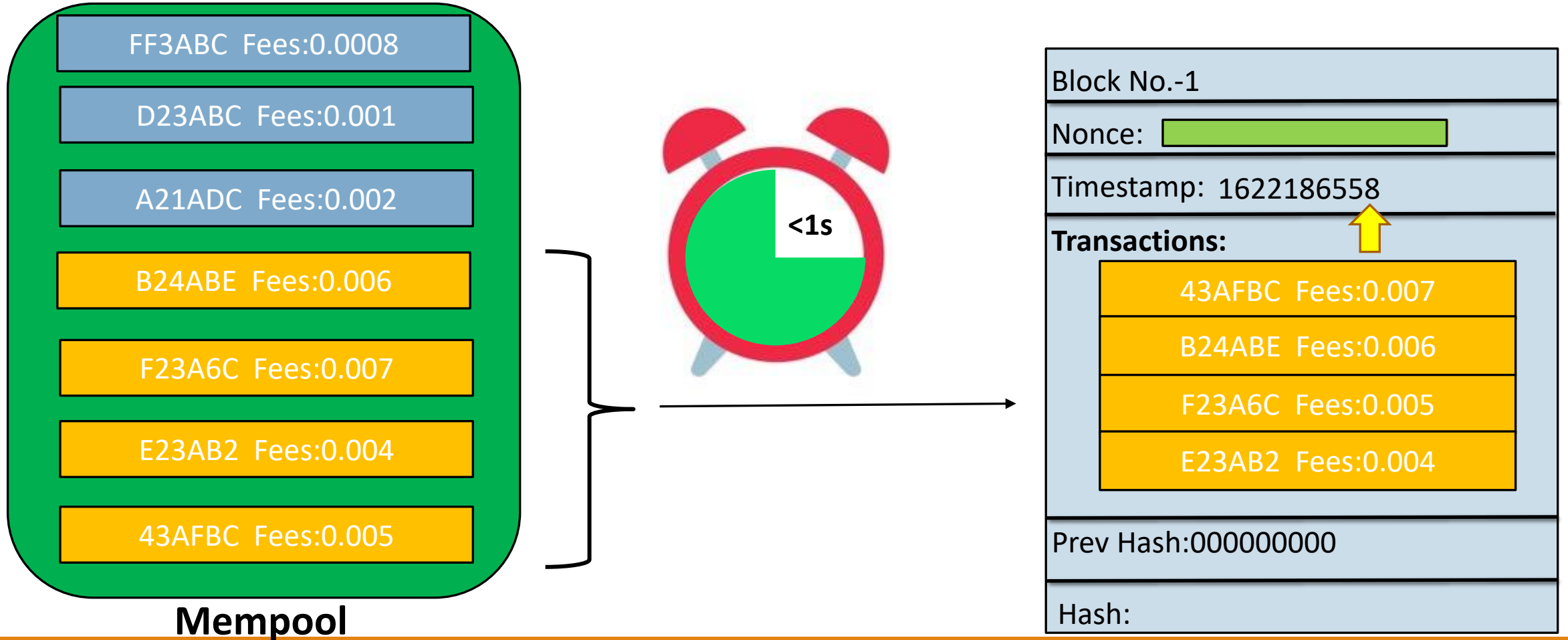
How actually mining of transaction takes place?



