Bitcoin

What is Bitcoin?

Nonce

Transactions

Bitcoin's Monetary Policy

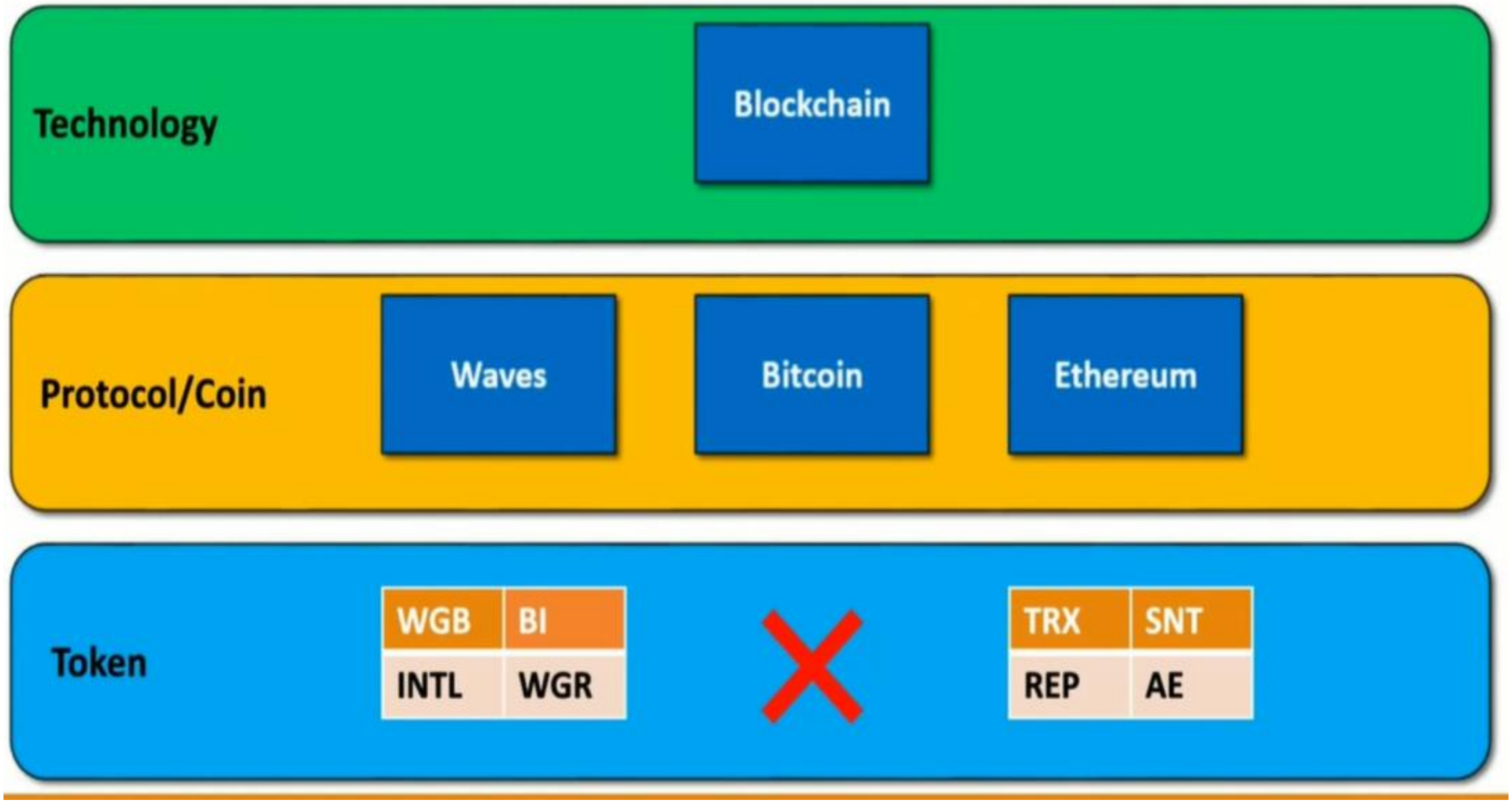
CPU's vs GPU's vs ASICs

Wallets

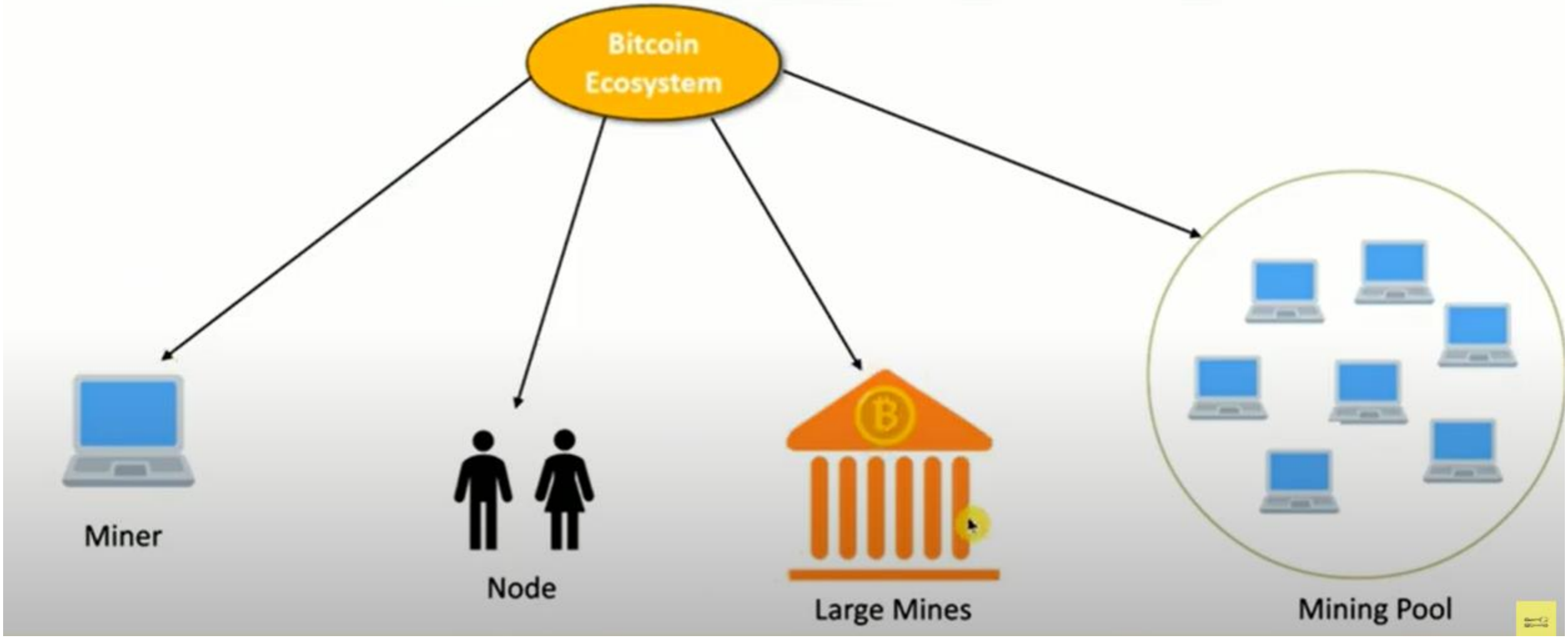
Mining

Mempool

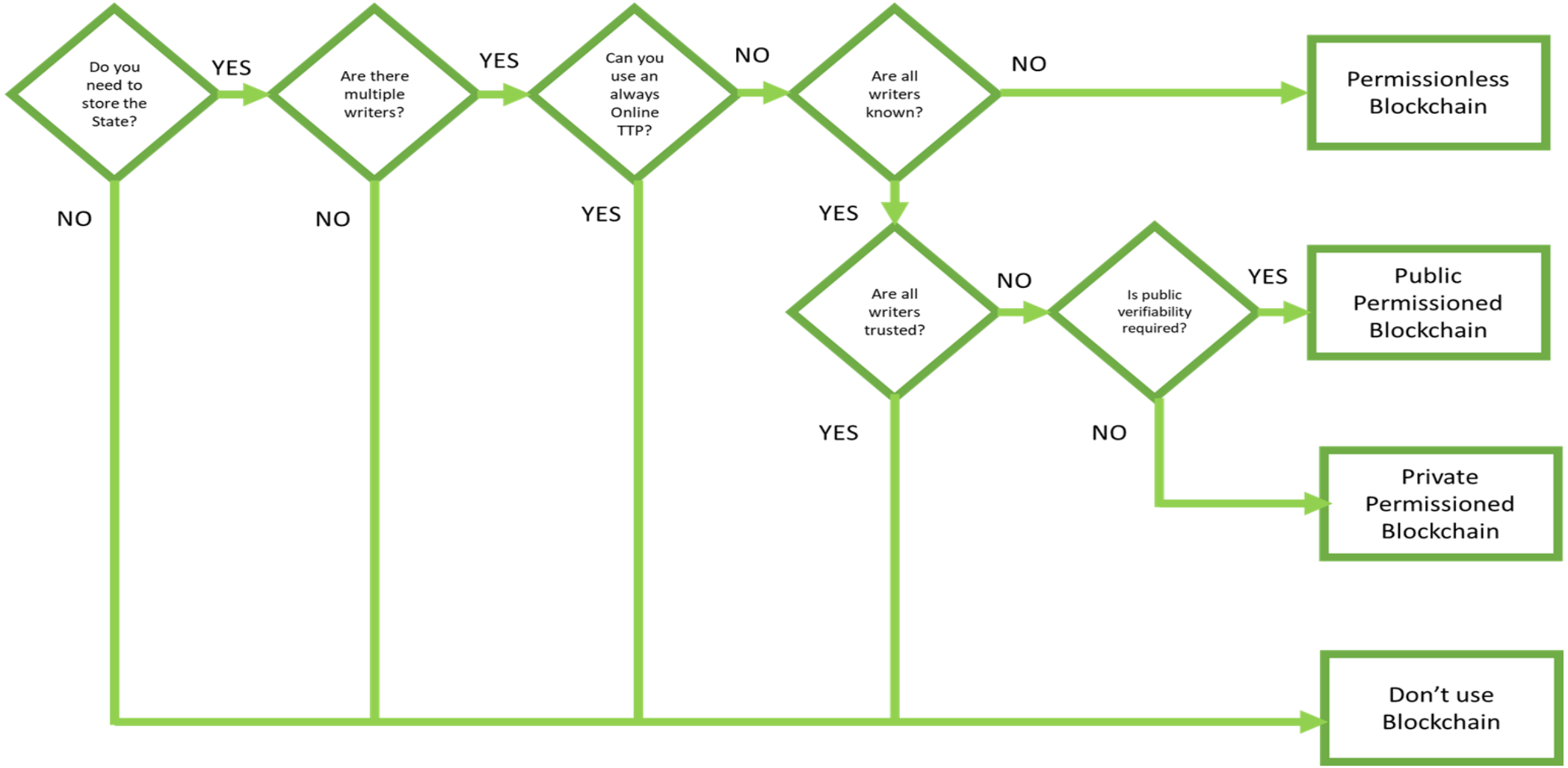
Public Key and Private Key


Technology
Blockchain
Protocol/Coin
Waves
Bitcoin
Ethereum
Token
WGB
BI
INTL
WGR
TRX
SNT
REP
AE

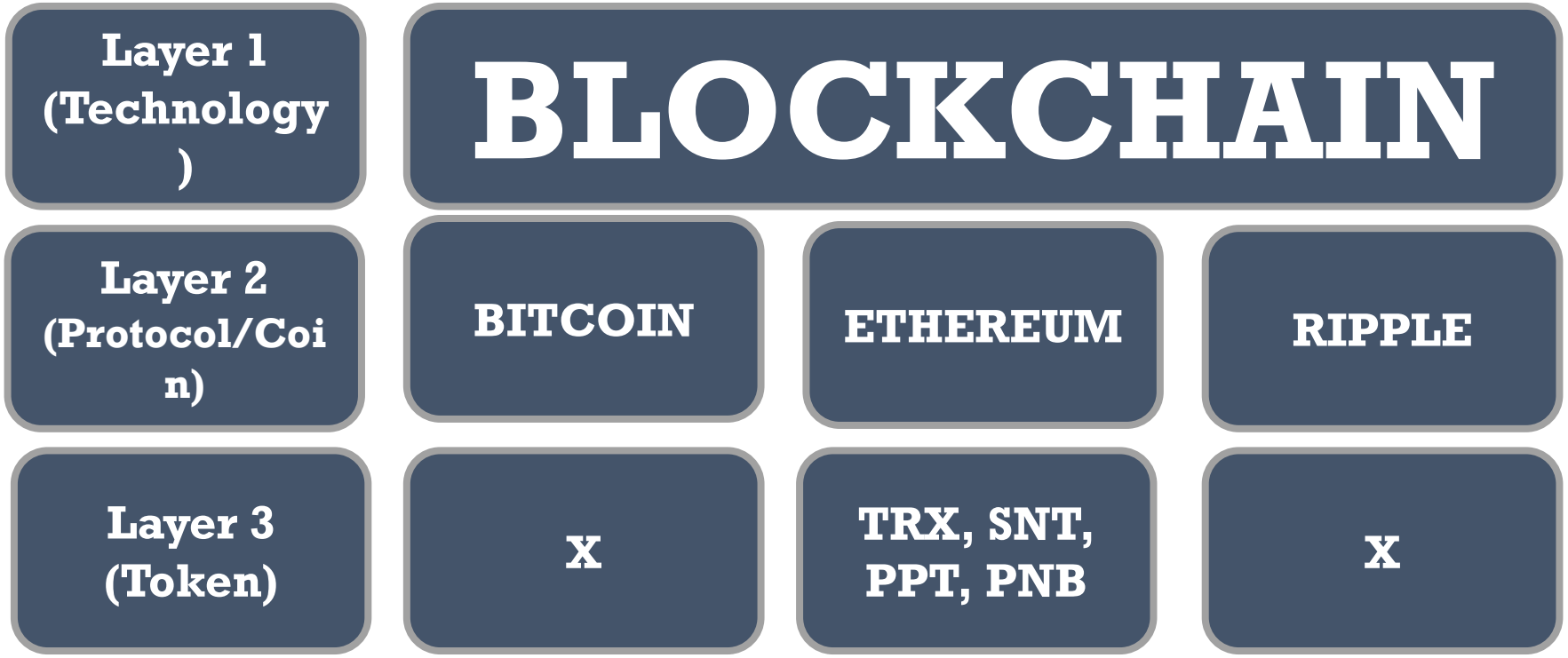
Bitcoin Ecosystem



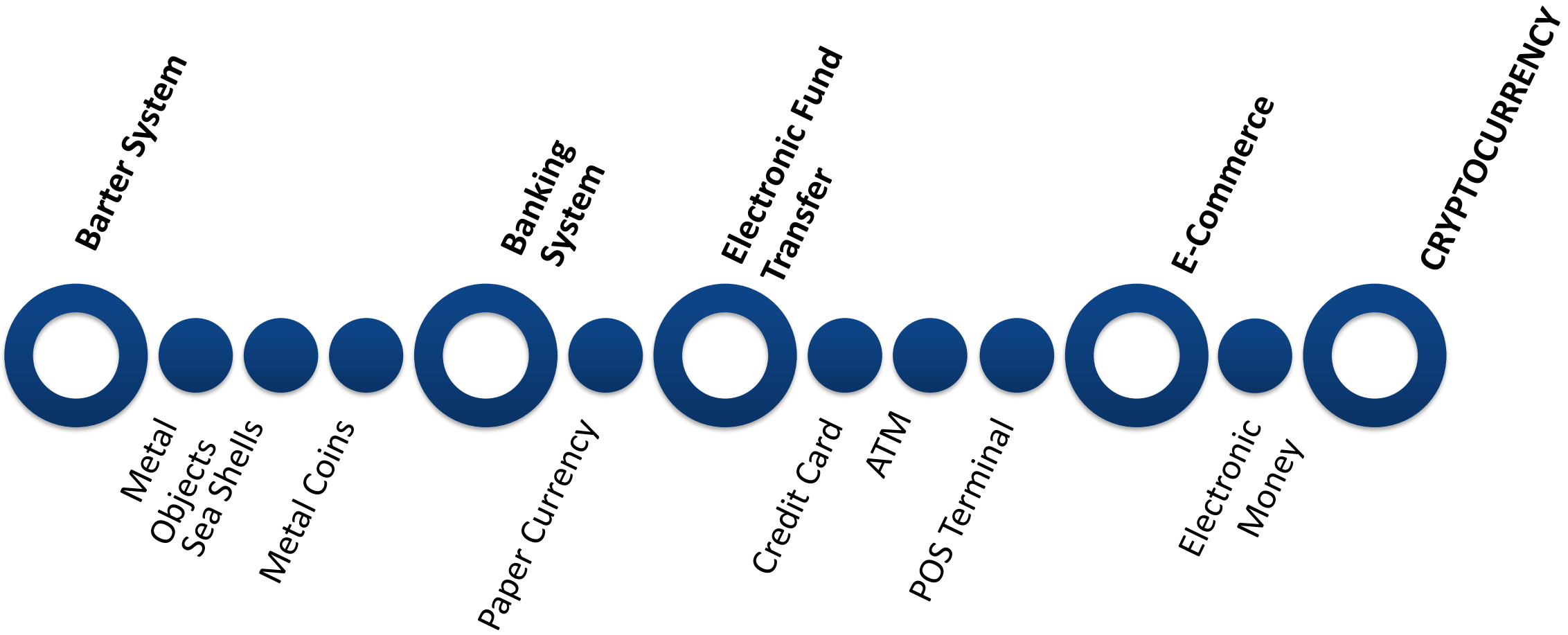
Blockchain


Do you need to store the State?
YES
Are there multiple writers?
YES
Can you use an always Online TTP?
NO
Are all writers known?
NO
Permissionless Blockchain
NO
NO
YES
YES
Are all writers trusted?
NO
Is public verifiability required?
YES
Public Permissioned Blockchain
YES
NO
Private Permissioned Blockchain
Don't use Blockchain

Blockchain Layers



Evolution of Currency



Banks acted as the ultimate gatekeepers of the financial world and charged fees for the services that they provided. This monopoly, however, had its disadvantages, especially for people in lower-income groups who did not have accounts or IDs or instances where the transaction fees took a toll on their earnings.

Financial institutions incur significant costs related to back-office expenses, reconciliations, legalities, secure data storage, prevention measures for security breaches, and potentially fraudulent activities. These costs are passed down to the end-users as fixed transaction fees irrespective of the size of the transaction.

There was also the question of transparency. People deposit money, trusting the banks to keep them safe. However, these deposits are used by banks to find opportunities for additional financial returns like extending mortgage and other loans, and investments. When people defaulted on loan payments and the investments the banks made did not pay off, the banks declared bankruptcy. The result was that while the Government bailed out many of the financial institutions, the depositors lost all the money that they trusted the banks to keep safe, as was seen during the financial crisis of 2008.

Birth of Bitcoin (Contd.)

Three key requirements eventually brought about the birth of the Bitcoin. The need was felt for a monetary system

- where one can directly transact with another person without involving a third party, like a bank, to verify and validate the transaction and thus avoiding the cost of mediation.
- that is not backed and controlled by a central authority and can assure the value of the money is maintained
- where there is transparency in transactions, while still maintaining the users' privacy

What is Cryptocurrency?

A cryptocurrency is a digital asset that is used as a medium of exchange on the blockchain. The most popular cryptocurrency is Bitcoin, followed by Ether of Ethereum and Ripples XRP tokens.

Since the creation of the first decentralized cryptocurrency Bitcoin, thousands of alternative digital currencies have emerged that are referred to as altcoins or coins (used for buying or selling products or services) and tokens (used as a utility or security).

According to CoinMarketCap, there are over 3000 active cryptocurrencies as of October 2019.

Characteristics of Crypto Currency

- Decentralized
- Form of existence
- Limited supply
- Global Access
- Anonymity & transparency
- Impossible to duplicate
- Irreversible

Cryptocurrency Wallets

Bitcoin or any other cryptocurrency transaction can be done only using a digital wallet. A digital wallet or **cryptocurrency wallet** is a software program that stores the user's private and public keys enabling the user to transact crypto assets.

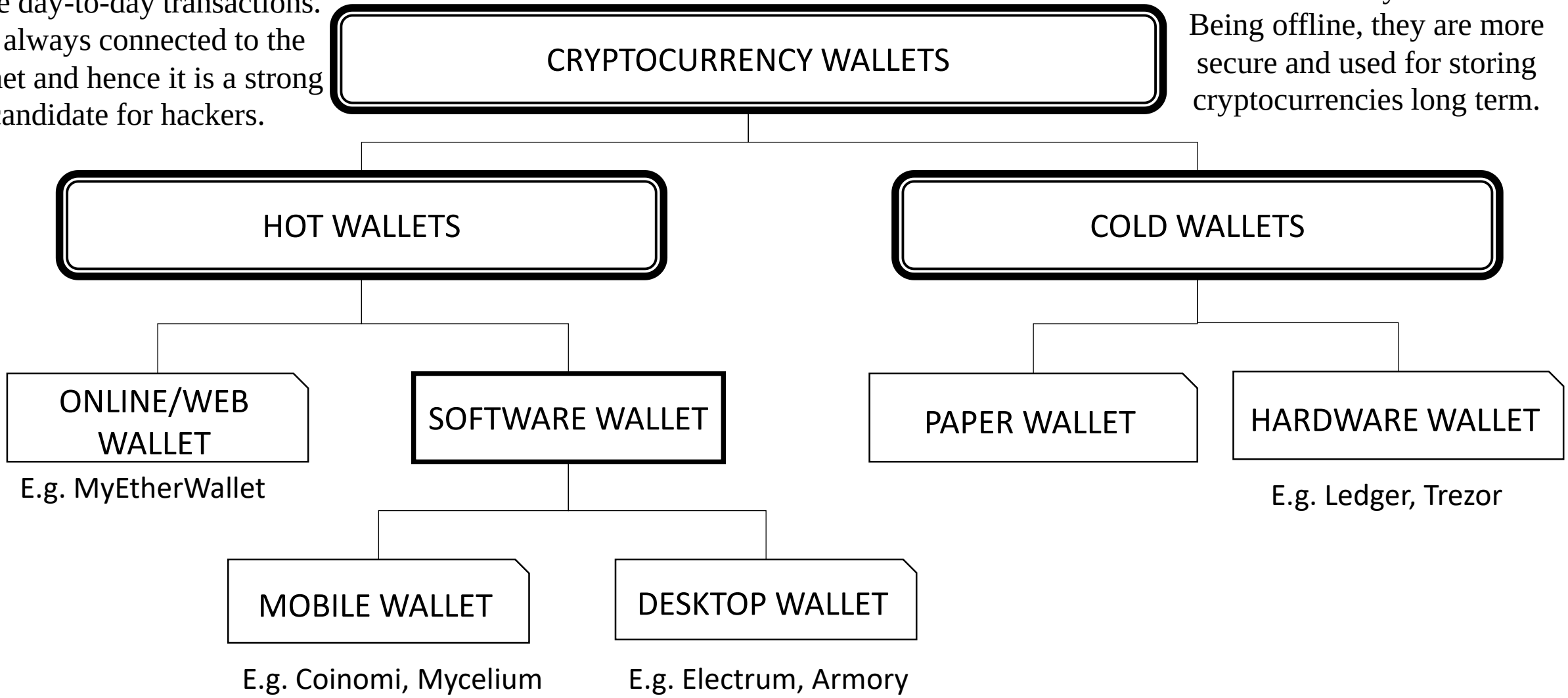
It is a management system that interacts with various blockchains to enable users to send and receive digital currency and monitor their balance.

Cryptocurrencies are stored immutably on the blockchain using your public key, i.e., your public key is used by other wallets to send funds to your wallet's address. However, the private key is required if you want to spend cryptocurrency from your address.