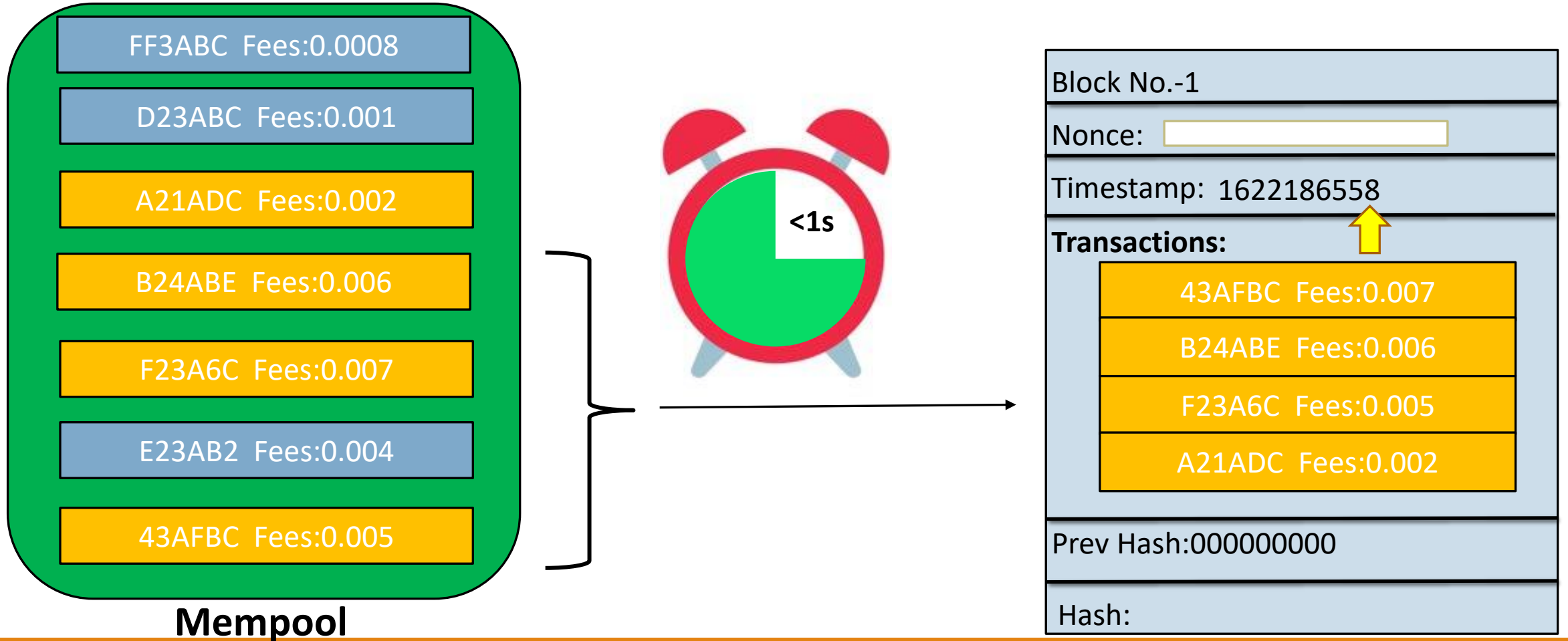
How actually mining of transaction takes place?



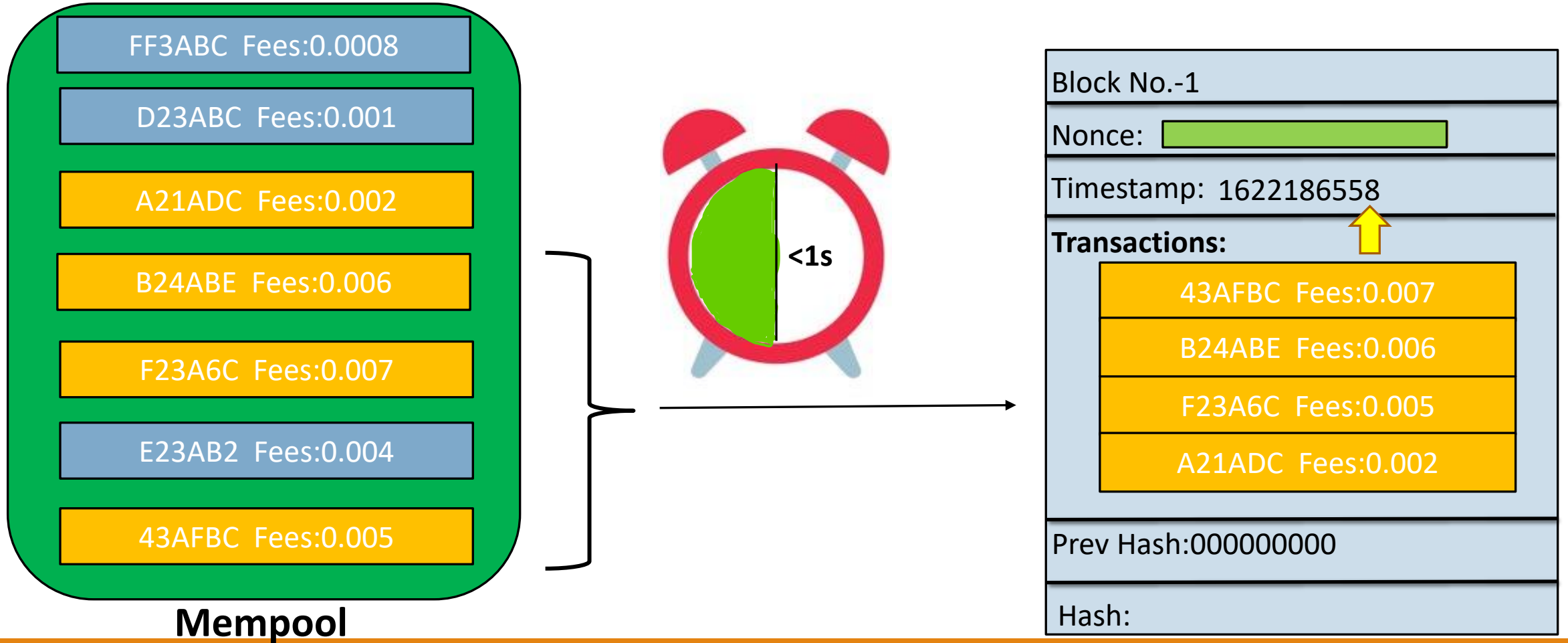
How actually mining of transaction takes place?