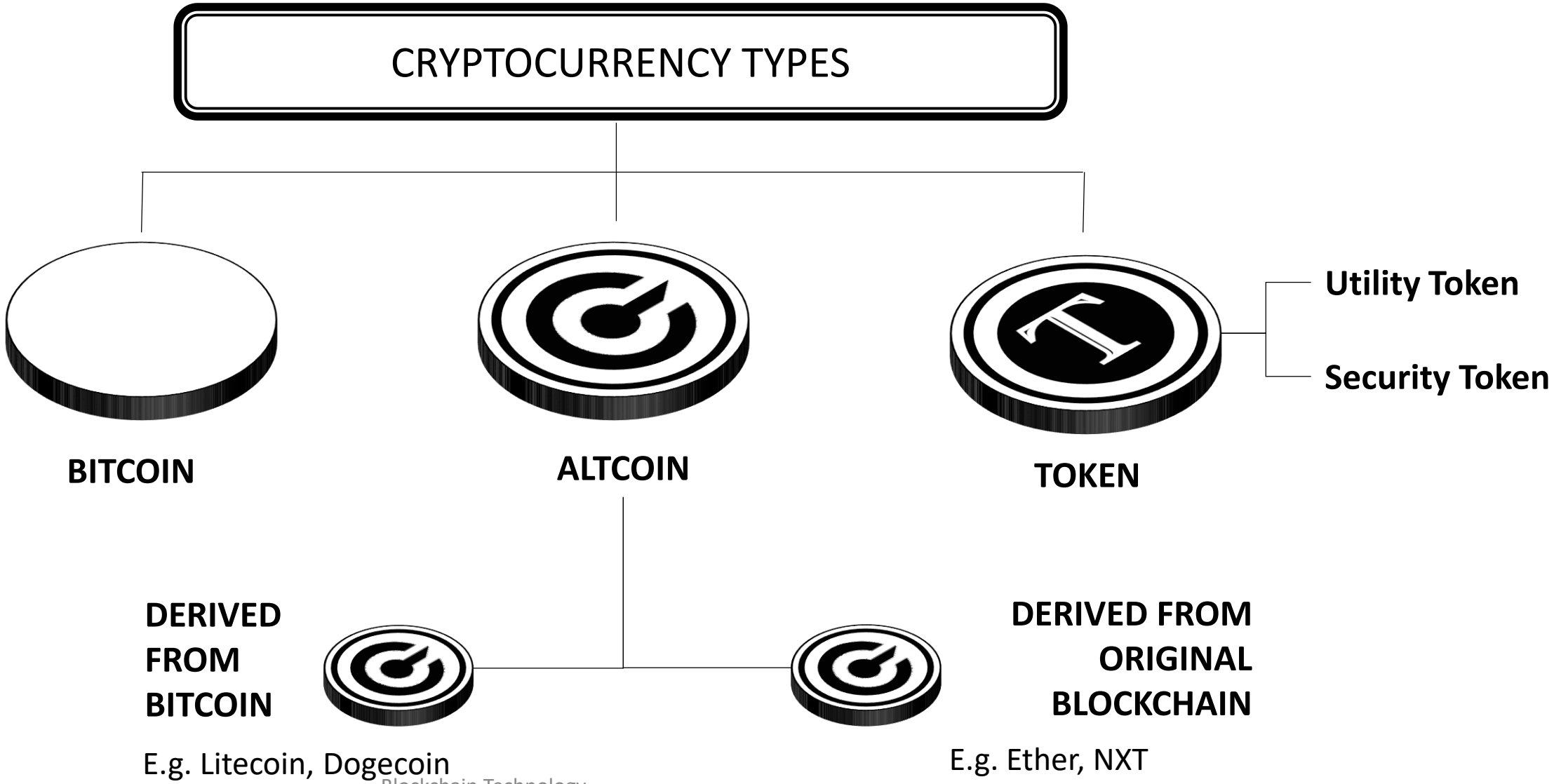
Types of Wallets

A hot wallet is designed for online day-to-day transactions. It is always connected to the internet and hence it is a strong candidate for hackers.

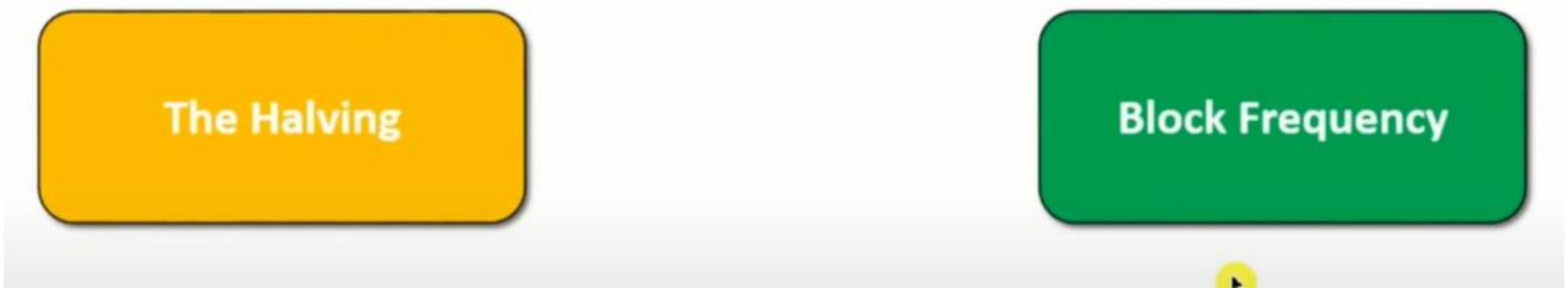
A cold wallet is a digital wallet that is not connected to the internet. They are not free. Being offline, they are more secure and used for storing cryptocurrencies long term.



Cryptocurrency Types



Bitcoin Monetary policy



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

Note- Supply cap of Bitcoin is 21 million.

Block Frequency

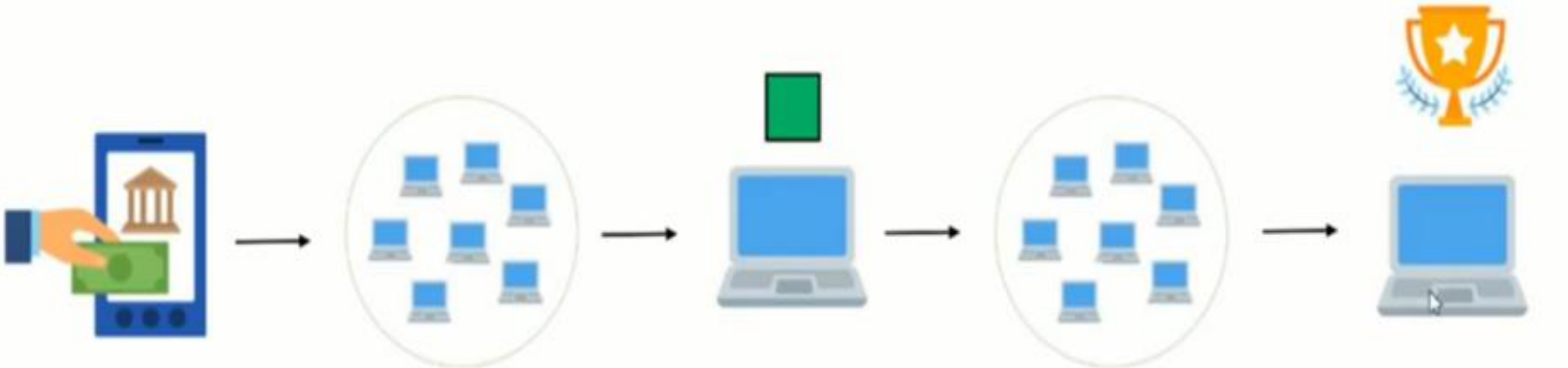
This states that on an average it will take 10 minute to create a new block.

For more refer

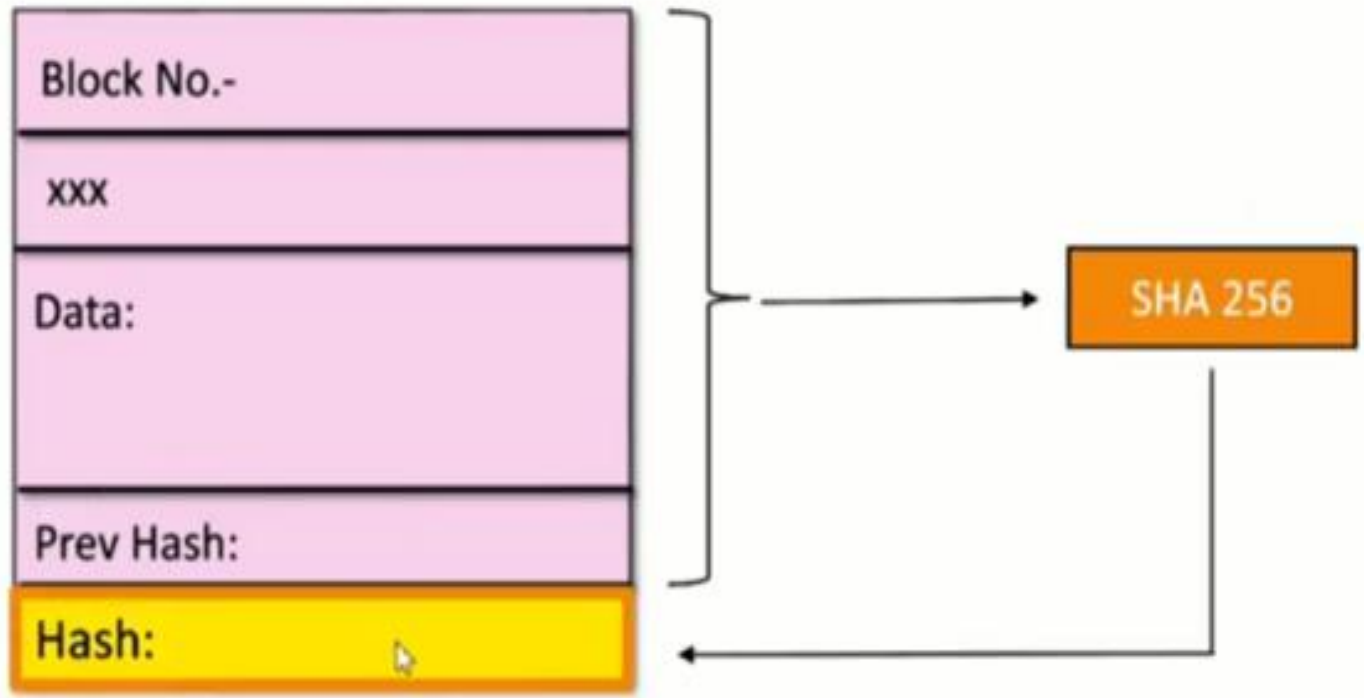
https://www.blockchain.com/

How Mining works: The Nonce

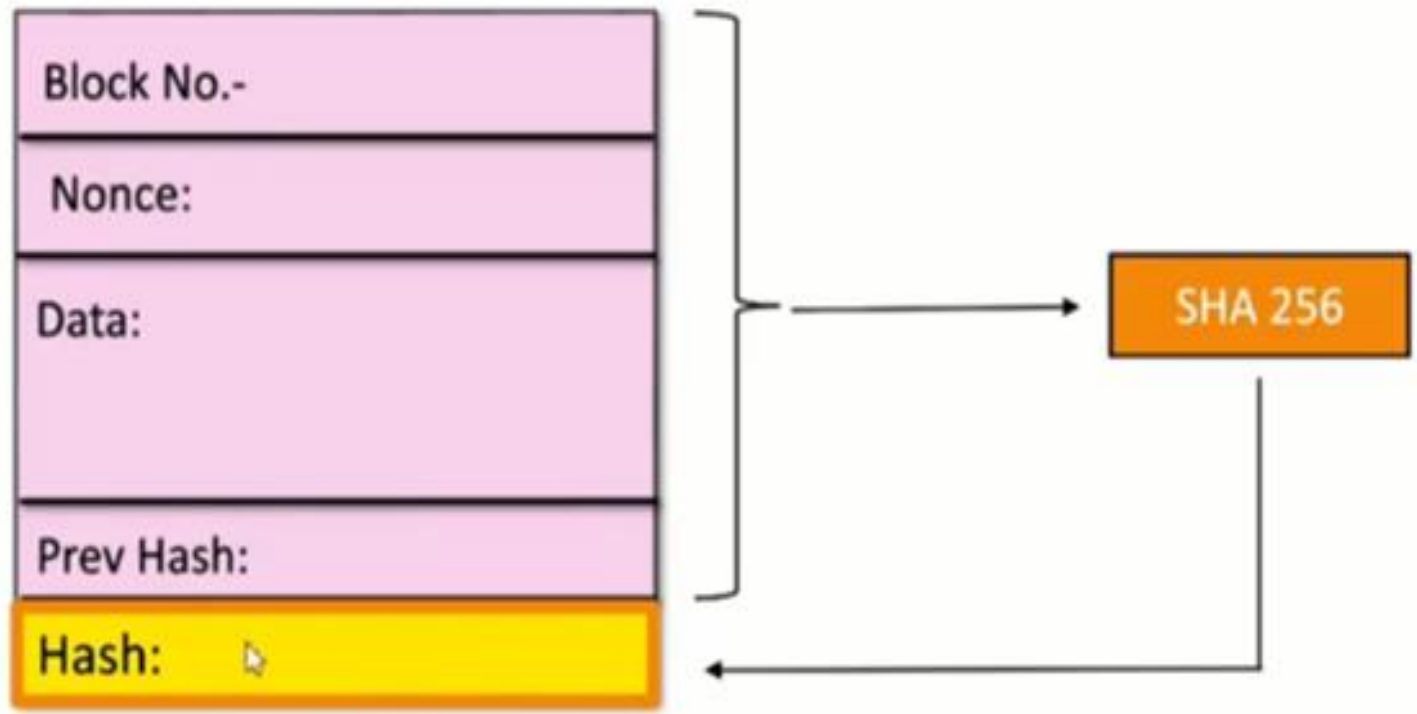
Blockchain Mining



The Nonce



The Nonce



The Nonce


Block No.- 6
Nonce:
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash:

The Nonce


Block No.- 6
Nonce: 50
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000fb12

The Nonce


Block No.- 6
Nonce: 1001
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000ef23

https://demoblockchain.org/block

Mining Pools

How Mining Works ?

How Mining Works ?

Nonce:

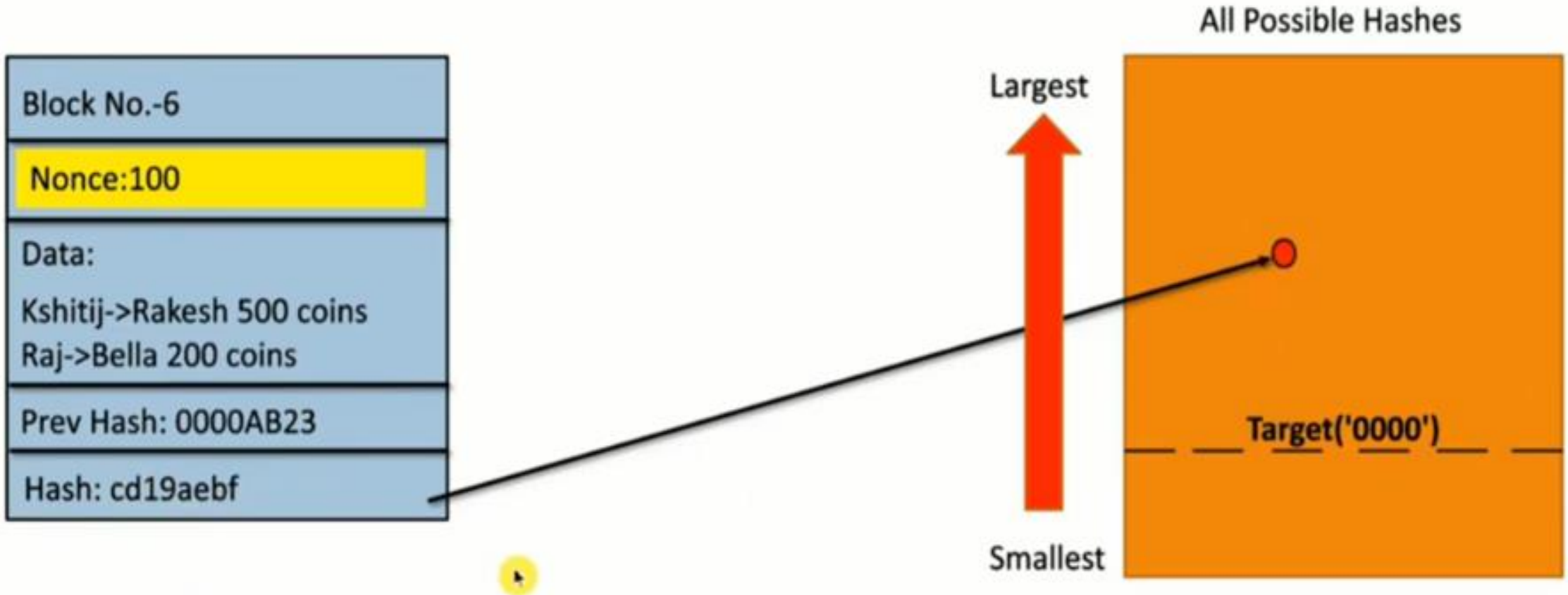
- The nonce is the number that blockchain miners are solving for.

How Mining Works ?

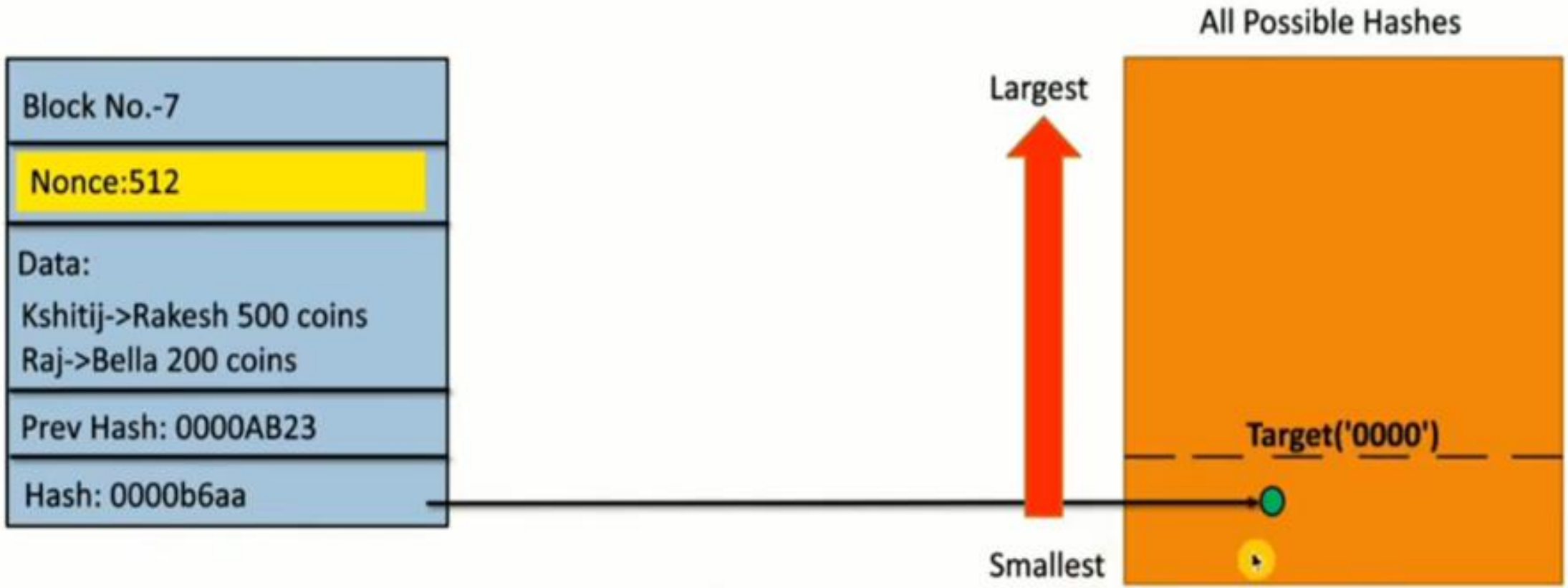
Target:

- 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.

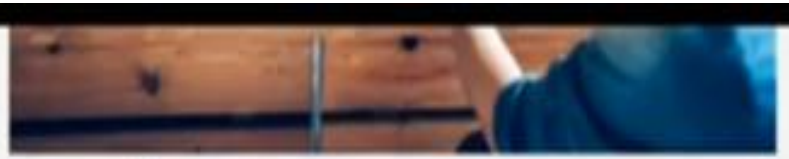
How Mining Works ?



How Mining Works ?





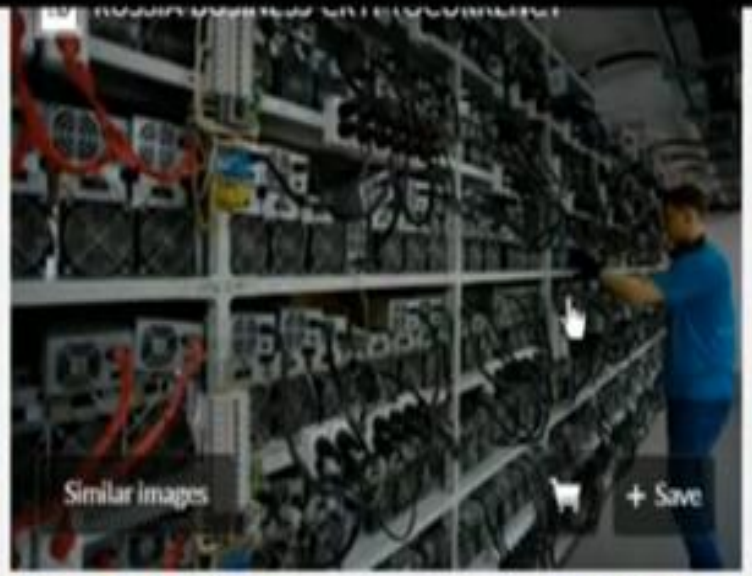


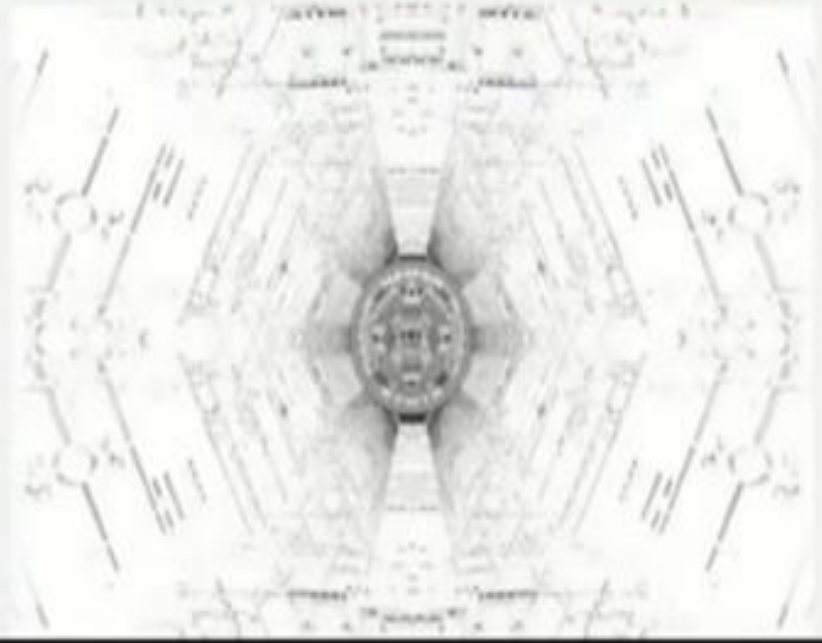

INDUSTRY ICONS
EDITABLE SMART STROKE



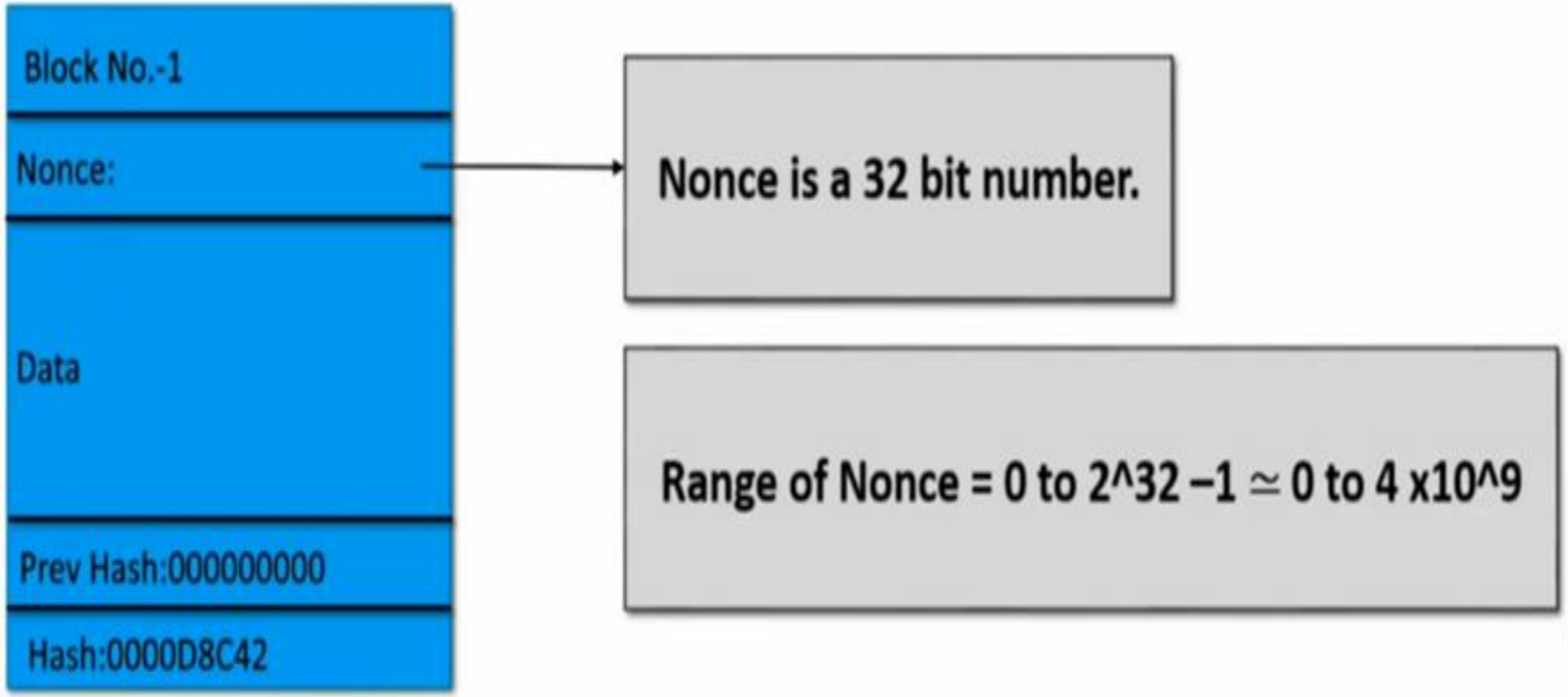


Similar images
+ Save



Similar images
+ Save



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

Nonce Range

SHA 256

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

Nonce Range

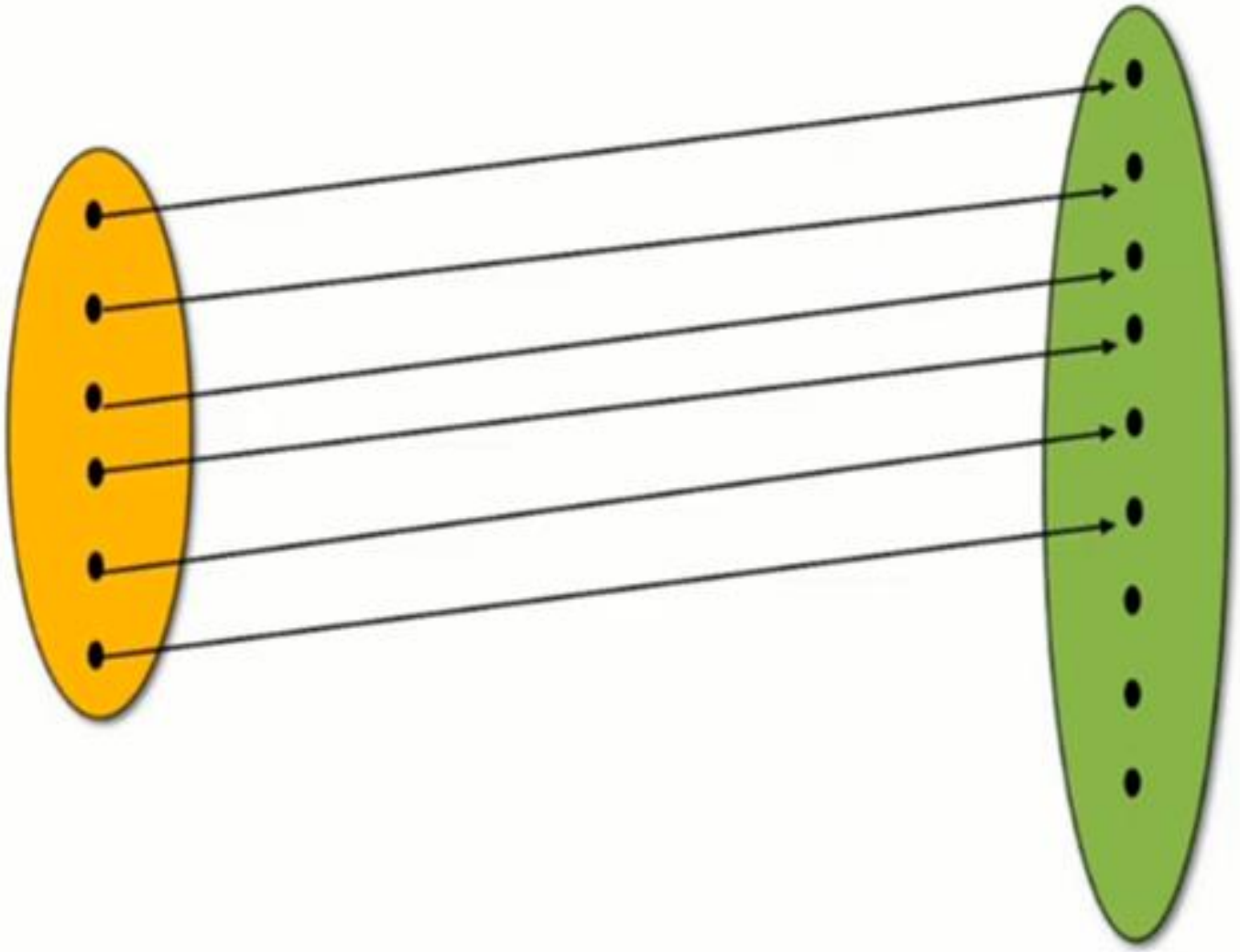
Total valid hashed $\simeq 10^{77}$

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

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

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

Nonce Range



?

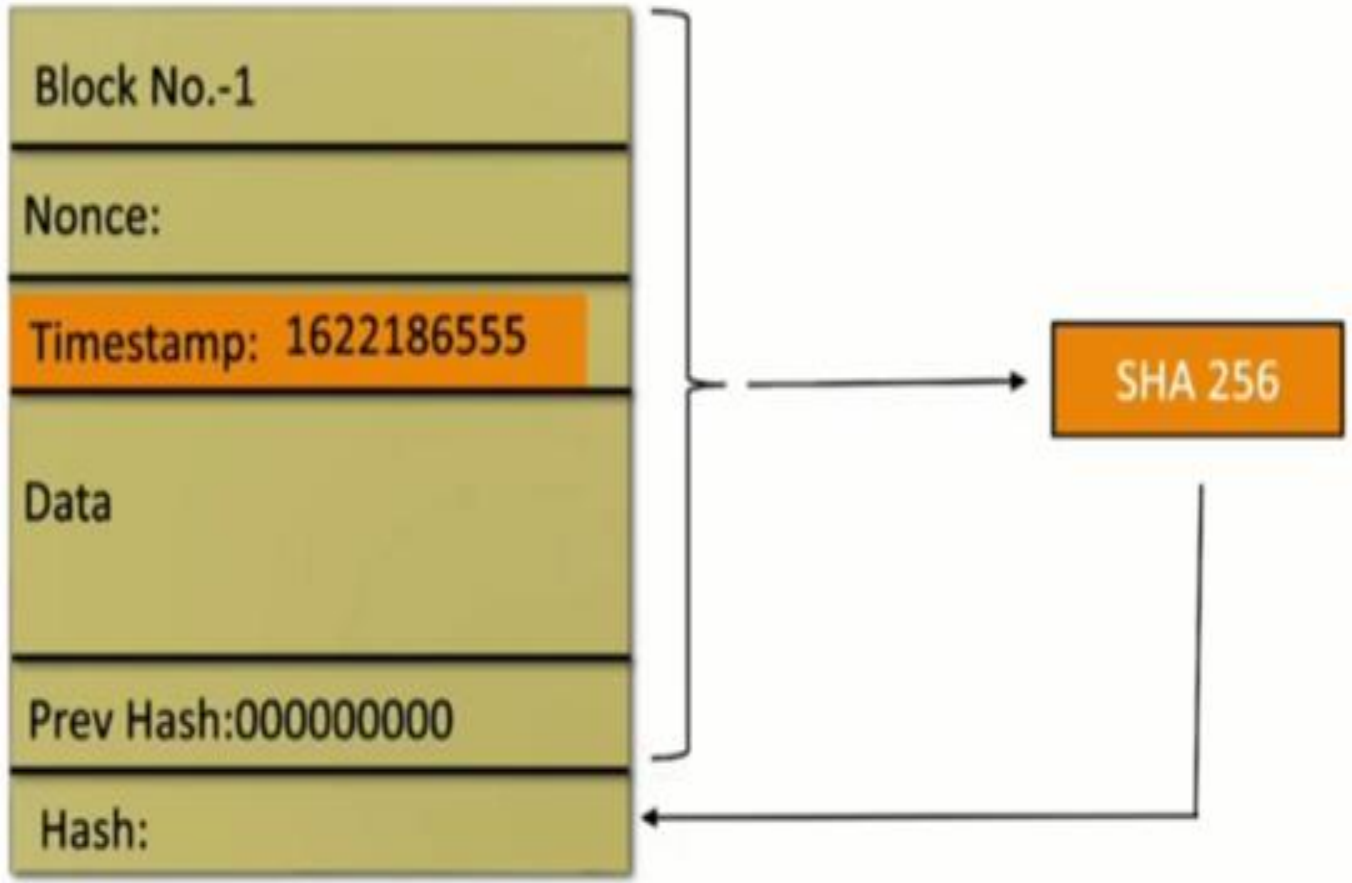
Nonce Range

A modest mines does 10^8 hashes/sec.

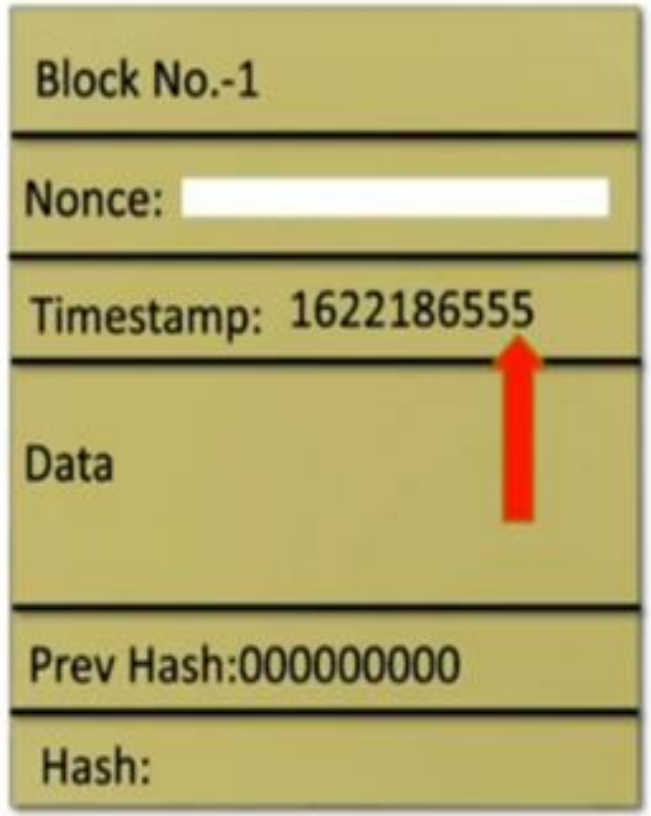
4 x 10^9 nonce will be covered in = (4 x 10^9)/(10^8)= 40 seconds.

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

Timestamp


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

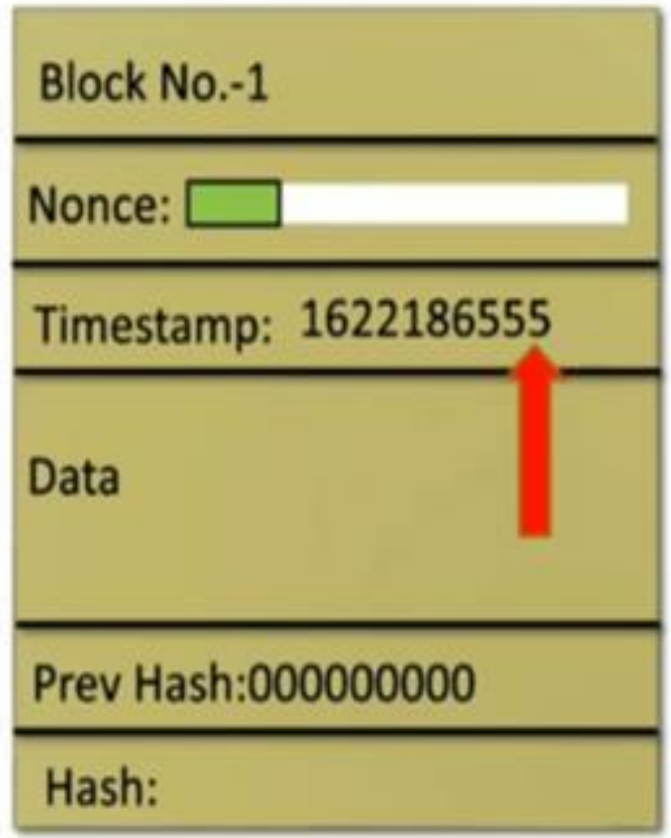
Timestamp



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

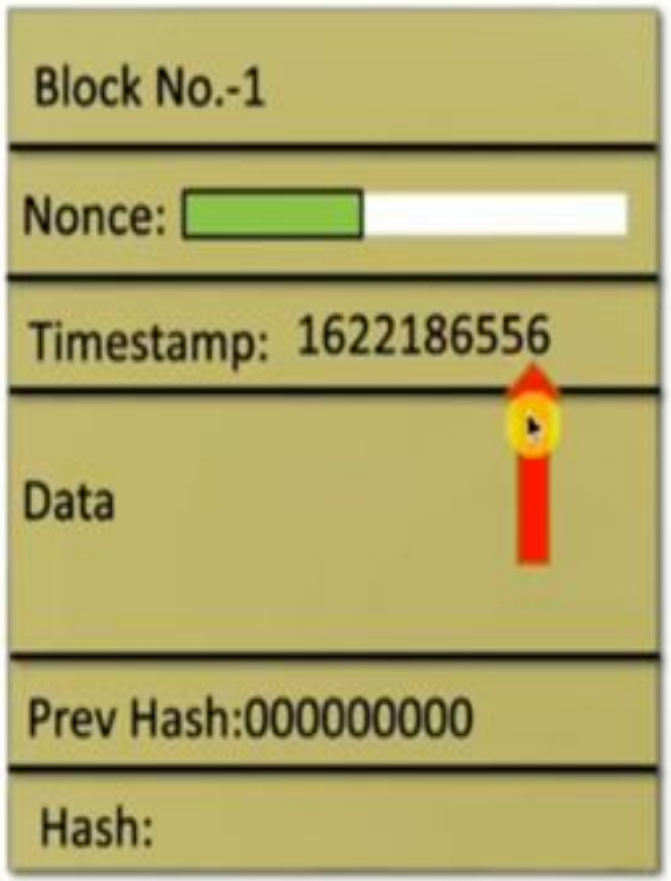
A miner will exhaust 0.1 **Billion nonce** in 1 **sec**.

Timestamp

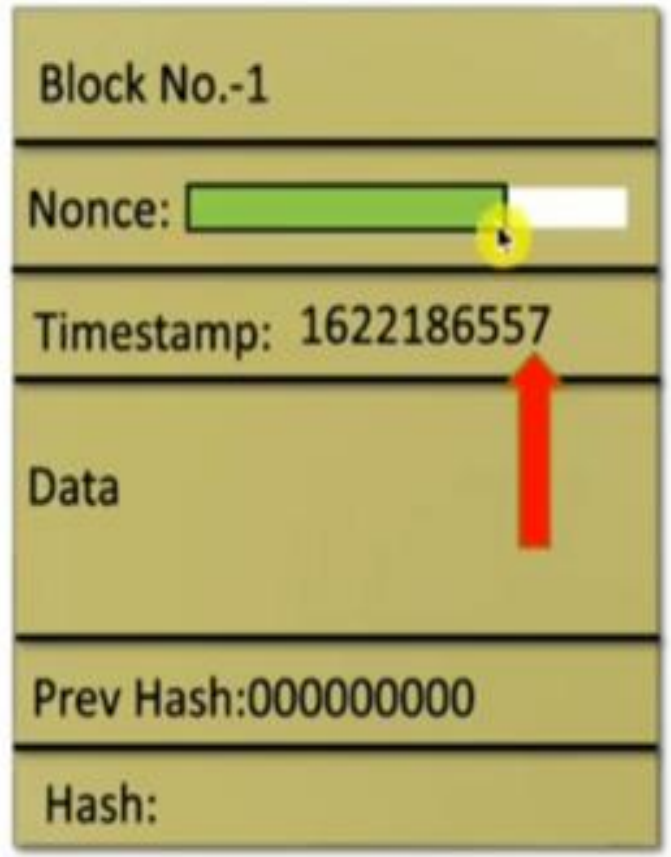


0.5 seconds

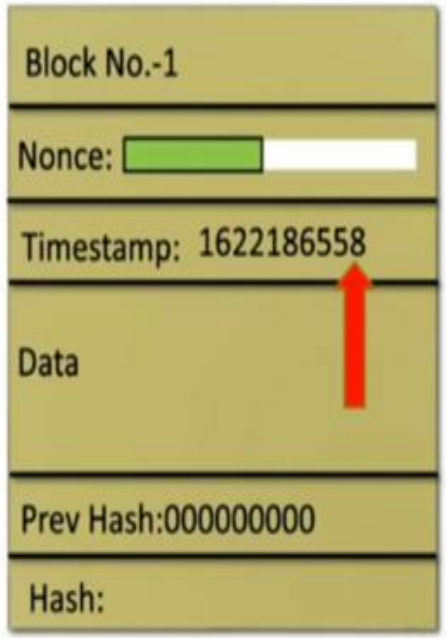
Timestamp


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

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

https://www.blockchain.com/charts

blockchain.com/charts/hash-rate

Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Sponsored Content

Currency Statistics

Block Details

Mining Information

Total Hash Rate (TH/s)

Hashrate Distribution

Hashrate Distribution Over Time

Network Difficulty

Miners Revenue (USD)

Total Transaction Fees (BTC)

Total Transaction Fees (USD)

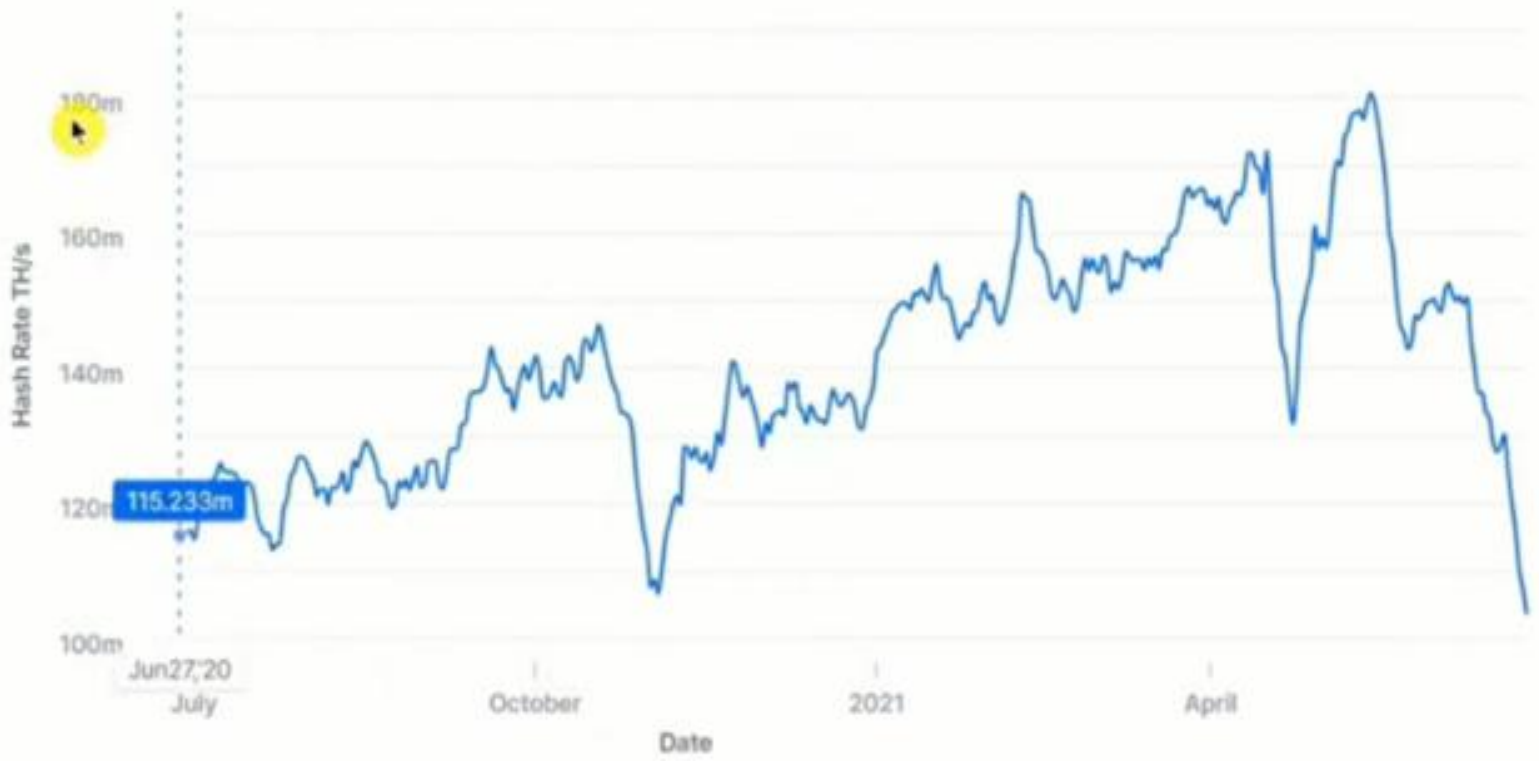
Fees Per Transaction (USD)

Cost % of Transaction Volume

Cost Per Transaction

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



Prices
Charts
DeFi
NFTs
Academy
Developers

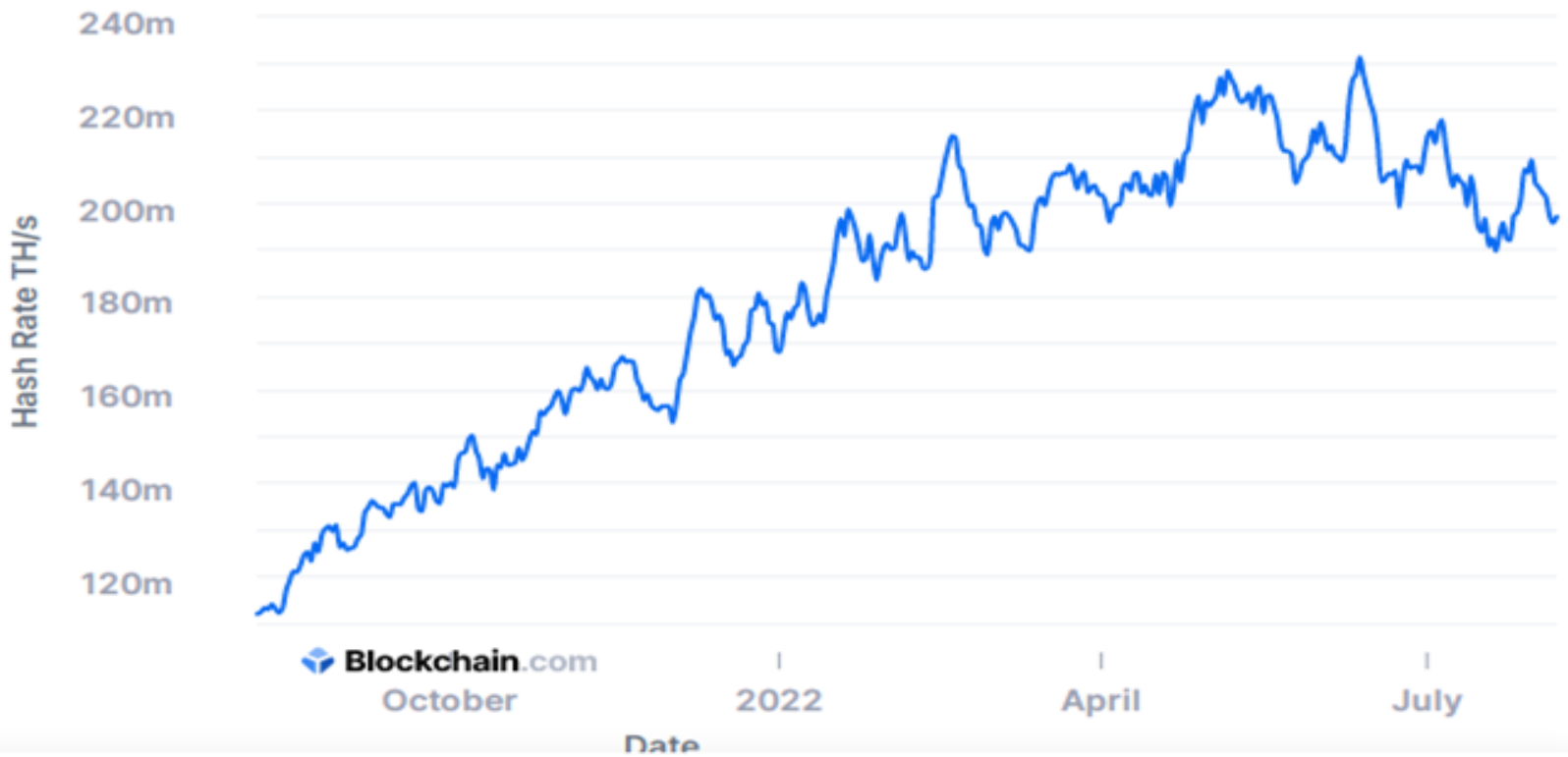
Assets

Bitcoin
Ethereum
Bitcoin Cash
BTC Testnet

Currency Statistics
Block Details
Mining Information
Total Hash Rate (TH/s)
Hashrate Distribution
Hashrate Distribution Over Time
Network Difficulty
Miners Revenue (USD)
Total Transaction Fees (BTC)
Total Transaction Fees (USD)
Fees Per Transaction (USD)
Cost % of

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



Timestamp

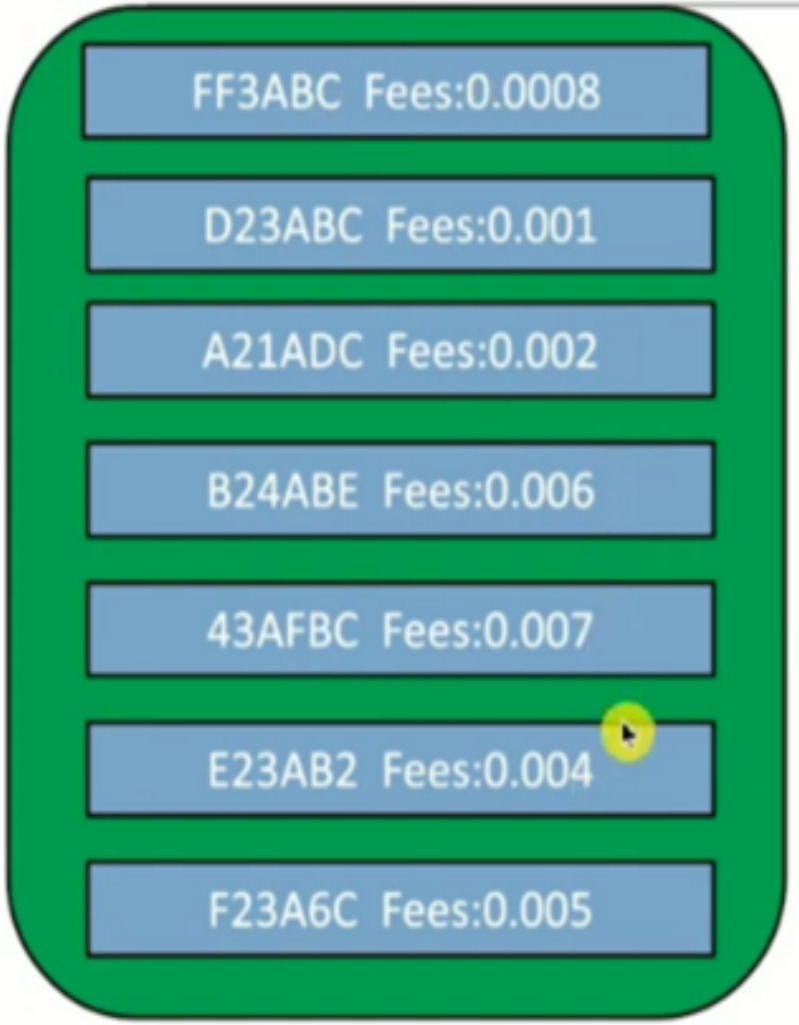
Current hashing rate is equal to **180 million trillion hashes/sec**.