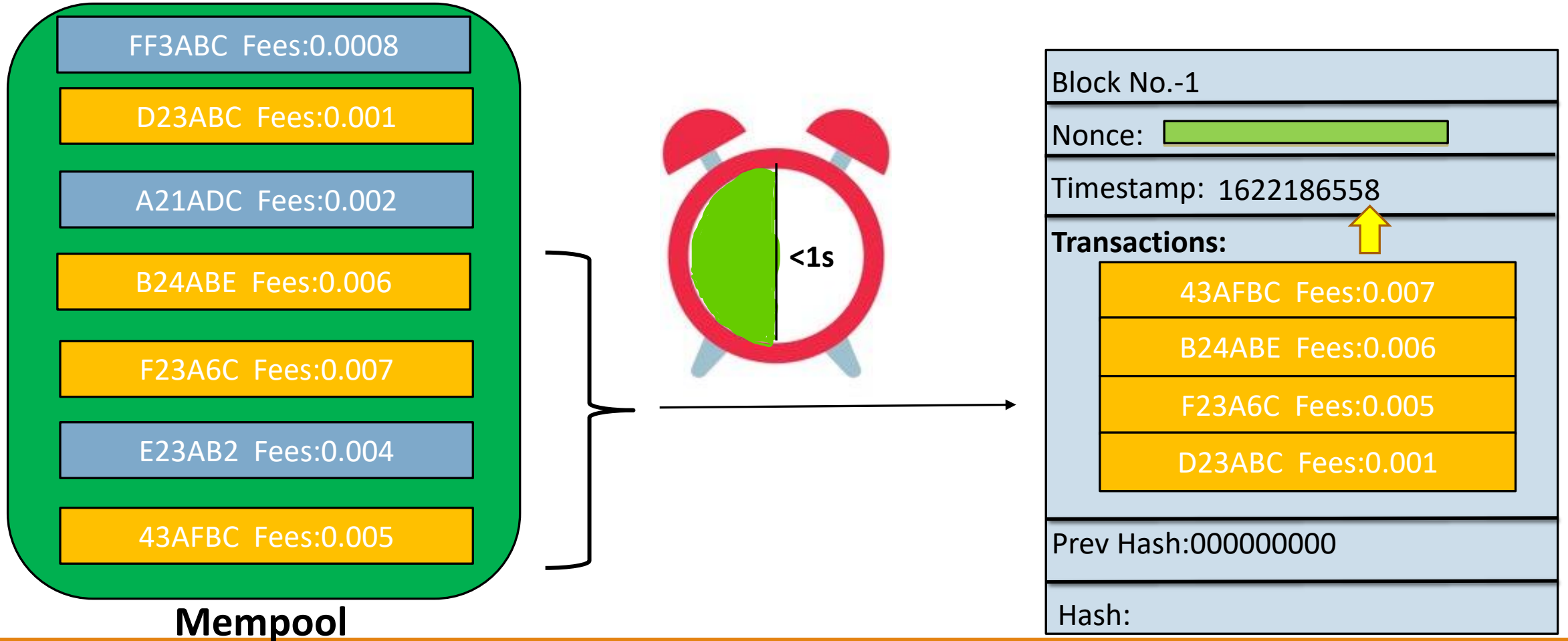
How actually mining of transaction takes place?