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

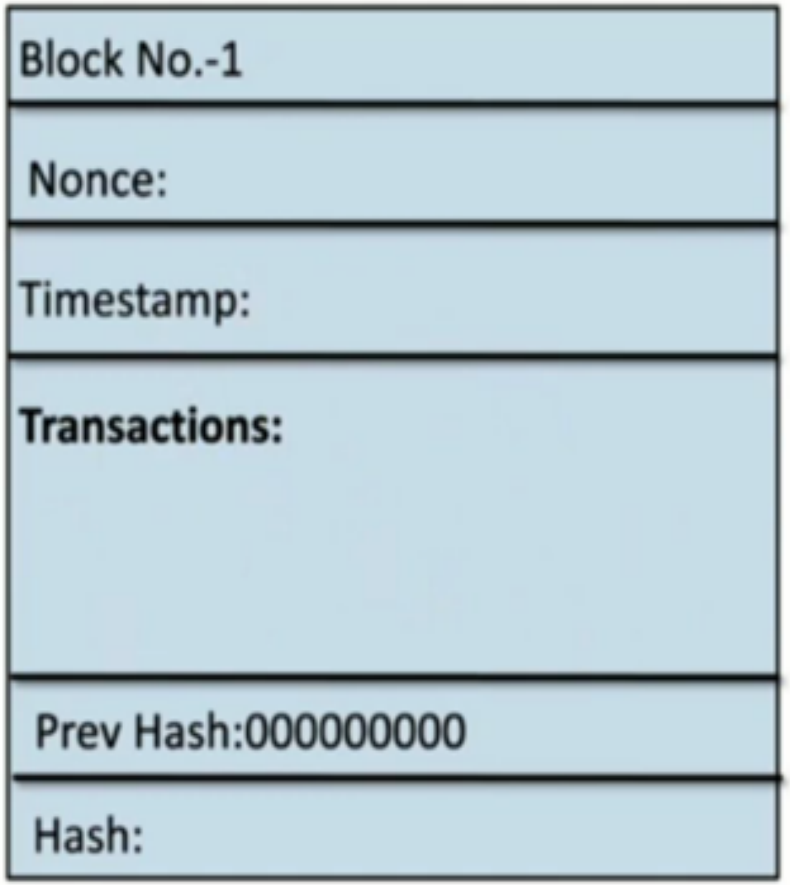
4 x 10^-9 sec <<<<< 1 sec

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

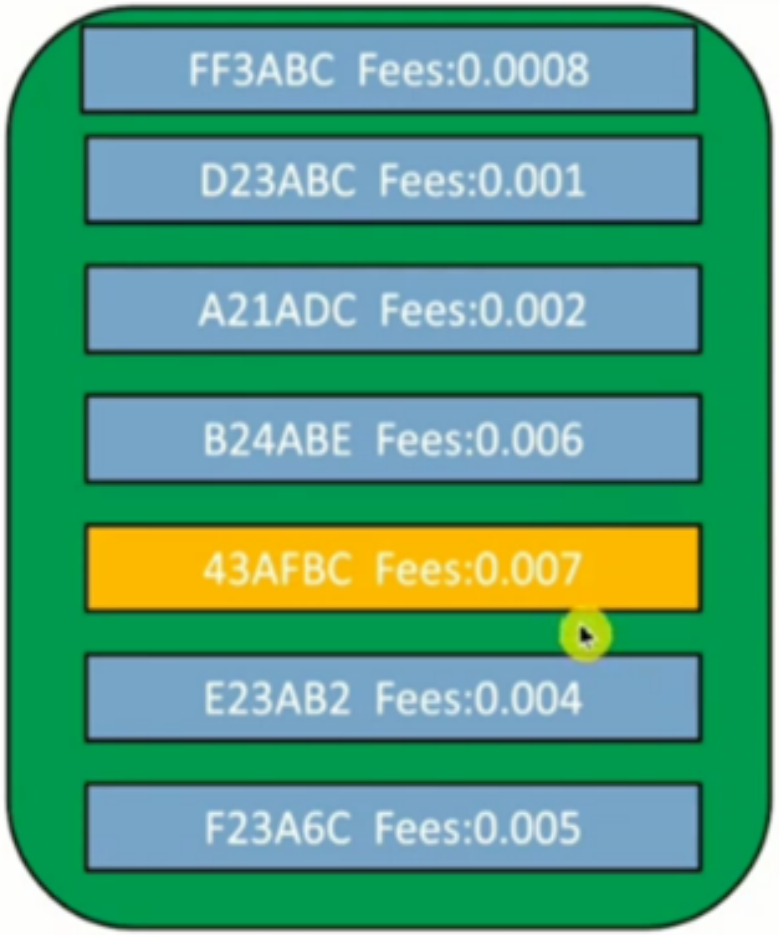
Mempool



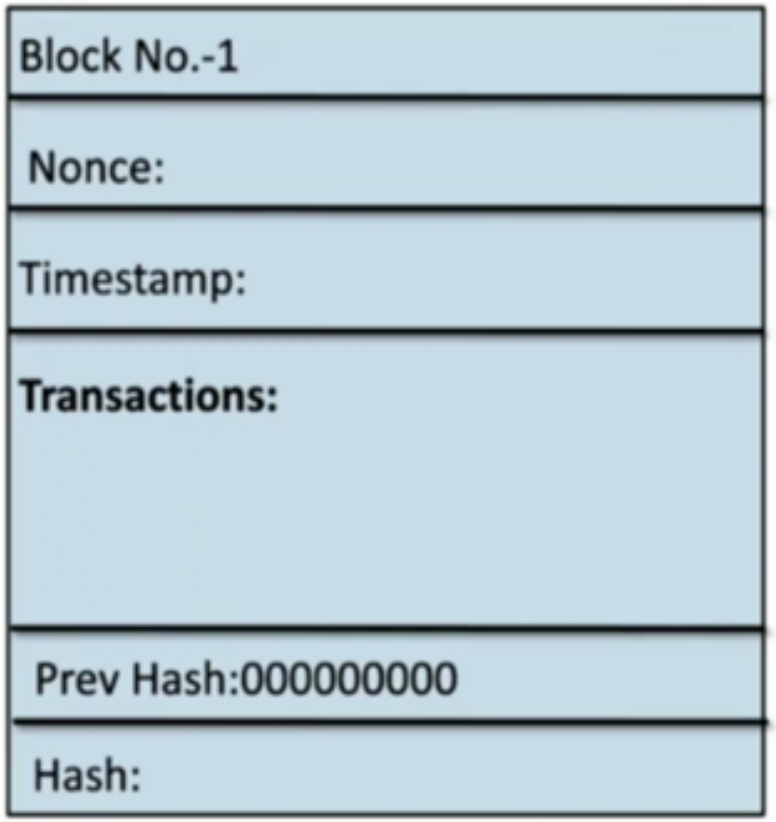
Mempool



How actually mining of transaction takes place?

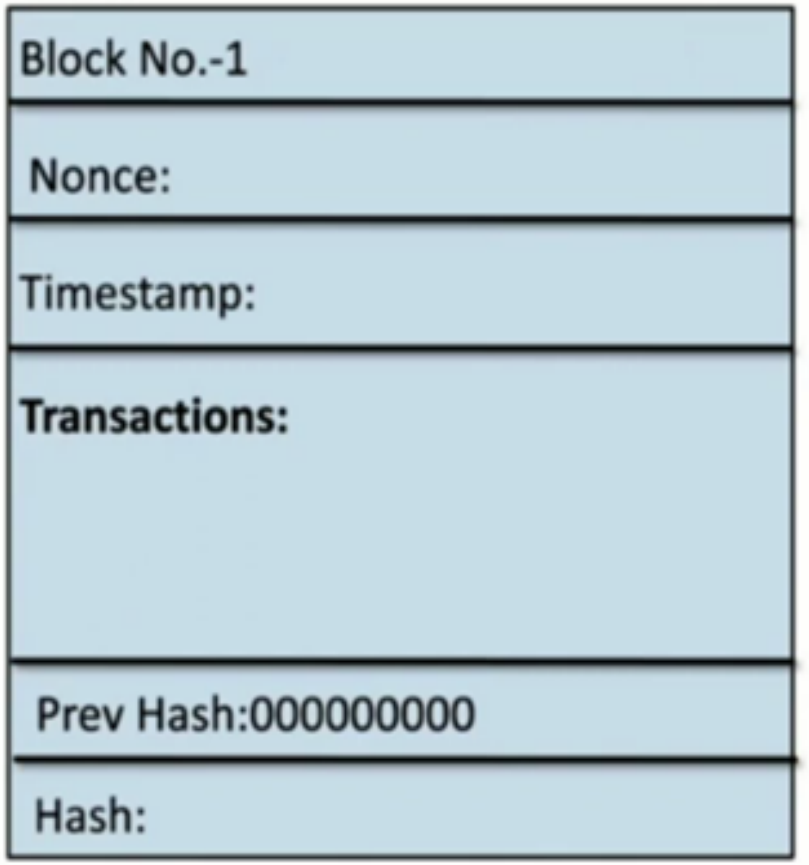


Mempool



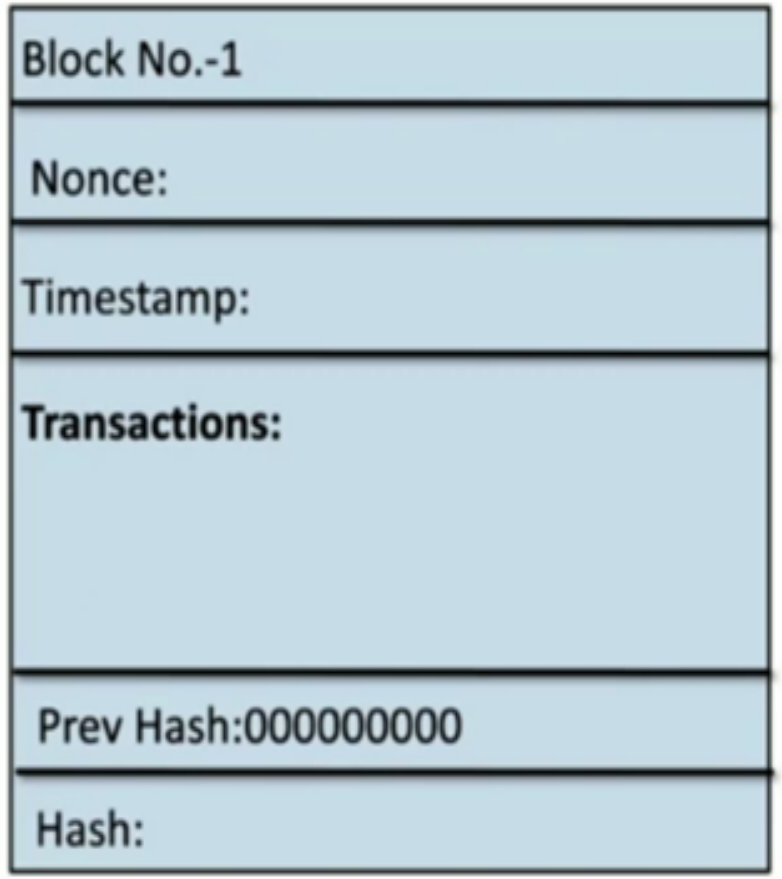
How actually mining of transaction takes place?

Mempool

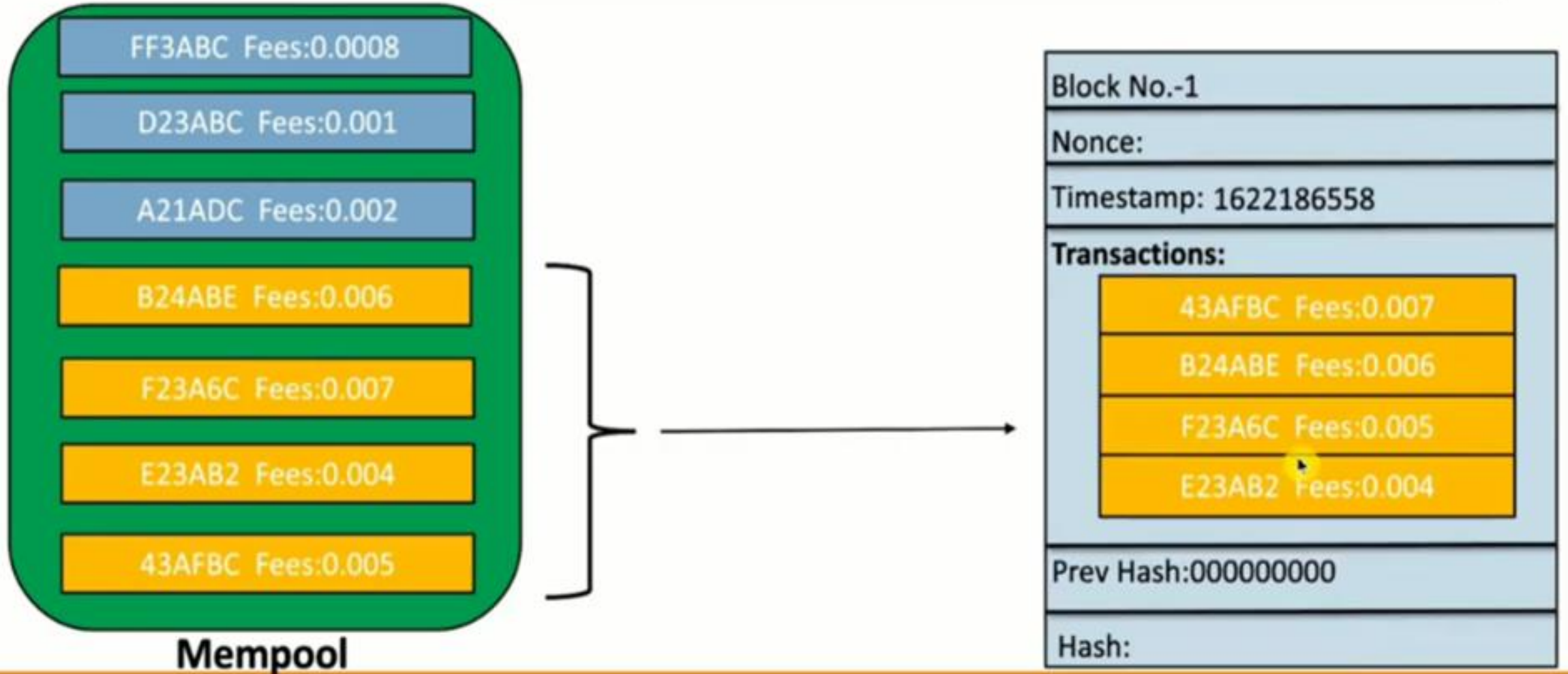


How actually mining of transaction takes place?

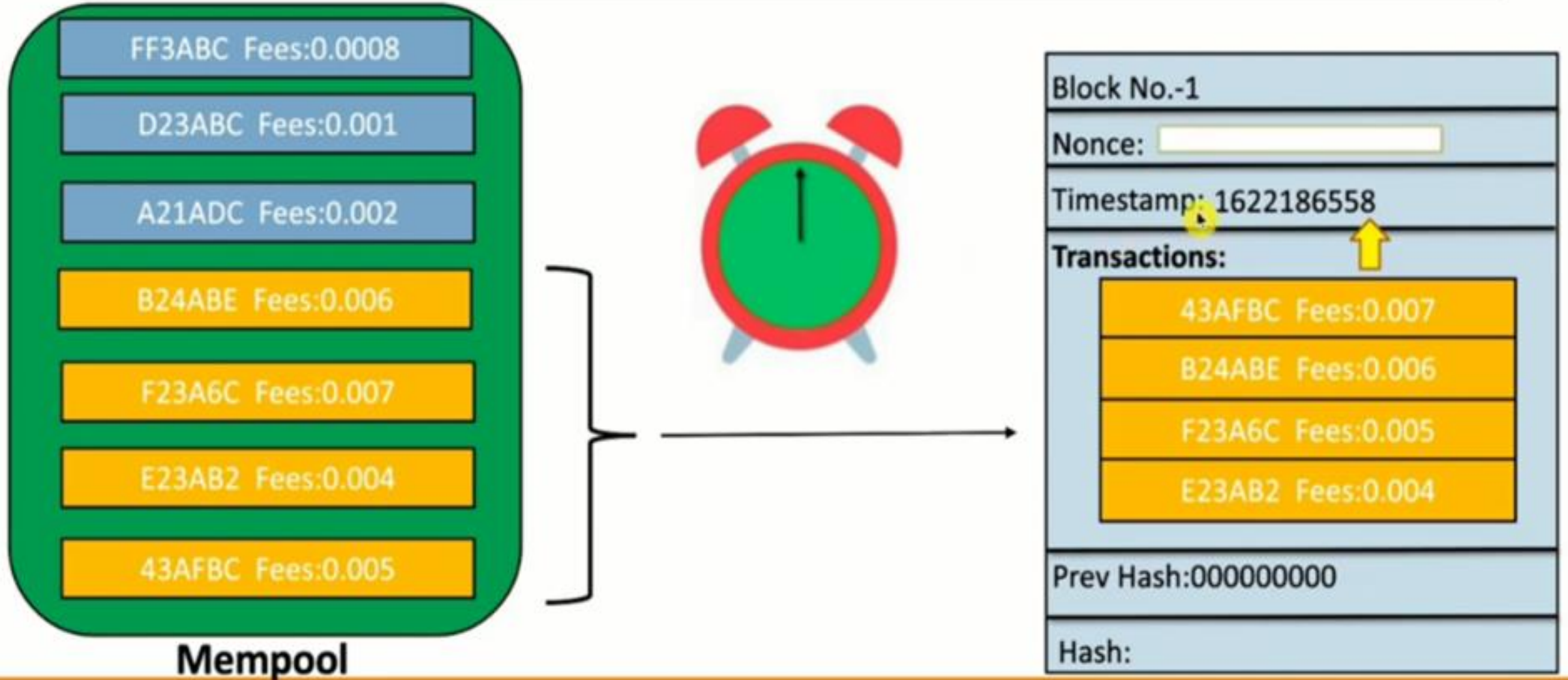
Mempool



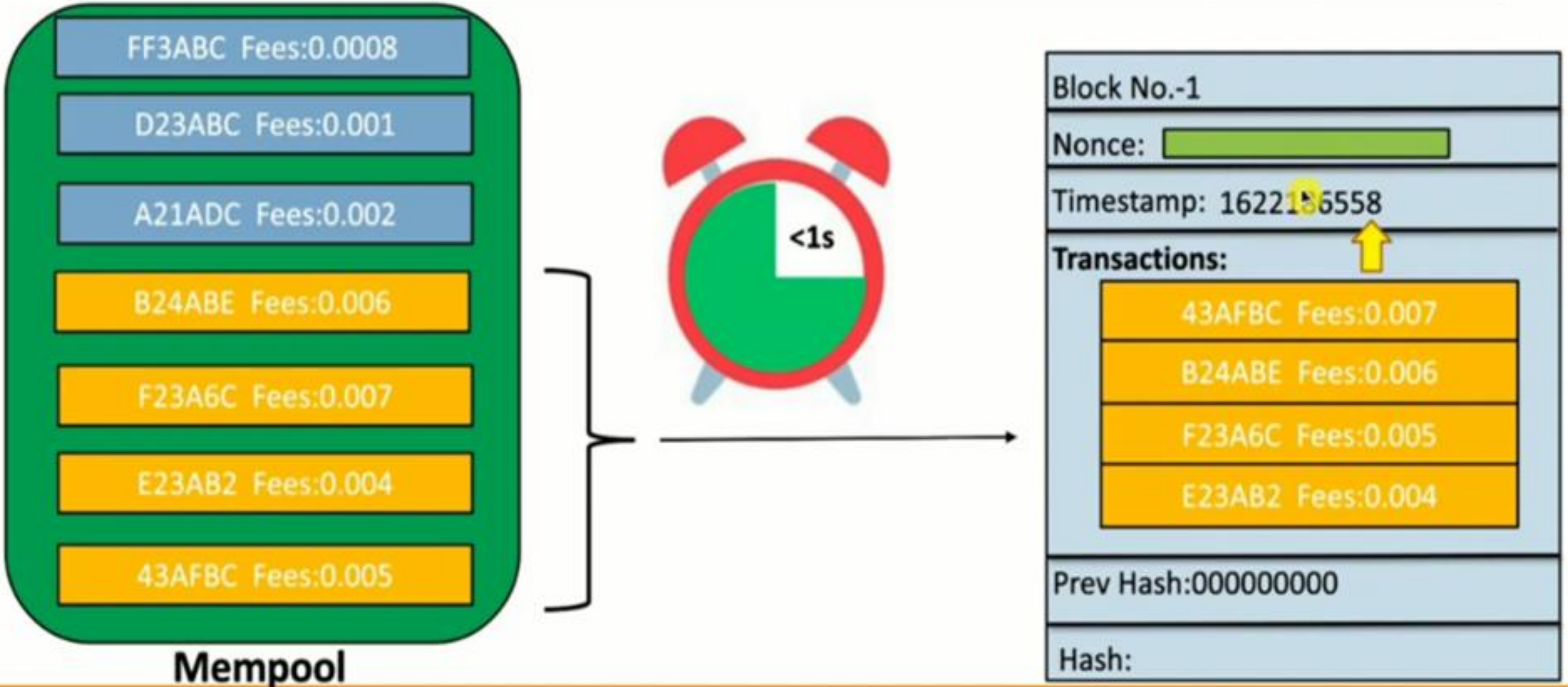
How actually mining of transaction takes place?