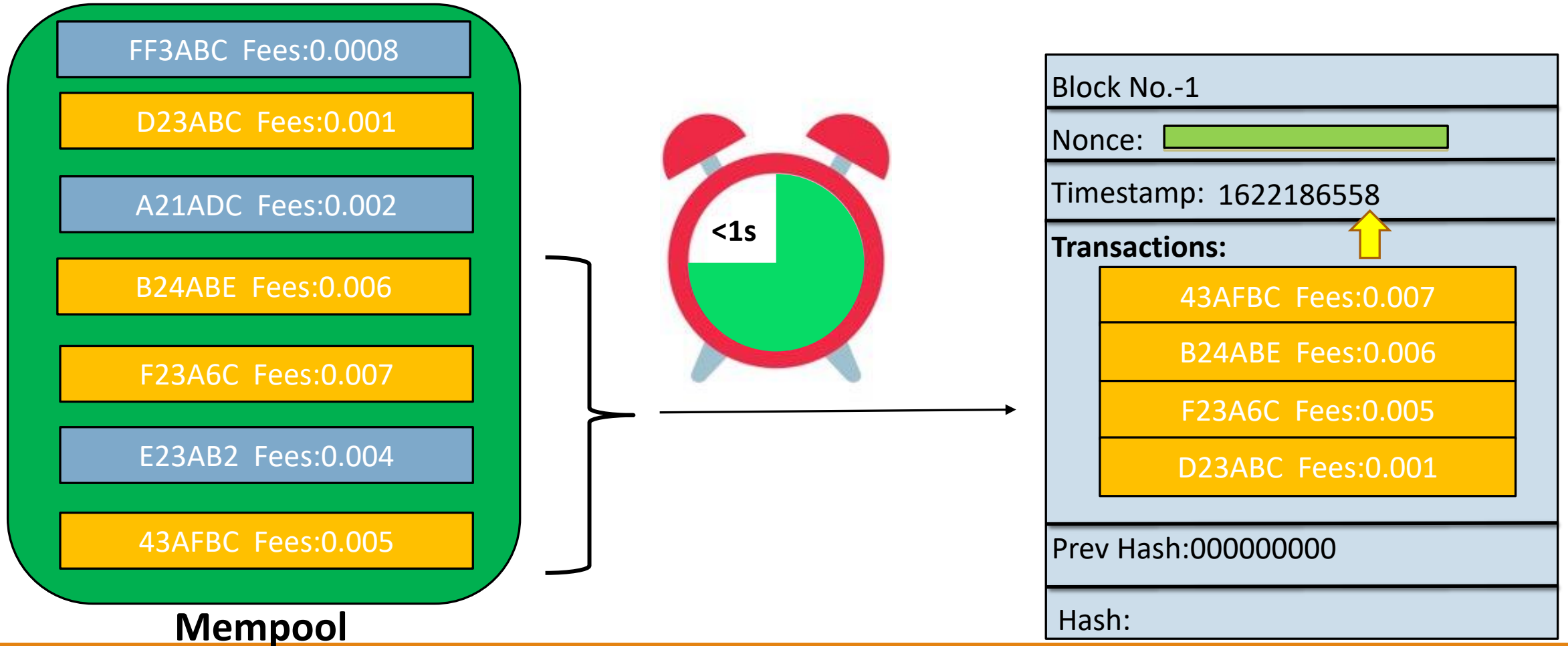
How actually mining of transaction takes place?



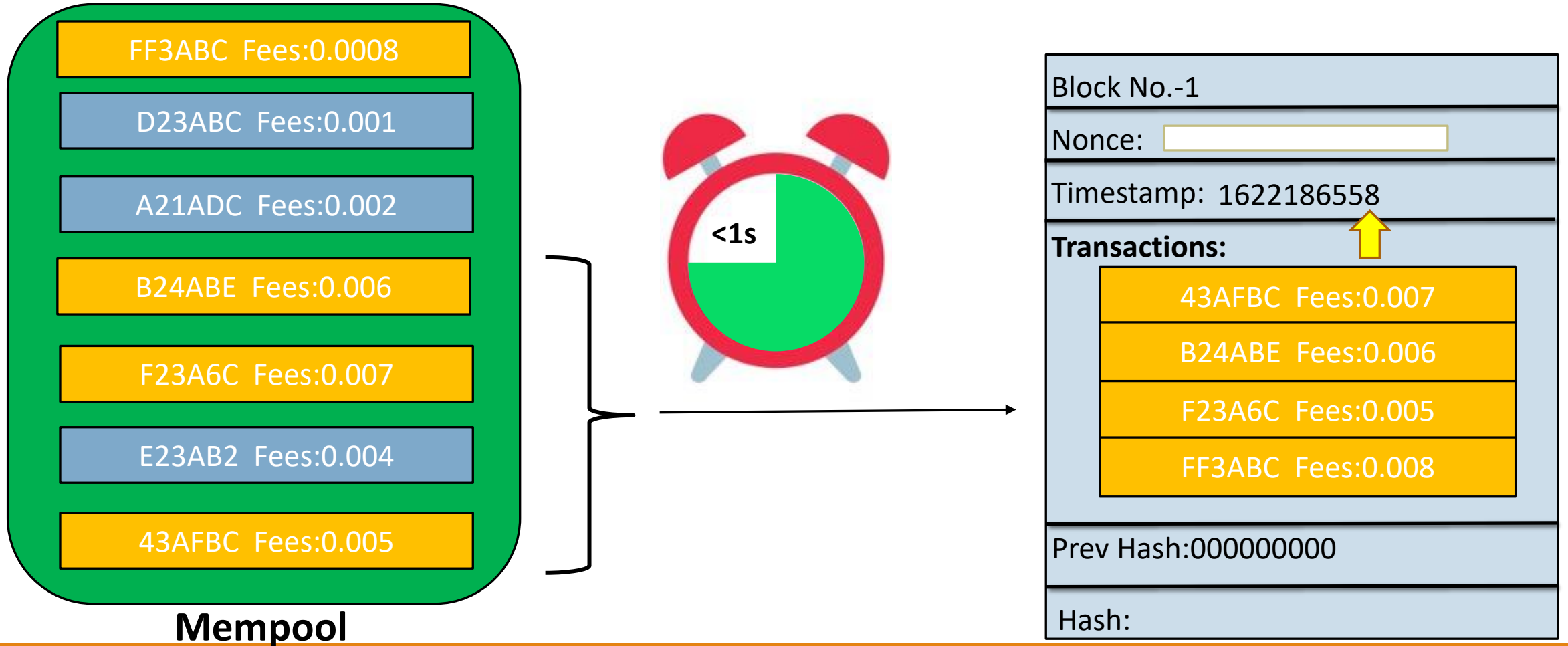
How actually mining of transaction takes place?



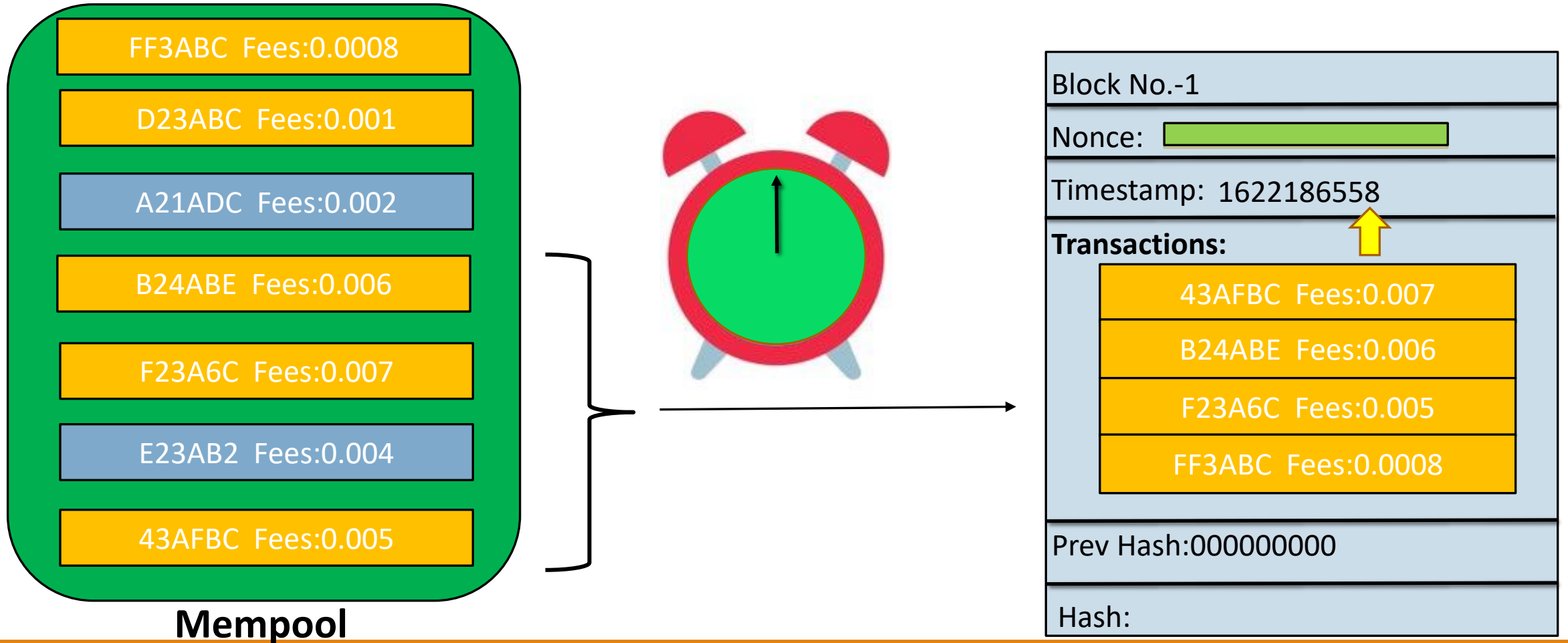