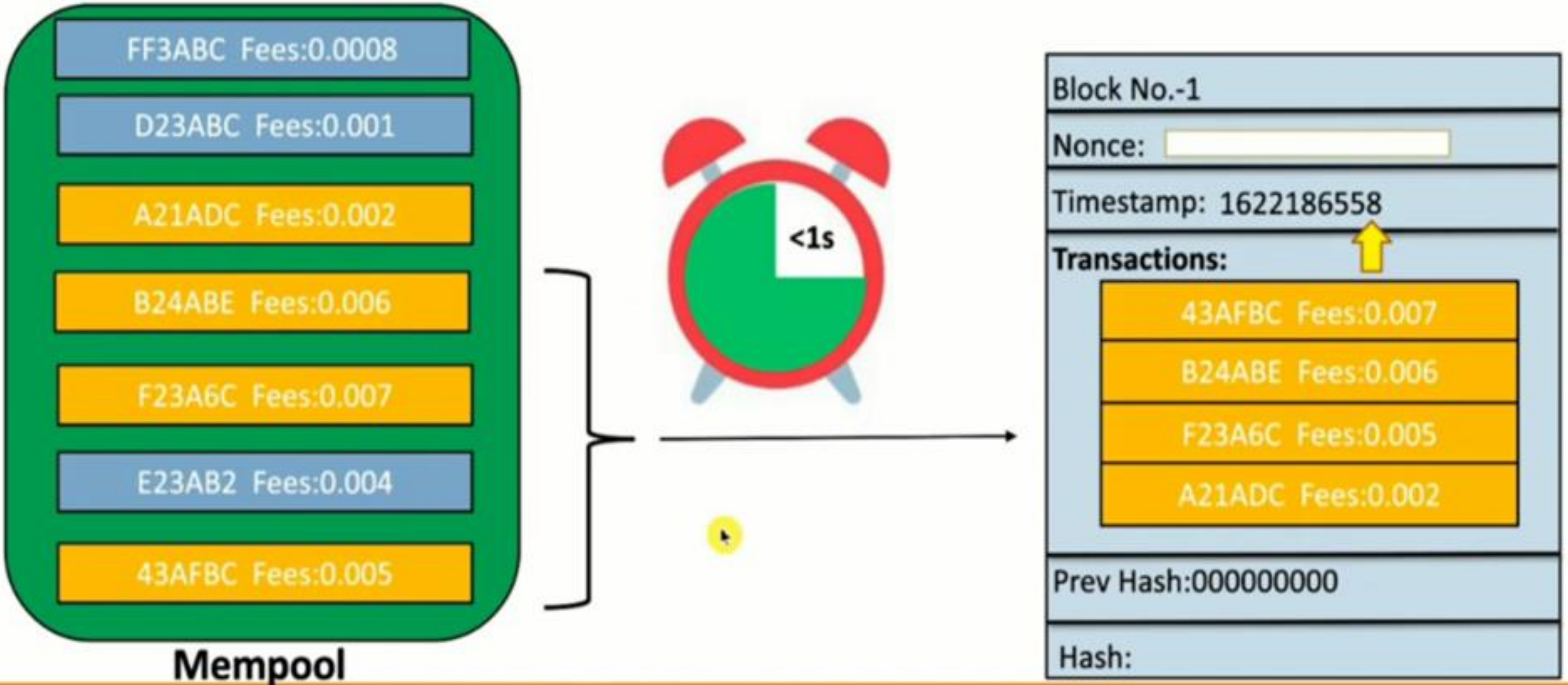
How actually mining of transaction takes place?



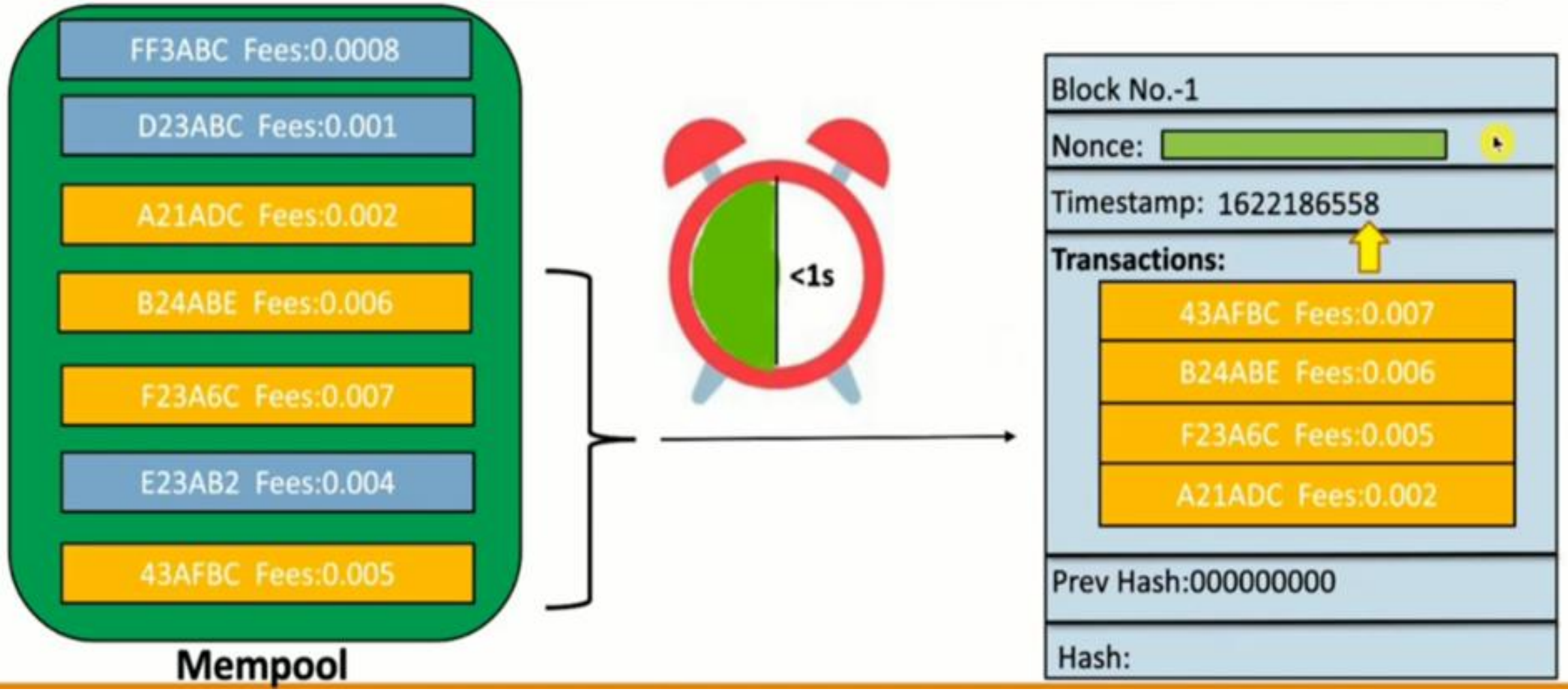
How actually mining of transaction takes place?



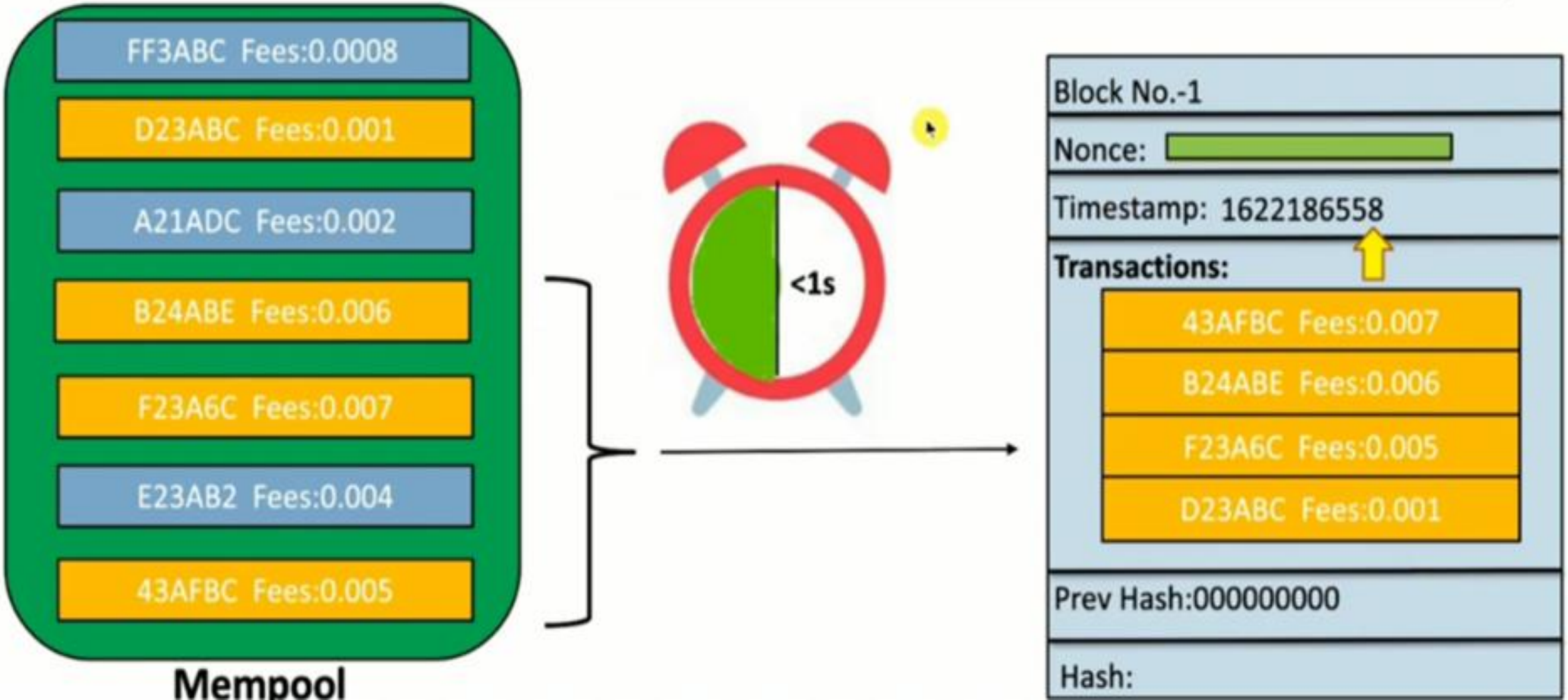
How actually mining of transaction takes place?



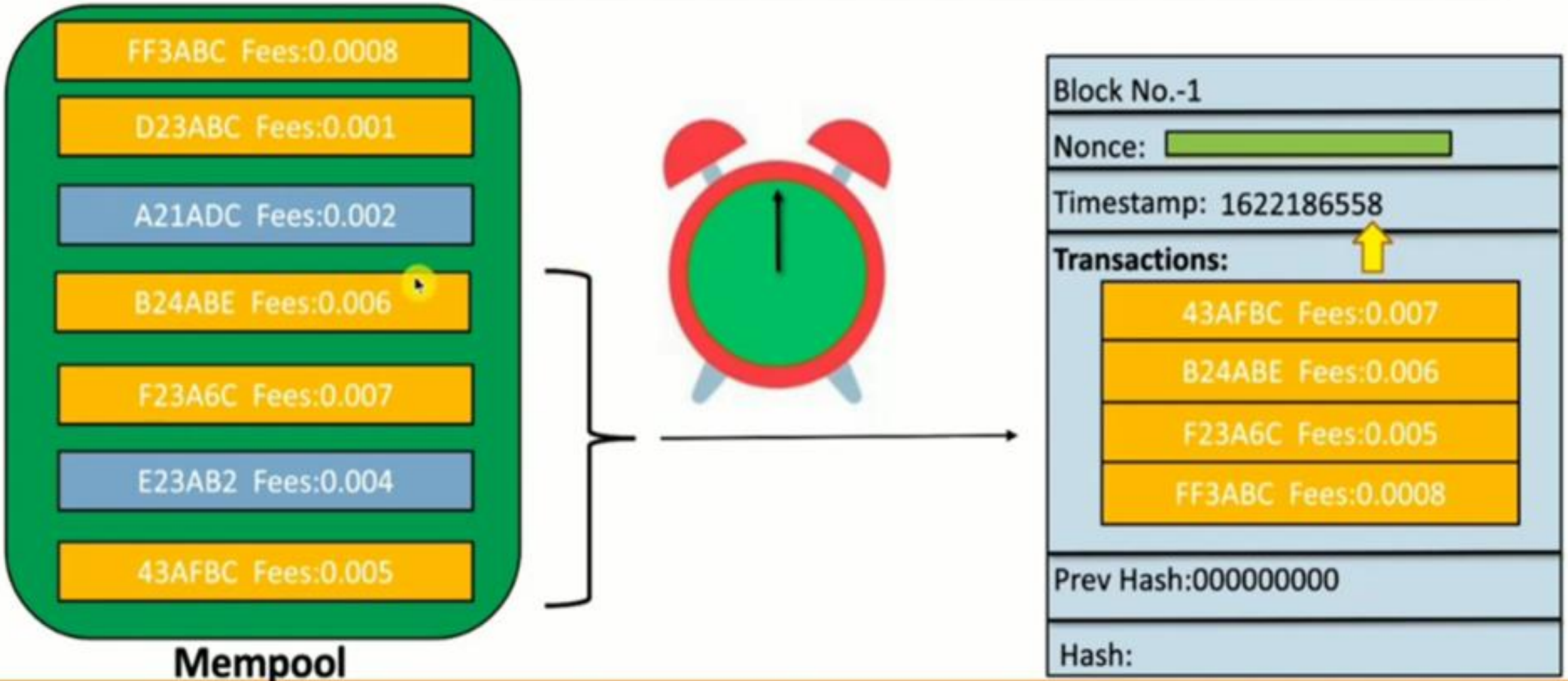
How actually mining of transaction takes place?



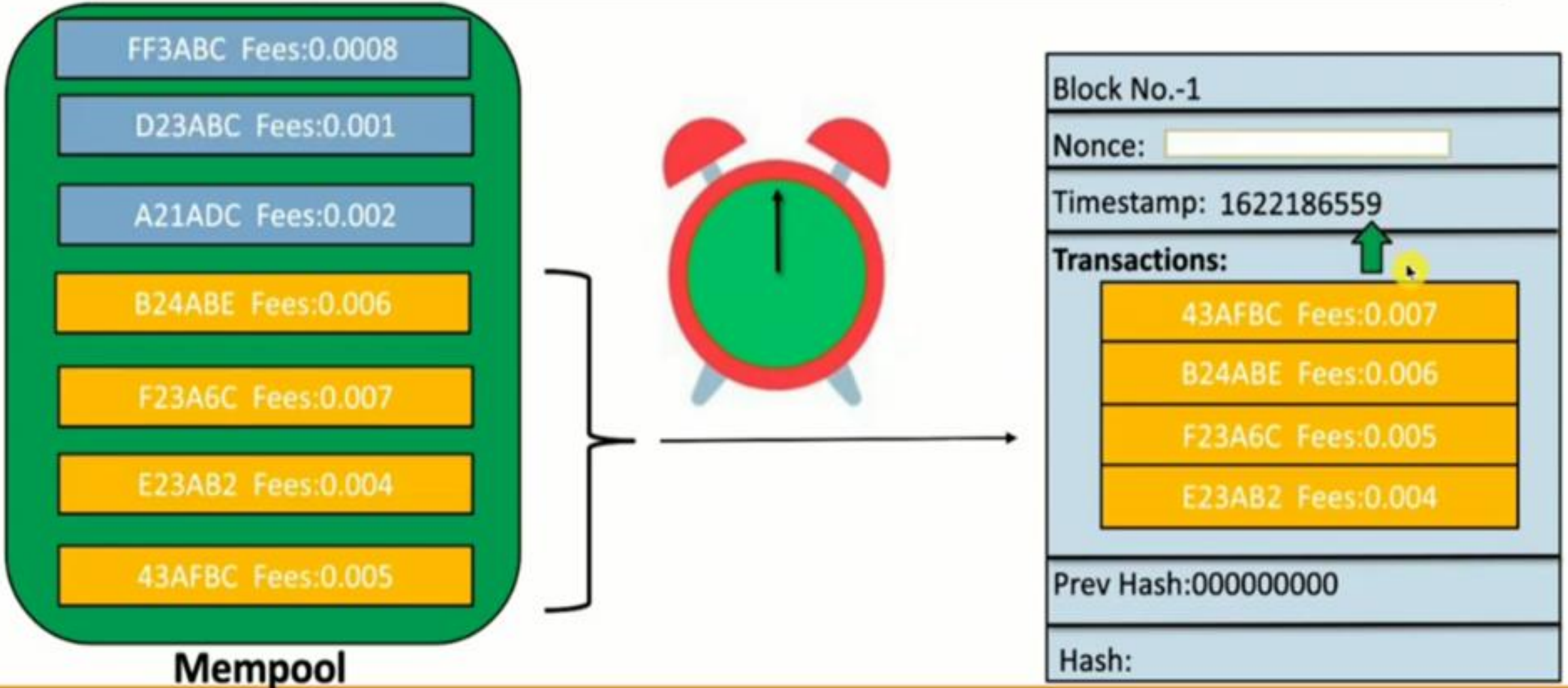
How actually mining of transaction takes place?



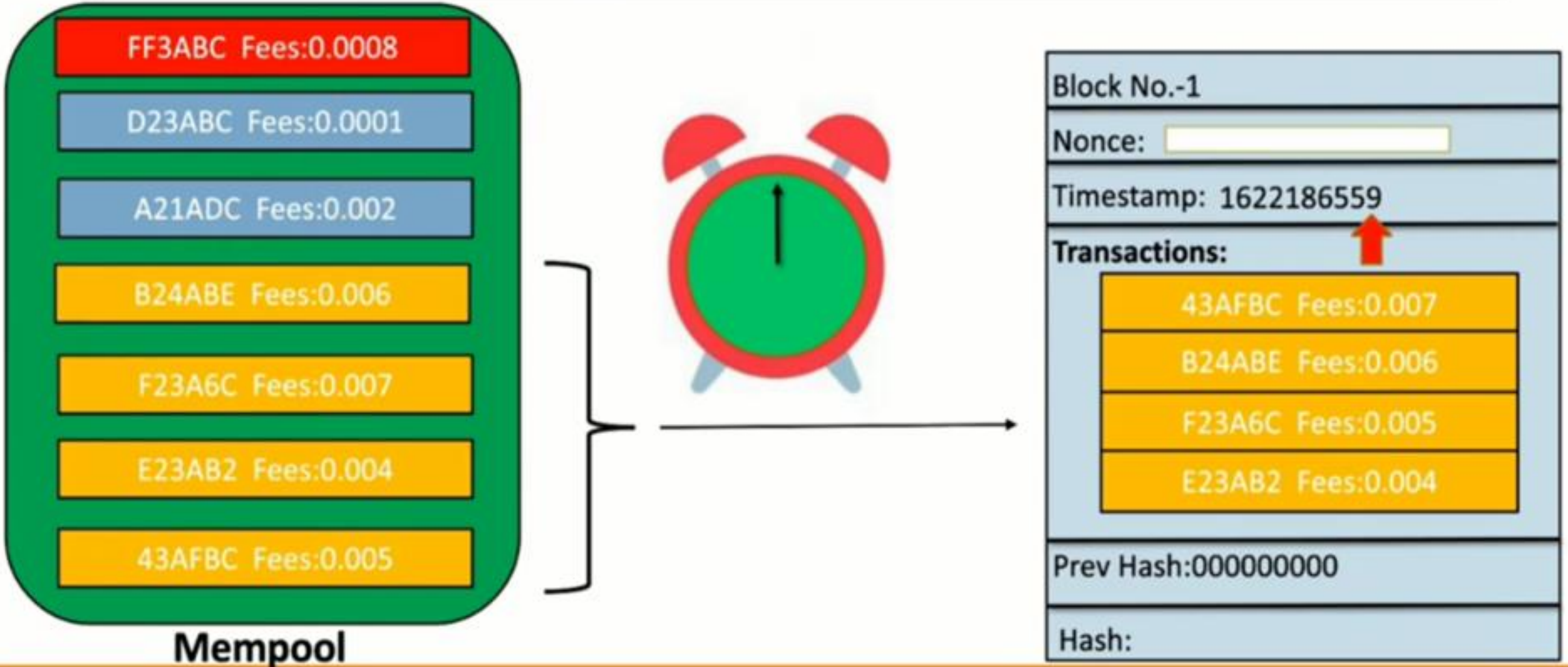
How actually mining of transaction takes place?



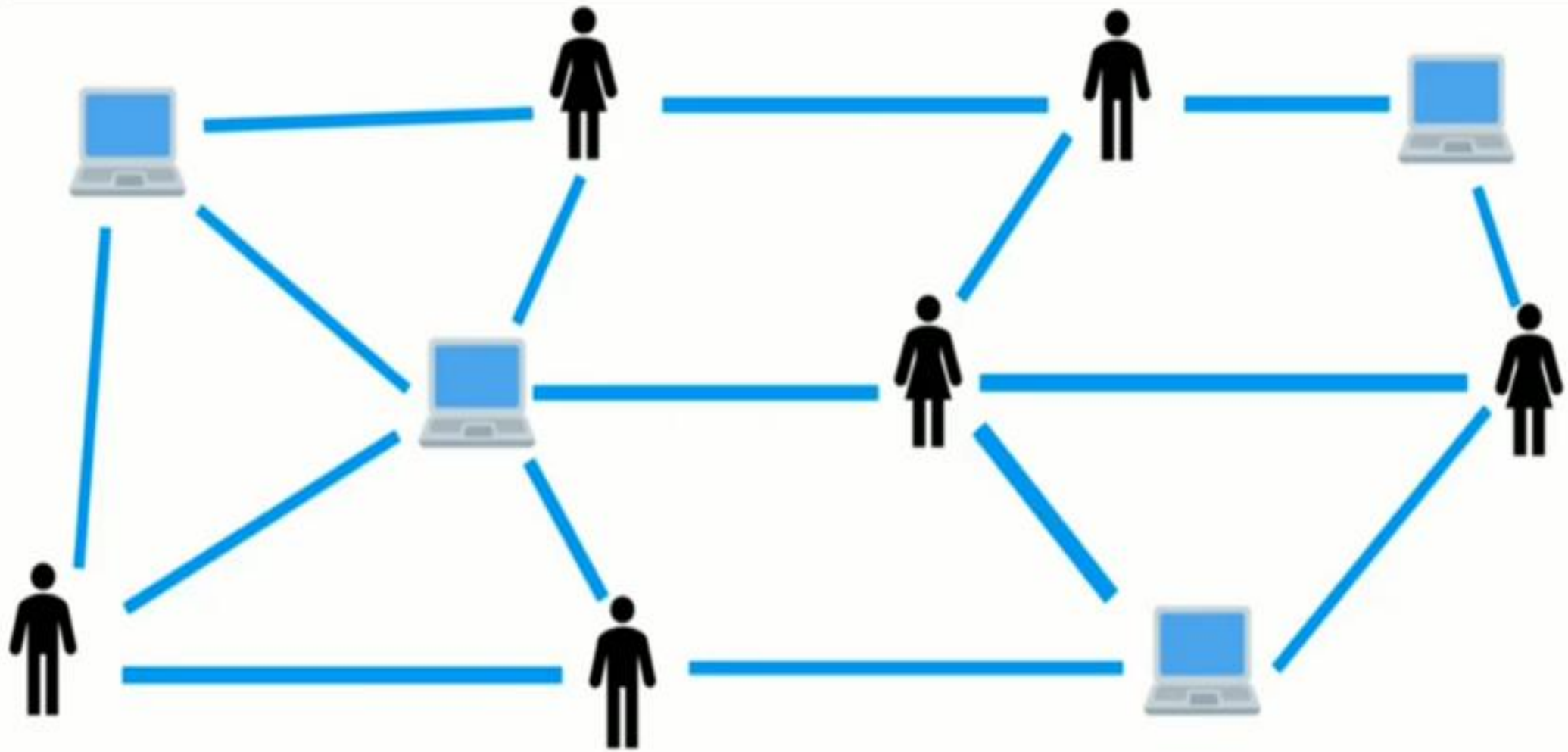
How actually mining of transaction takes place?



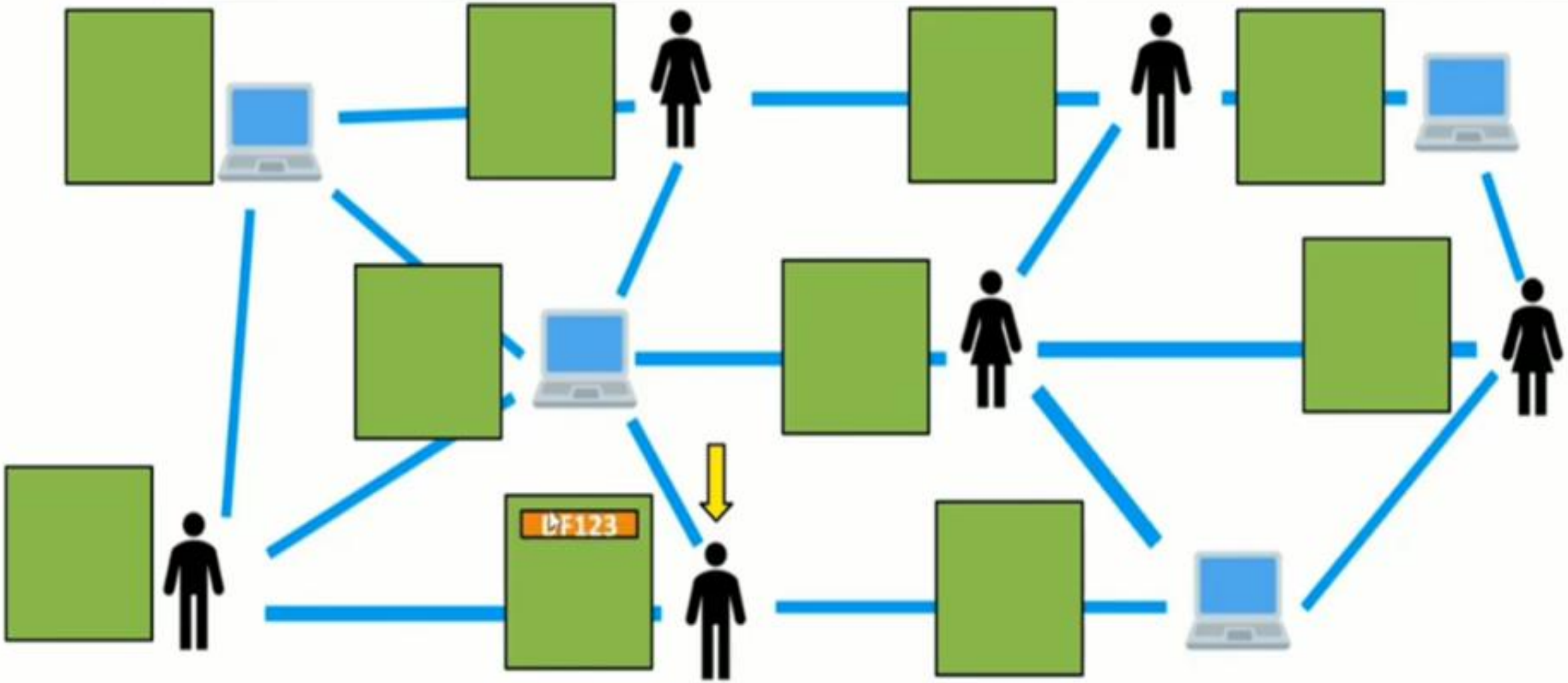
How actually mining of transaction takes place?



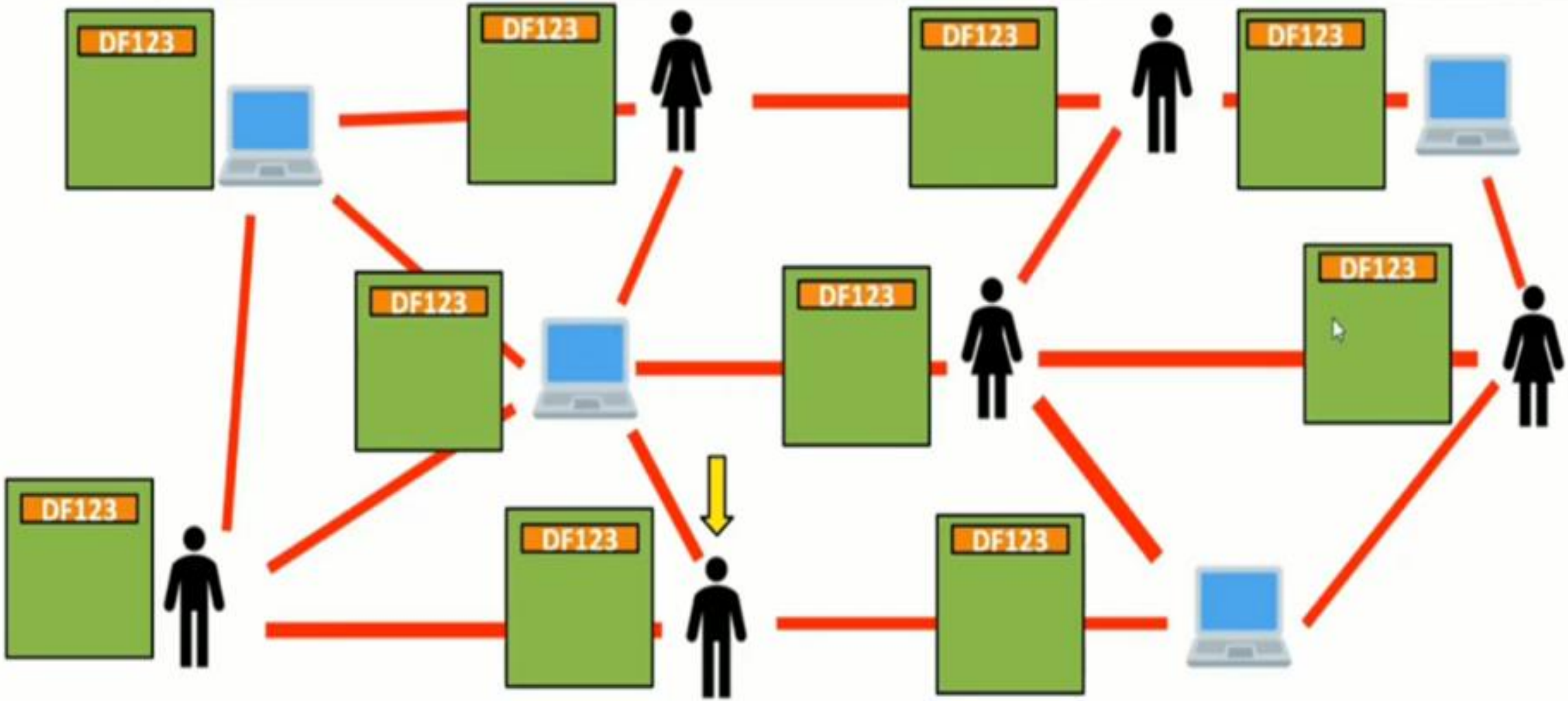
How do Mempool works?(Behind the scenes)



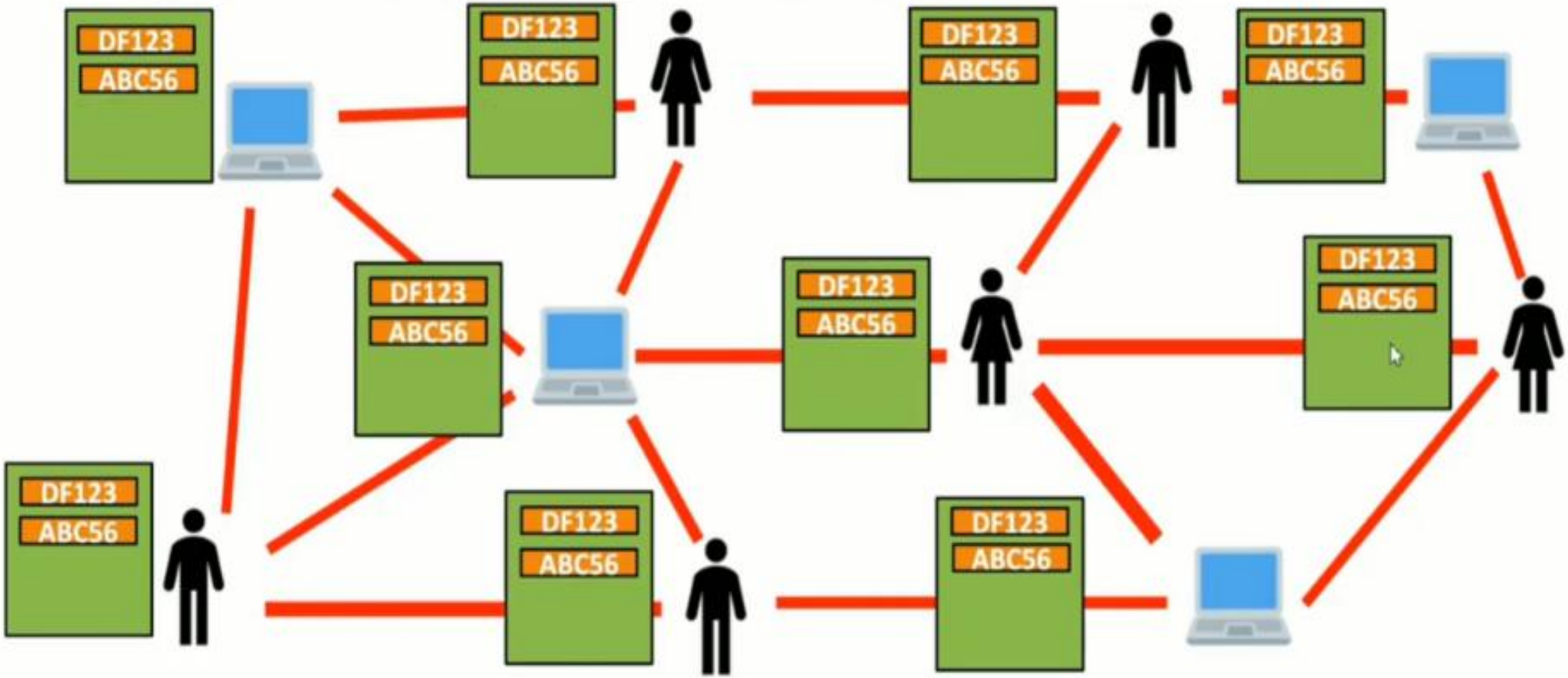
How do Mempool works?(Behind the scenes)

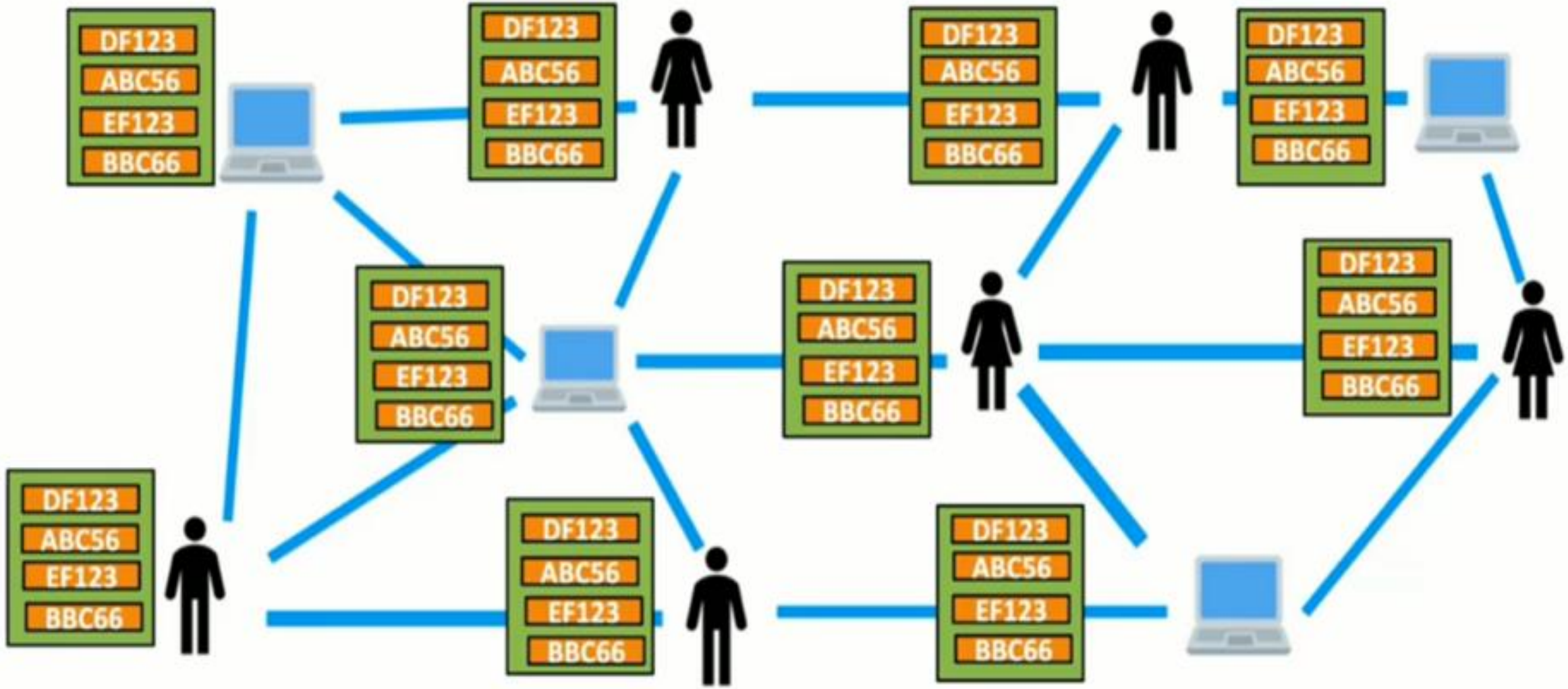


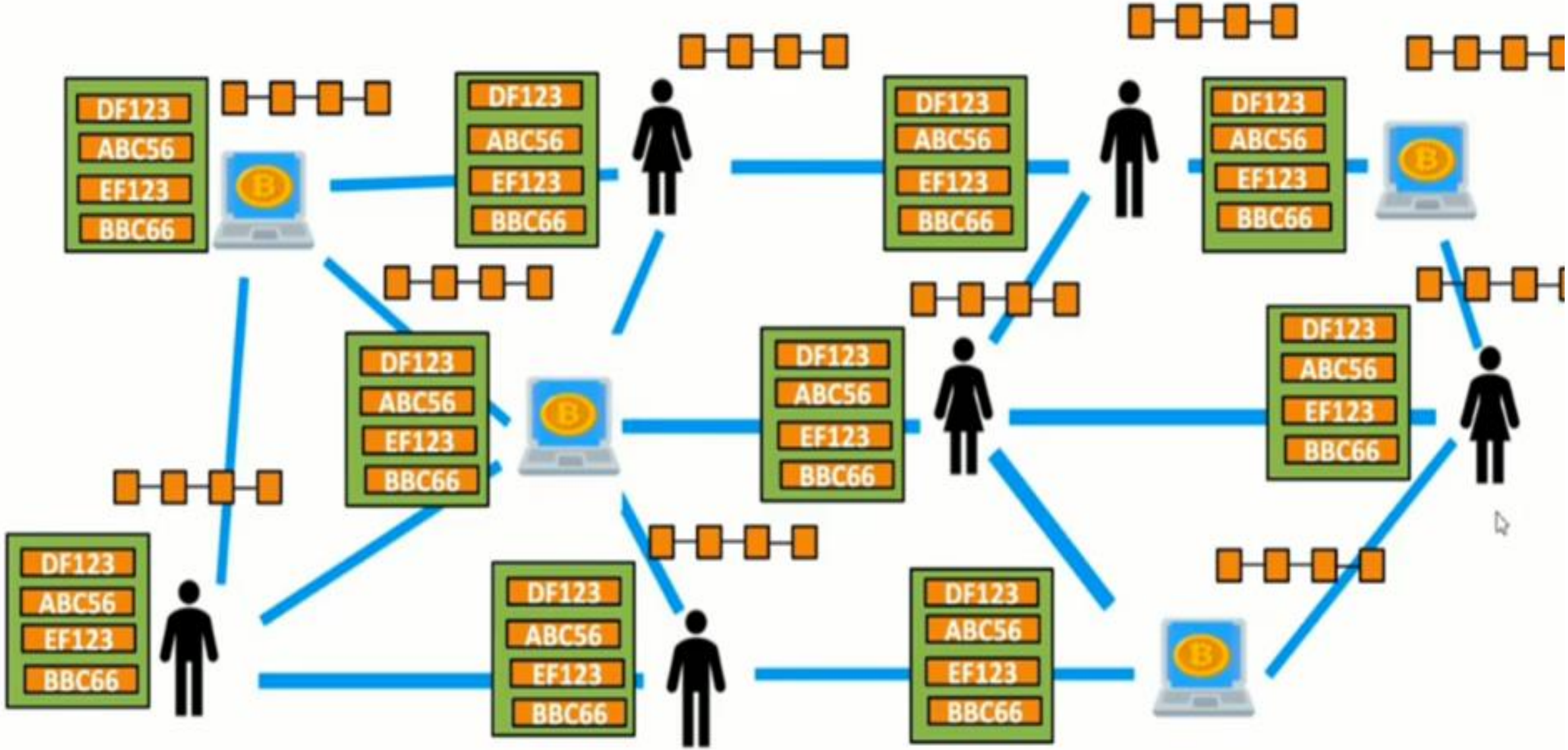
How do Mempool works?(Behind the scenes)

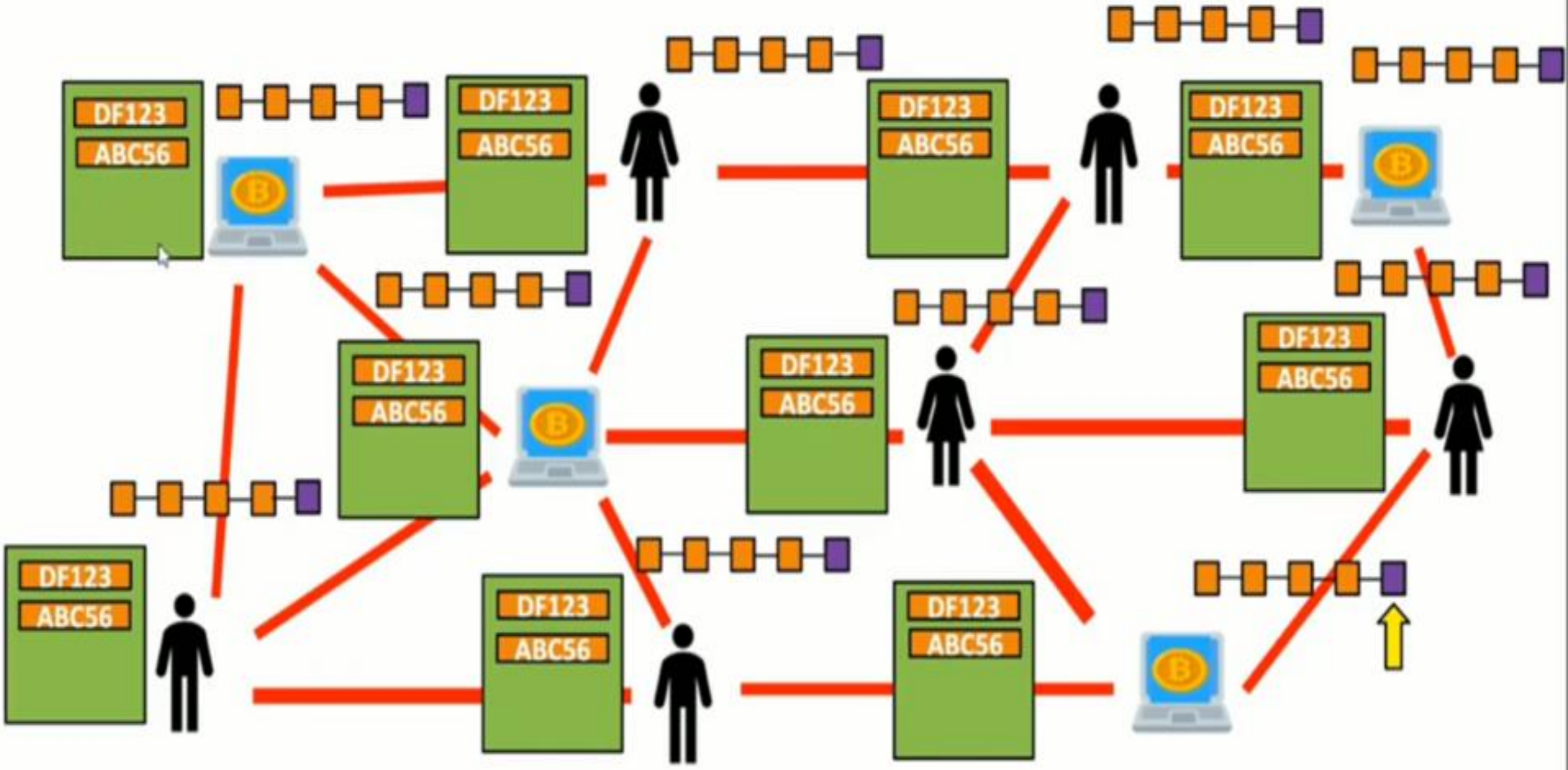


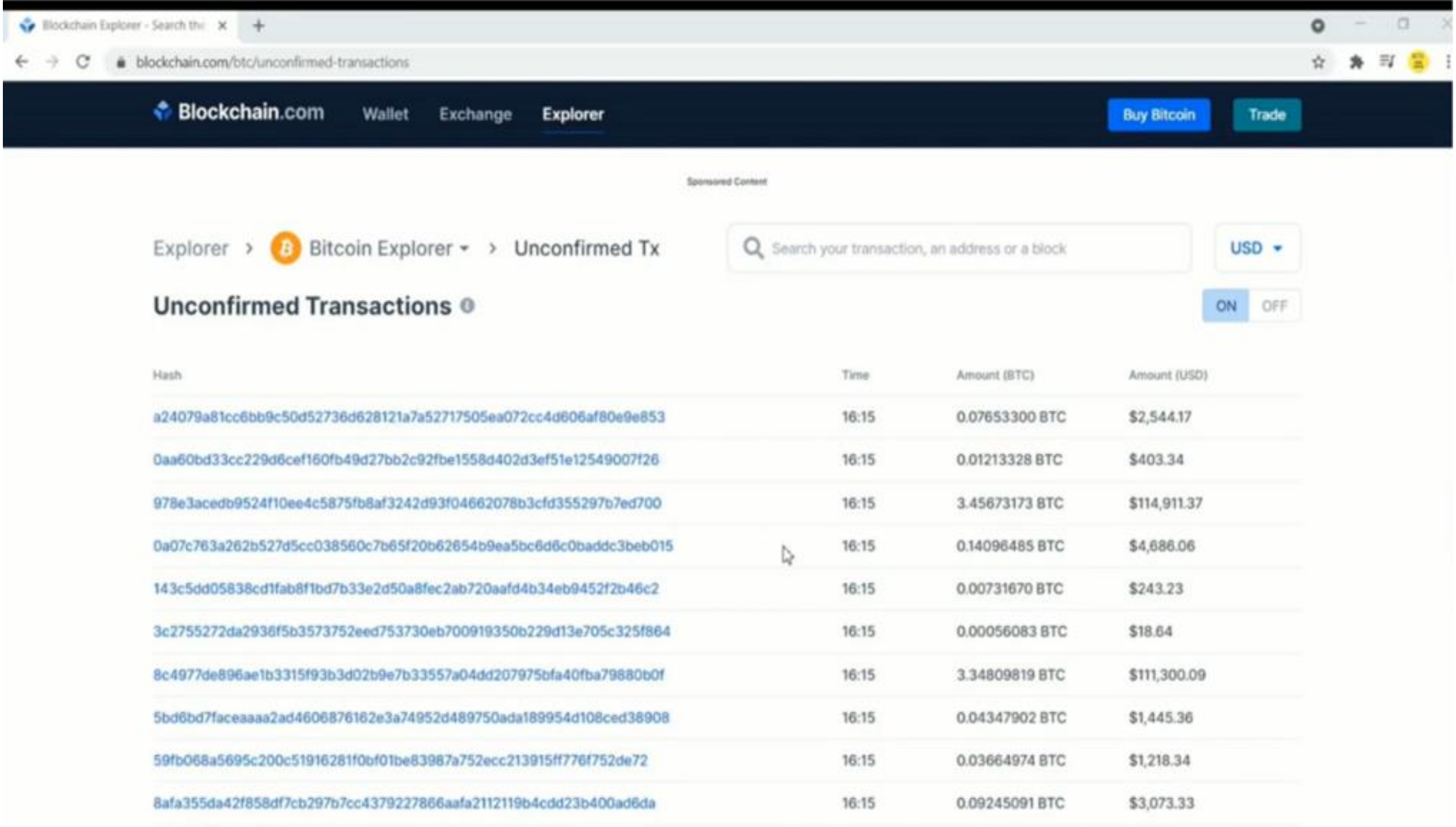
How do Mempool works?(Behind the scenes)




DF123
ABC56
EF123
BBC66


DF123
ABC56
EF123
BBC66


DF123
ABC56


Blockchain Explorer - Search the
blockchain.com/btc/unconfirmed-transactions
Blockchain.com
Wallet
Exchange
Explorer
Buy Bitcoin
Trade
Sponsored Content
Explorer
Bitcoin Explorer
Unconfirmed Tx
Search your transaction, an address or a block
USD
Unconfirmed Transactions
ON
OFF
Hash
Time
Amount (BTC)
Amount (USD)
a24079a81cc6bb9c50d52736d628121a7a52717505ea072cc4d606af80e9e853
16:15
0.07653300 BTC
$2,544.17
0aa60bd33cc229d6cef160fb49d27bb2c92fbe1558d402d3ef51e12549007f26
16:15
0.01213328 BTC
$403.34
978e3acedb9524f10ee4c5875fb8af3242d93f04662078b3cfd355297b7ed700
16:15
3.45673173 BTC
$114,911.37
0a07c763a262b527d5cc038560c7b65f20b62654b9ea5bc6d6c0baddc3beb015
16:15
0.14096485 BTC
$4,686.06
143c5dd05838cd1fab8f1bd7b33e2d50a8fec2ab720aafd4b34eb9452f2b46c2
16:15
0.00731670 BTC
$243.23
3c2755272da2936f5b3573752eed753730eb700919350b229d13e705c325f864
16:15
0.00056083 BTC
$18.64
8c4977de896ae1b3315f93b3d02b9e7b33557a04dd207975bfa40fba79880b0f
16:15
3.34809819 BTC
$111,300.09
5bd6bd7faceaaaa2ad4606876162e3a74952d489750ada189954d108ced38908
16:15
0.04347902 BTC
$1,445.36
59fb068a5695c200c51916281f0bf01be83987a752ecc213915ff776f752de72
16:15
0.03664974 BTC
$1,218.34
8afa355da42f858df7cb297b7cc4379227866aafa2112119b4cdd23b400ad6da
16:15
0.09245091 BTC
$3,073.33

https://www.blockchain.com/btc/unconfirmed-transactions?show_adv=true

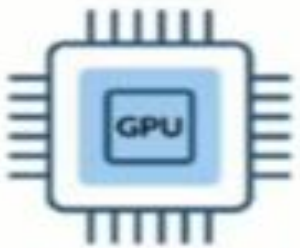
How Mining Works ?

How Mining Works ?