How actually mining of transaction takes place?



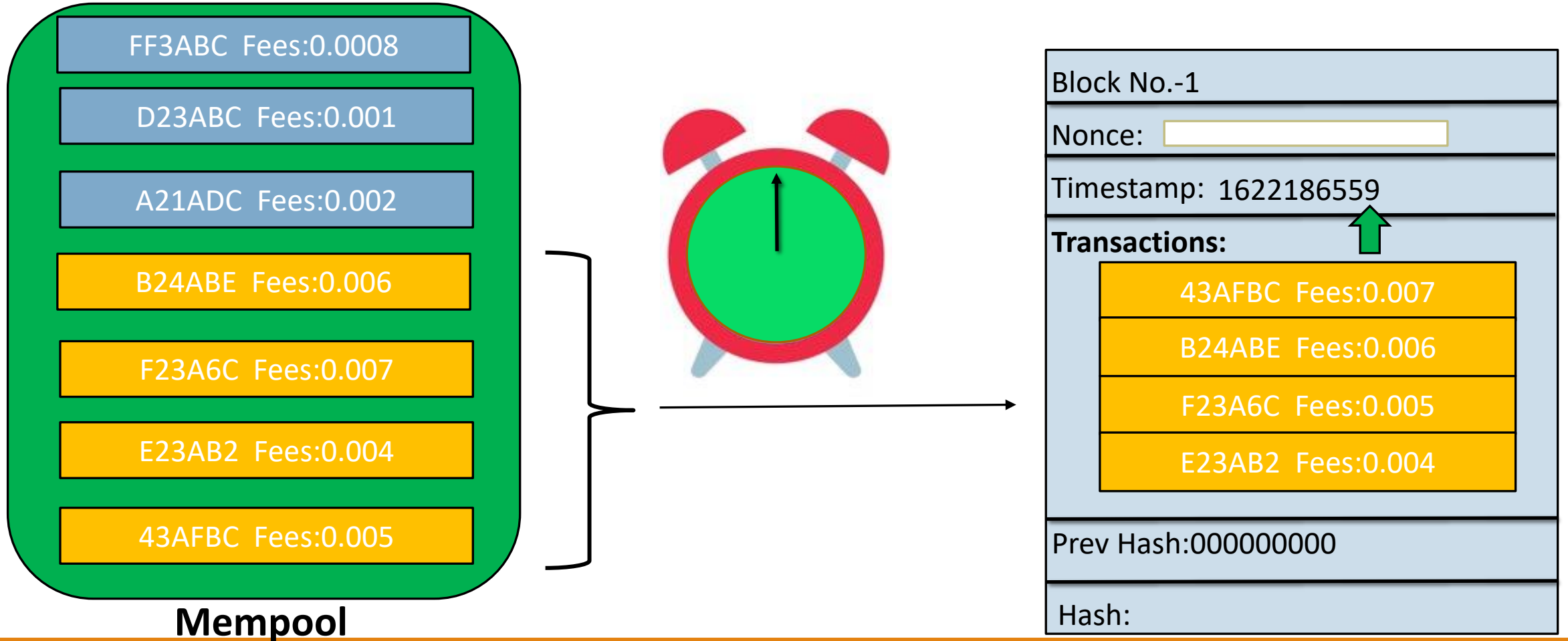
How actually mining of transaction takes place?