CPUs Vs GPUs Vs ASCIs

CPU < 10 MH/s

GPU< 1 GH/s



ASIC> 1000 GH/s

ebay.com/itm/363412825041?_trkparms=aid%3D1110006%26algo%3DHOMESPLICE.SIM%26ao%3D1%26asc%3D232959%26meid%3D6abe89cdafbc4d7ab1a1746ba1ee70ae%26pid%3D101195%26rk...

BUY 1, GET 1 AT 10% OFF (add 2 to cart) See all eligible items and terms ▸

Graphic Processing Unit Rack

Holds up to 8 GPUs

ebay.com/itm/363412825041?_trkparms=aid%3D1110006%26algo%3DHOMESPLICE.SIM%26ao%3D1%26asc%3D232959%26meid%3D8abe89cdafbc4d7ab1a1746ba1ee70ae%26pid%3D101195%26rk...

30 DÍAS DESPUÉS DE LA ENTREGA

tu compra está protegida

1 more account

BUY 1, GET 1 AT 10% OFF (add 2 to cart) See all eligible items and terms ▸

HEAT DISSIPATION DESGIN

55mm space betwen 8 GPUs

ebay.com/itm/363412825041?_trkparms=aid%3D1110006%26algo%3DHOMESPLICE.SIM%26ao%3D1%26asc%3D232959%26meid%3D8abe89cdafbc4d7ab1a174

Hi! Sign in or register Daily Deals Help & Contact

ebay Shop by category Search for anything

Back to home page | Listed in category: Coins & Paper Money > Virtual Currency > Miners

Computers/Tablets & Networking > Computer Components & Parts > Computer Cases & Accessories > Computer Cases

BUY 1, GET 1 AT 10% OFF (add 2 to cart) See all eligible items and terms ►

6/8 GPU Mining Rig Rack Open Air Computer Case Frame Miner BT
ETH ETC Ethereum

42 viewed per day

Condition: New

Quantity: 1 More than 10 available / 1 sold

Price: US $85.99

Buy It Now

Add to cart

Best Offer:

Make Offer

♡ Add to Watchlist

amazon.com/ASICMiner-Block-Erupter-USB-Sapphire/dp/B00CUJT7TO

Electronics › Computers & Accessories › Data Storage › USB Flash Drives

ASICMiner Block Erupter USB 330MH/s Sapphire Miner

Brand: Block Erupter

4.3 out of 5 stars 232 ratings | 162 answered questions

Color	Black
Memory Storage Capacity	333 MB
Brand	Block Erupter
Hardware Interface	USB

About this item

- MINIMUM ORDER OF 5 UNITS FOR THIS DISCOUNTED PRICE.
- BitFountain
- ASIC Block Erupter USB
- 300 MH/s

See All Buying Options

Deliver to India

Add to List

Share

Have one to sell?

Sell on Amazon





Antminer S9i 14TH/S 16nm ASIC BTC Bitcoin Miner

By: AntMiner Item#: 9541970

INR113779 IN STOCK

Order now and get it around Saturday, July 17

Qty 1 ADD TO CART

ADD TO WISHLIST | SHARE:

Note: Electronic products sold in US store operate on 110-120 volts, a step-down power converter is required for the smooth device function. It is mandatory to know the wattage of the device in order to choose the appropriate power converter. Recommended power converters Buy Now

Additional Information | Product Description

Product Dimensions	13.78 x 5.31 x 6.22 inches
Item Weight	12.13 pounds

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.

Transaction :

Input:

0.7 BTC from Alice

Output:

0.5 BTC to the coffee shop.

0.2 BTC back to me.

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.

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.

Transaction and UTXOs

Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Bob -> Me 0.1 BTC
Me -> Me 0.2 BTC

UTXOs

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.

Transaction and UTXOs

Bob -> Me 0.1 BTC } UTXOs

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.

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

Transaction Fee

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.

Transaction :

Input:

0.7 BTC from Alice

Output:

0.5 BTC to the coffee shop.

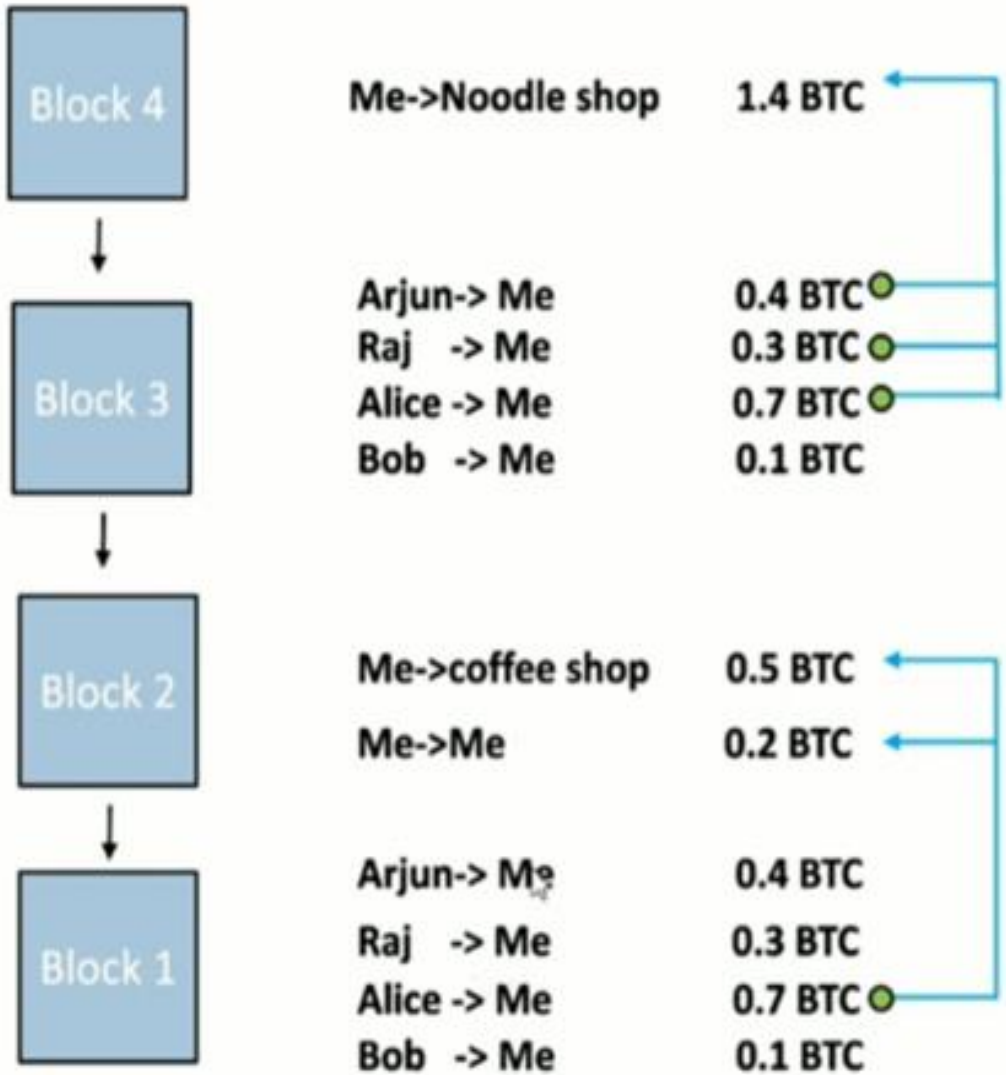
0.1 BTC back to me.

UTXO for the coffee shop.

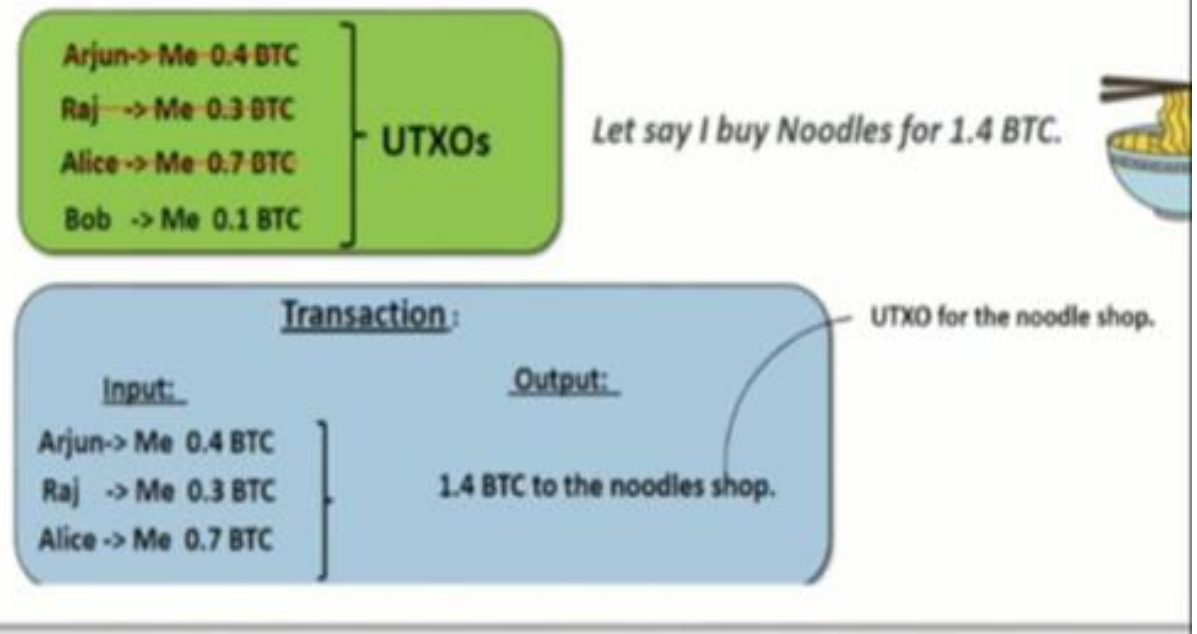
UTXO for the miner.

Fees: 0.1 BTC

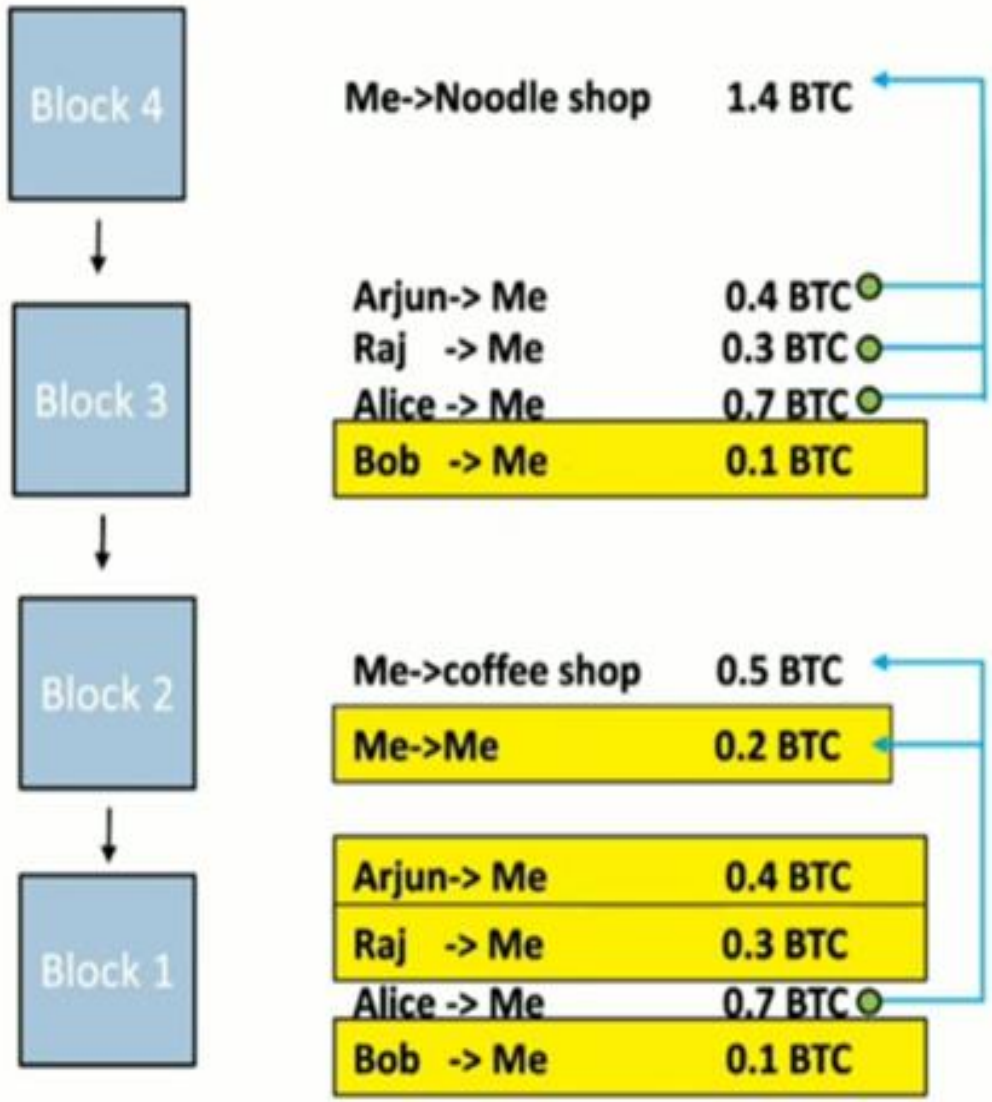
Cryptocurrency Wallets



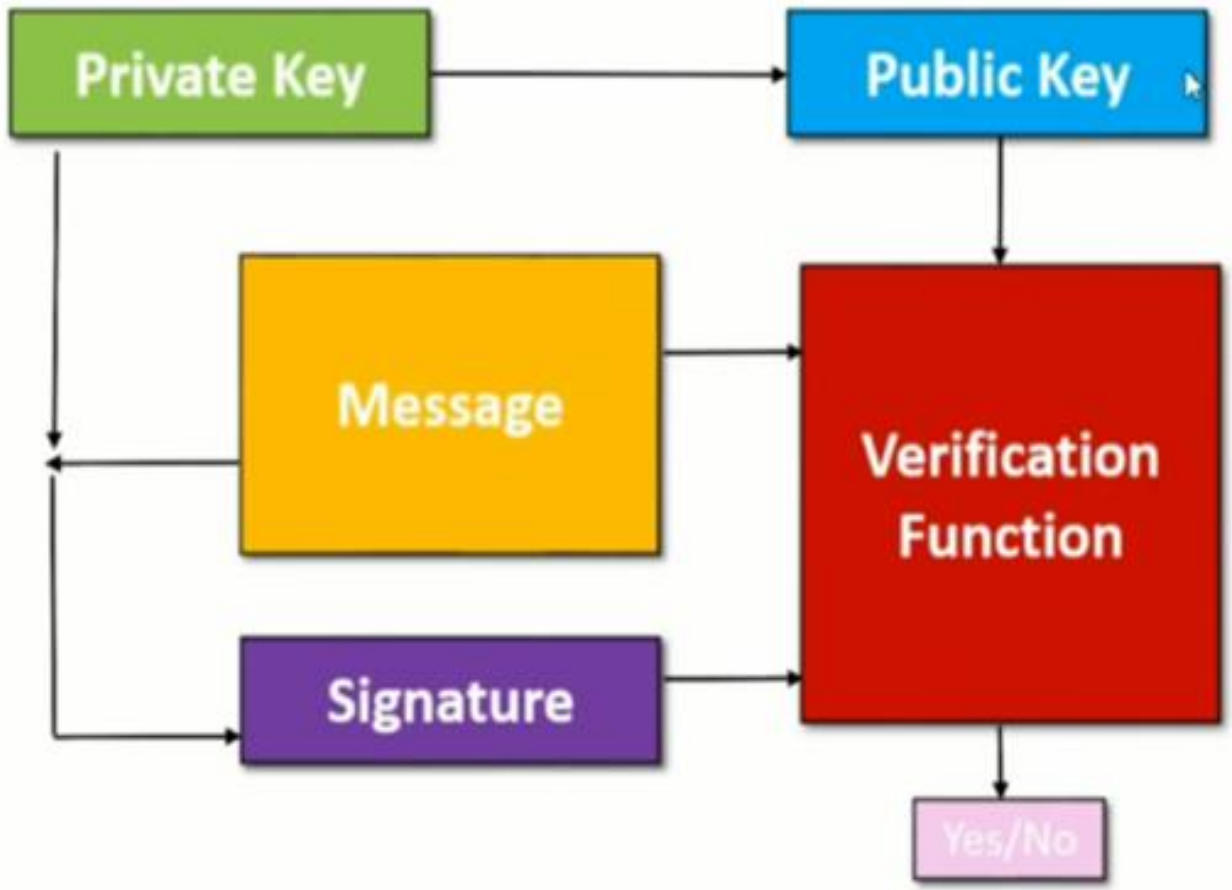
Transaction and UTXOs

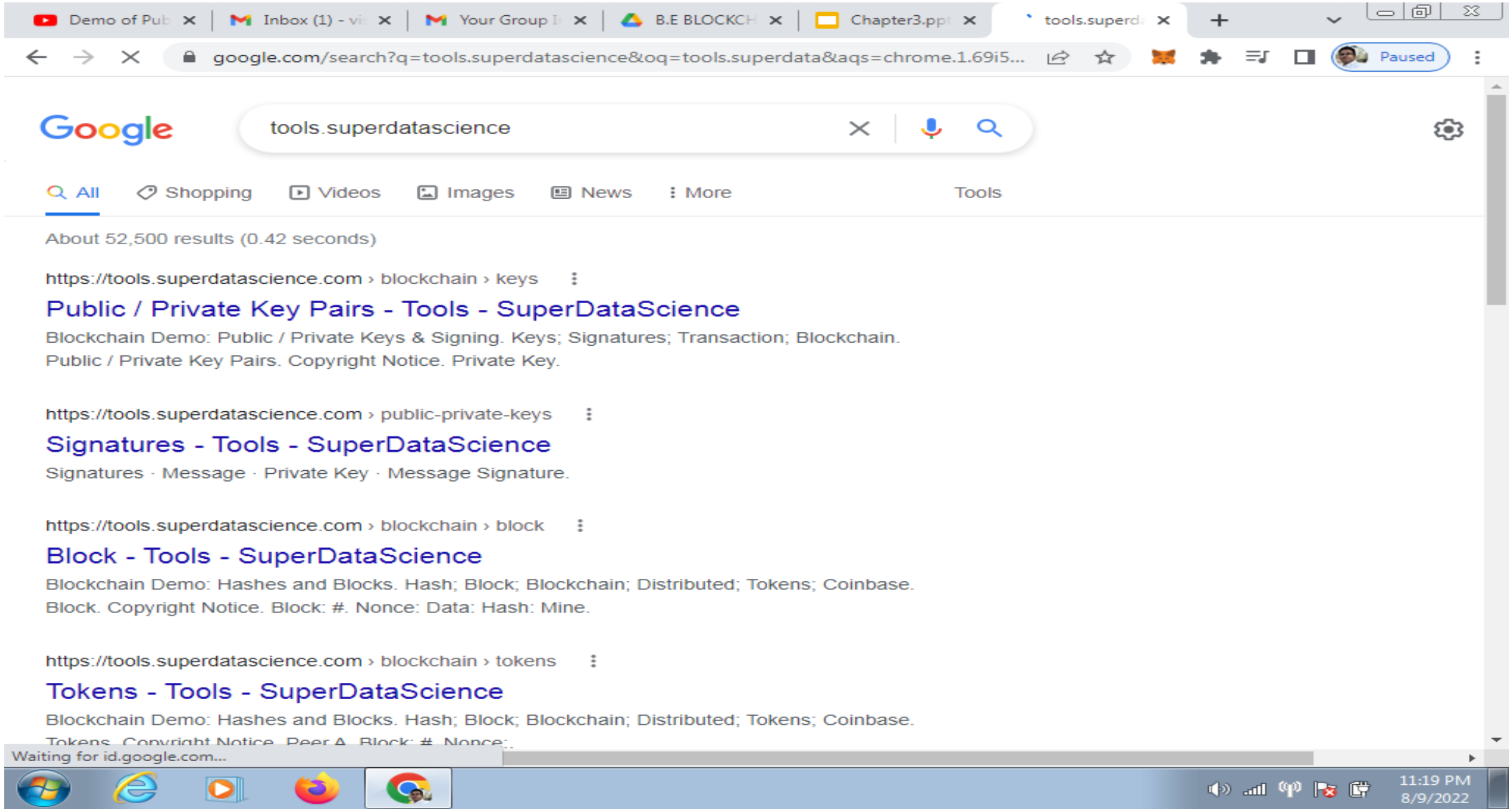


Cryptocurrency Wallets



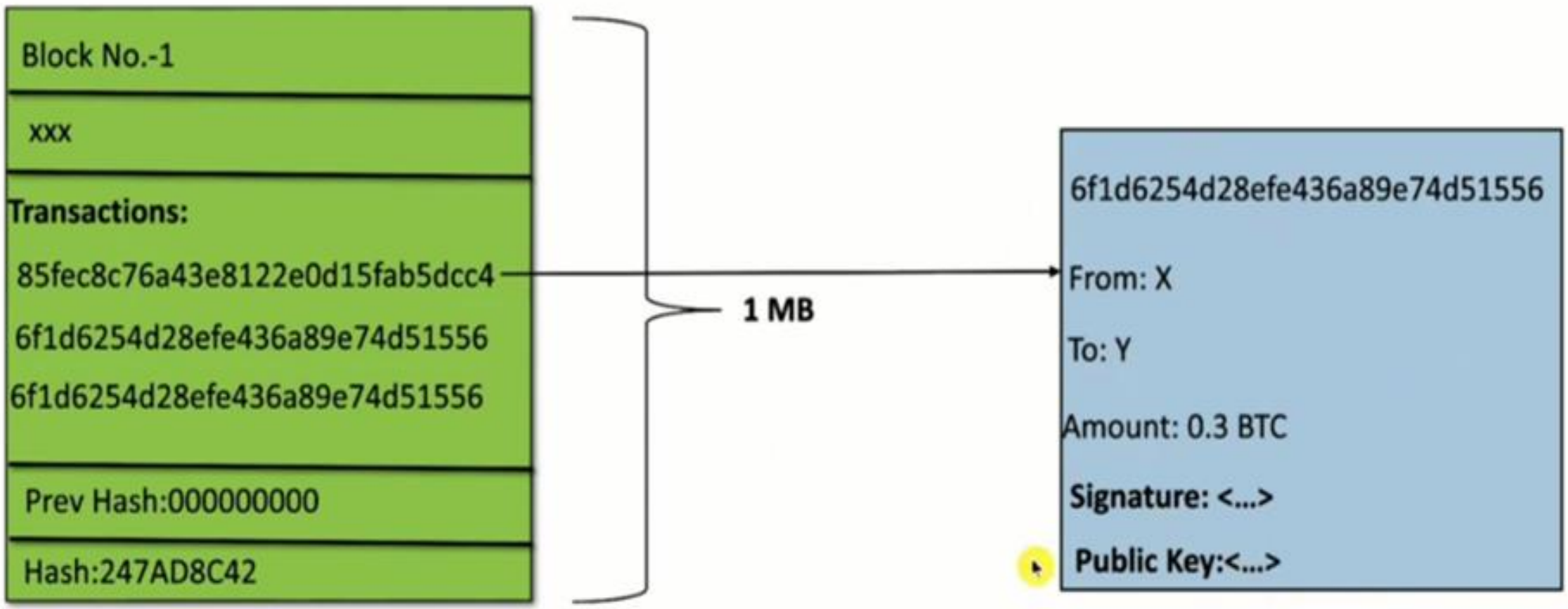
Private and Public Key



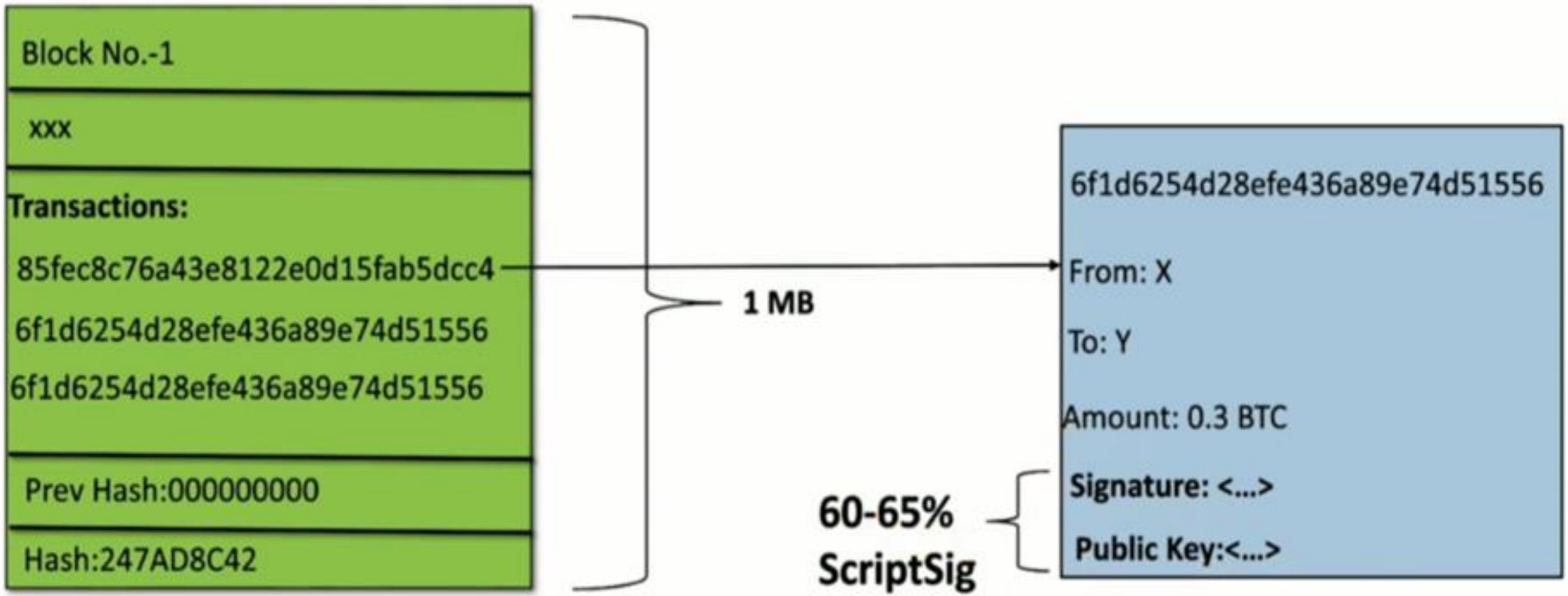

Demo of Pub
Inbox (1) - vi
Your Group I
B.E BLOCKCH
Chapter3.ppt
tools.superda
google.com/search?q=tools.superdatascience&oq=tools.superdata&aqs=chrome.1.69i5...
Paused
Google
tools.superdatascience
All
Shopping
Videos
Images
News
More
Tools
About 52,500 results (0.42 seconds)
https://tools.superdatascience.com › blockchain › keys
Public / Private Key Pairs - Tools - SuperDataScience
Blockchain Demo: Public / Private Keys & Signing. Keys; Signatures; Transaction; Blockchain.
Public / Private Key Pairs. Copyright Notice. Private Key.
https://tools.superdatascience.com › public-private-keys
Signatures - Tools - SuperDataScience
Signatures · Message · Private Key · Message Signature.
https://tools.superdatascience.com › blockchain › block
Block - Tools - SuperDataScience
Blockchain Demo: Hashes and Blocks. Hash; Block; Blockchain; Distributed; Tokens; Coinbase.
Block. Copyright Notice. Block: #. Nonce: Data: Hash: Mine.
https://tools.superdatascience.com › blockchain › tokens
Tokens - Tools - SuperDataScience
Blockchain Demo: Hashes and Blocks. Hash; Block; Blockchain; Distributed; Tokens; Coinbase.
Tokens. Copyright Notice. Peer A. Block: #. Nonce:.
Waiting for id.google.com...
11:19 PM
8/9/2022