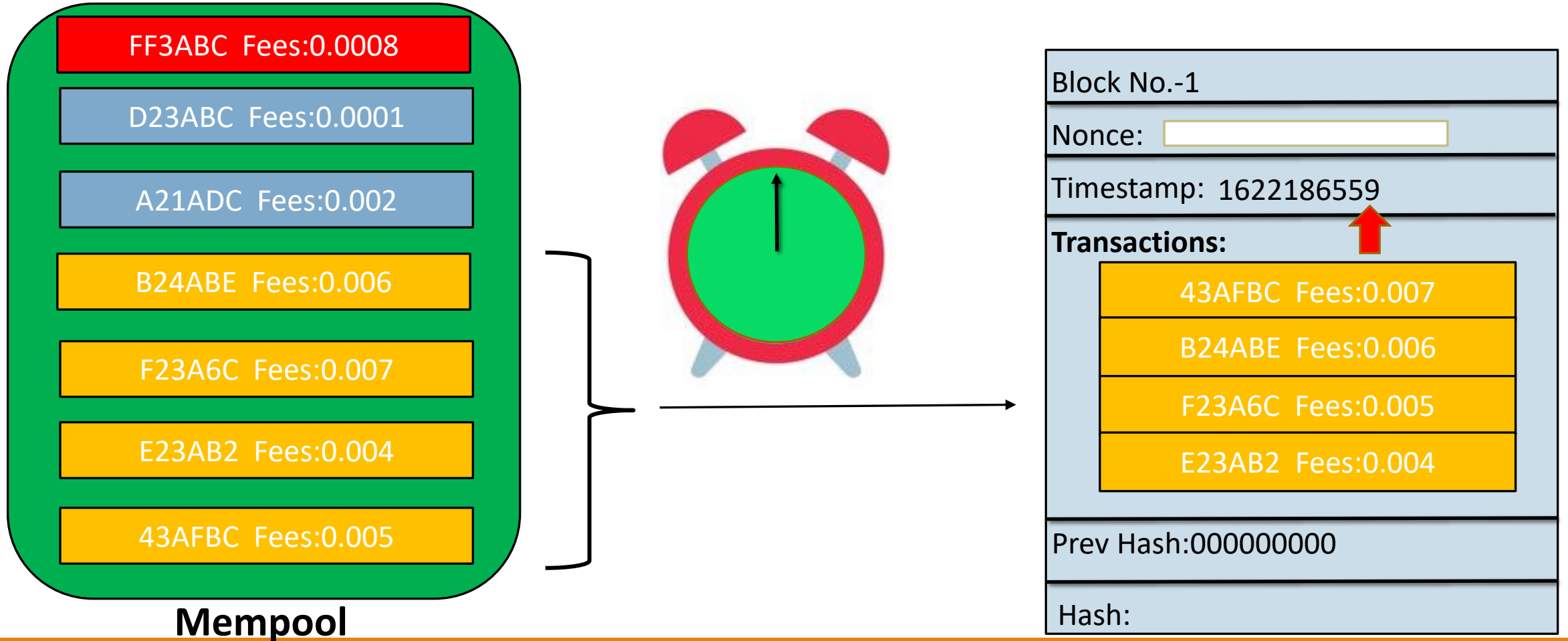
How actually mining of transaction takes place?



How actually mining of transaction takes place?



How actually mining of transaction takes place?



Mempool

- Generally, the miners pick transactions with high fees
- If a transaction is assigned minimum fees, then there is a chance that the transaction will not be picked by any miners
- A transaction is removed from the pool after 72 hours