https://tools.superdatascience.com/blockchain/public-private-keys/keys

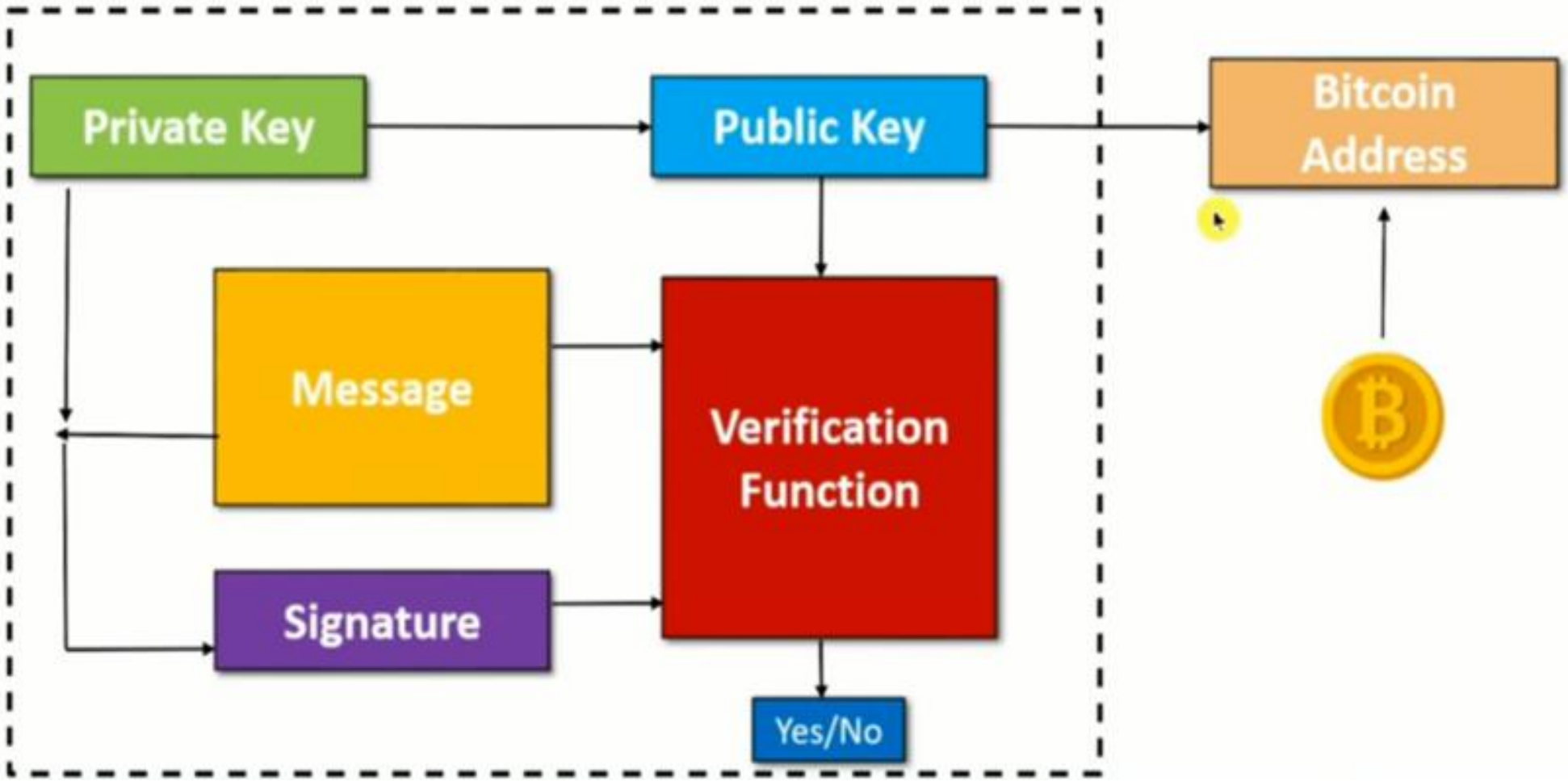
Segregated Witness



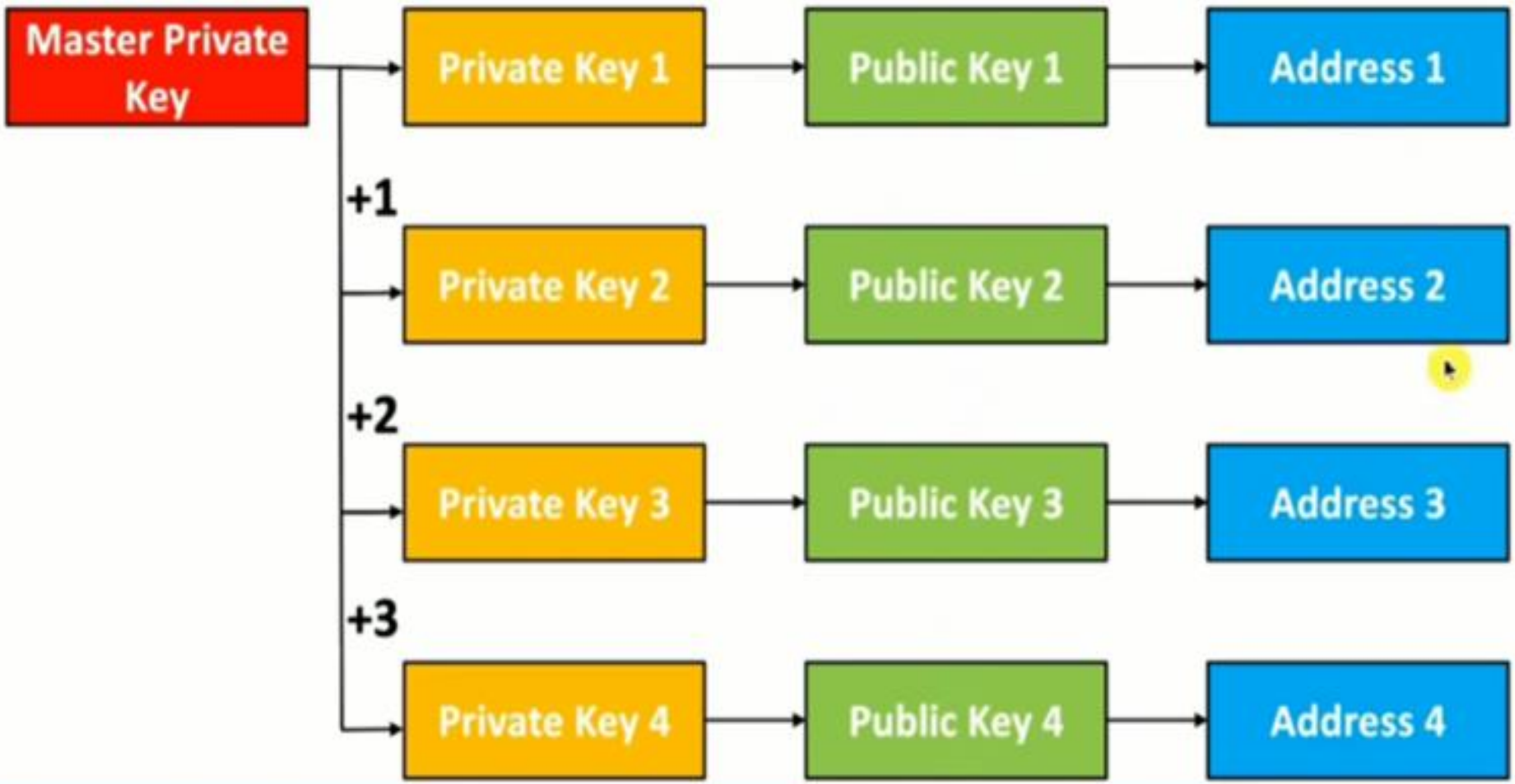
Segregated Witness



Private and Public Key



Hierarchically Deterministic (HD) Wallets



what is Proof of burn ?

Proof of burn is one of the several consensus mechanism algorithms implemented by a blockchain network to ensure that all participating nodes come to an agreement about the true and valid state of the blockchain network. This algorithm is implemented to avoid the possibility of any cryptocurrency coin double-spending.

- Proof of burn (POB) is an alternative consensus algorithm that tries to address the high energy consumption issue of a POW system.
- POB is often called a POW system without energy waste. It operates on the principle of allowing miners to “burn” virtual currency tokens. They are then granted the right to write blocks in proportion to the coins burnt.
- Iain Stewart, the inventor of the POB algorithm, uses an analogy to describe the algorithm: burnt coins are like mining rigs.
- In this analogy, a miner burns their coins to buy a virtual mining rig that gives them the power to mine blocks. The more coins burned by the miner, the bigger their virtual mining "rig" will be.

- To burn the coins, miners send them to a verifiably un-spendable address. This process does not consume many resources (other than the burned coins) and ensures that the network remains active and agile.
- Depending upon the implementation, miners are allowed to burn the native currency or the currency of an alternate chain, such as Bitcoin.
- In exchange, they receive a reward in the native currency token of the blockchain.
- You can send out transactions to the network that will burn your own cryptocurrency coins.
- Other participants can mine/burn on top of your block, and you can also take the transactions of other participants to add them to your block.
- Essentially, all of this burning activity keeps the network agile, and participants are rewarded for their activities (both burning their own coins and burning other people's coins).

To prevent the possibility of unfair advantages for early adopters, the POB system has implemented a mechanism that promotes the periodic burning of cryptocurrency coins to maintain mining power.

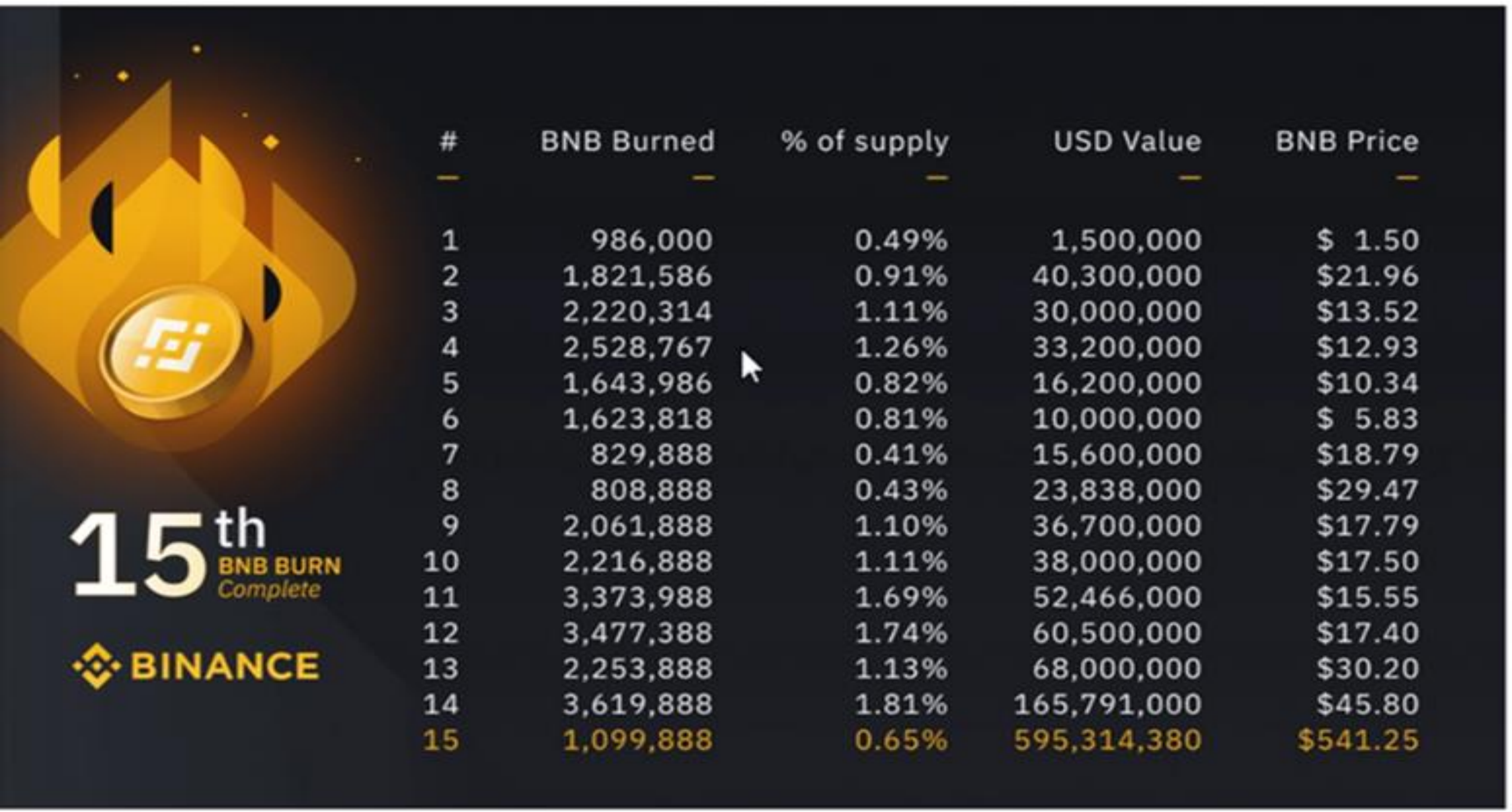
The power of burnt coins “decays” or reduces partially each time a new block is mined. This promotes regular activity by the miners, instead of a one-time, early investment. To maintain a competitive edge, miners may also need to periodically invest in better equipment as technology advances.

Example of Proof of Burn

POB implementation can be customized. For example, Slimcoin, a virtual currency network that uses POB, allows a miner to burn coins that not only gives them the right to compete for the next block but also gives them the chance to receive blocks during a longer time period, for at least a year.

Essentially, Slimcoin's POB implementation combines three algorithms: POW, POS, and the core POB concept.

The process of burning coins utilizes POW; the more coins one burns the more chances one has to mine, thus ensuring POS; and the whole ecosystem follows the POB concept.



#	BNB Burned	% of supply	USD Value	BNB Price
1	986,000	0.49%	1,500,000	$ 1.50
2	1,821,586	0.91%	40,300,000	$21.96
3	2,220,314	1.11%	30,000,000	$13.52
4	2,528,767	1.26%	33,200,000	$12.93
5	1,643,986	0.82%	16,200,000	$10.34
6	1,623,818	0.81%	10,000,000	$ 5.83
7	829,888	0.41%	15,600,000	$18.79
8	808,888	0.43%	23,838,000	$29.47
9	2,061,888	1.10%	36,700,000	$17.79
10	2,216,888	1.11%	38,000,000	$17.50
11	3,373,988	1.69%	52,466,000	$15.55
12	3,477,388	1.74%	60,500,000	$17.40
13	2,253,888	1.13%	68,000,000	$30.20
14	3,619,888	1.81%	165,791,000	$45.80
15	1,099,888	0.65%	595,314,380	$541.25

Market Cap
$52,415,865,239

24 Hour Trading Vol
$4,730,671,118

24h Low / 24h High
$336.44 / $385.86

Circulating Supply
154,533,651 / 170,533,651

Fully Diluted Valuation
$57,842,863,395

Max Supply
170,533,651

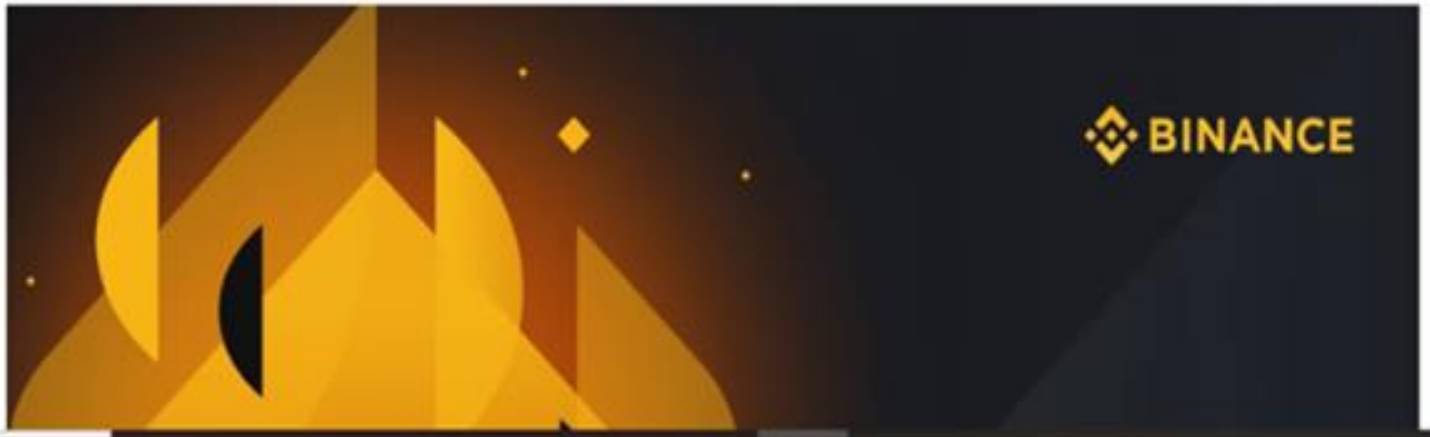
ystem | Exchange-based Tokens

USD

Apr 16
2021

15th BNB Burn | Quarterly Highlights and Insights from CZ

For our 15th quarterly BNB Burn (January to March 2021), ***Binance burned a total of 1,099,888 BNB****, equivalent to $595,314,380 (USD) worth of tokens. Binance CEO CZ also talked about the rise of Binance Smart Chain, the crypto bull run, and more.*



Alt Coins

THETA
THETA

USDT
Tether

LTC
Litecoin

ADA
Cardano

BNB
Binance Coin

LINK
Chainlink

Alt Coins

- Consensus Protocol.
- New Capabilities.
- As of March 2021, there were almost 9,000 cryptocurrencies.
- Ethereum and Binance Coin were the largest altcoins by market capitalization as of March 2021.

- Certain altcoins, such as Ethereum's ether and Ripple's XRP, have already gained traction among mainstream institutions, resulting in high valuations.
- Investors can choose from a wide variety of altcoins that perform different functions in the crypto economy.

and thin liquidity. As a result, their prices are more volatile as compared to Bitcoin.

- It is not always easy to distinguish between different altcoins and their respective use cases, making investing decisions even more difficult and confusing.
- There are several "dead" altcoins that ended up sinking investor dollars.

Early Examples of Altcoins

The earliest notable altcoin, Namecoin, was based on the Bitcoin code and used the same proof-of-work algorithm. Like Bitcoin, Namecoin is limited to 21 million coins. Introduced in April 2011, Namecoin primarily diverged from Bitcoin by making user domains less visible. Namecoin allowed users to register and mine using their own .bit domains, which was intended to increase anonymity and censorship resistance.

Introduced in October 2011, Litecoin was branded as the "silver to Bitcoin's gold." While fundamentally similar in code and functionality to Bitcoin, Litecoin differs from Bitcoin in several essential ways. It allows mining transactions to be approved more frequently. It also provides for a total of 84 million coins to be

https://www.investopedia.com/terms/a/altcoin.asp

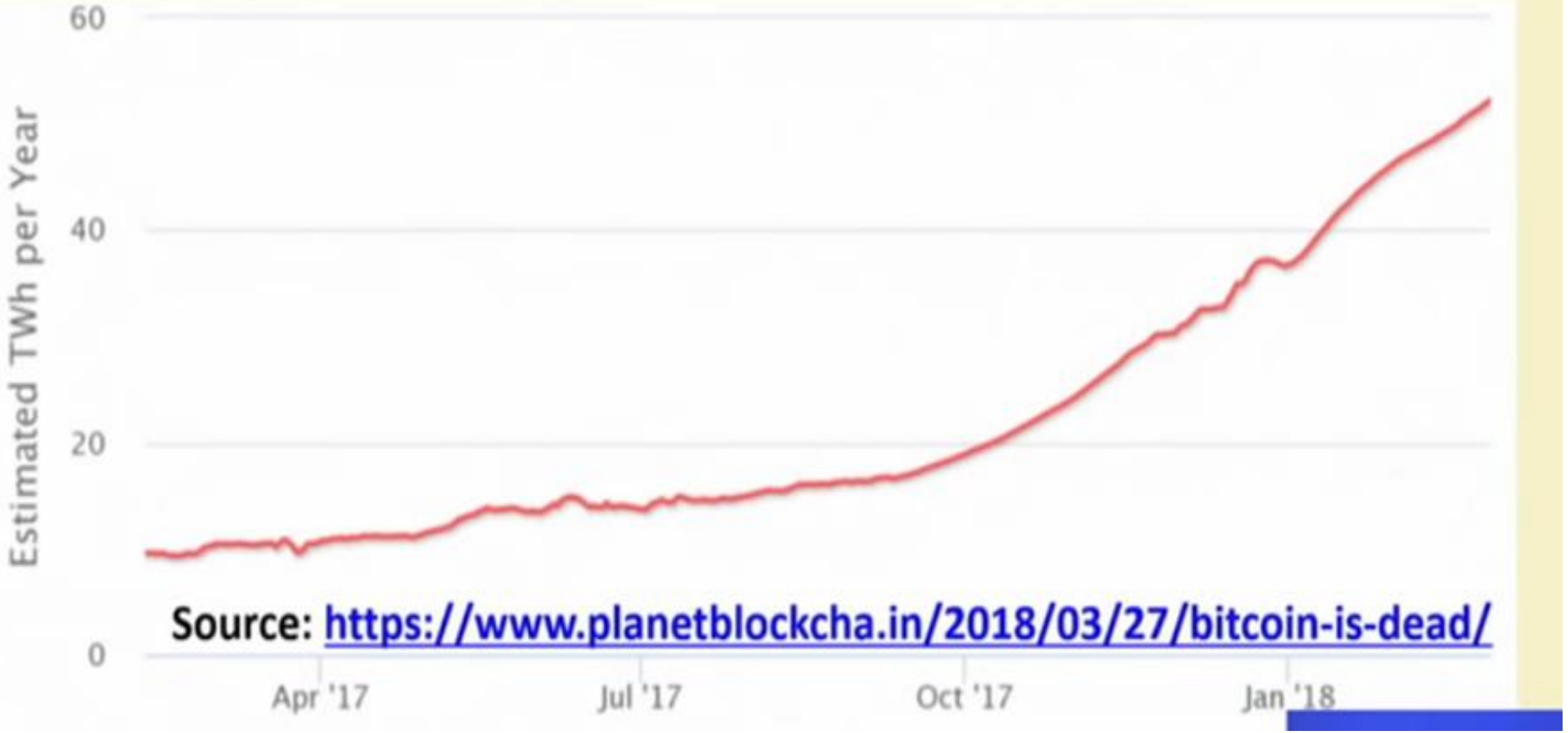
Breaking Bitcoin PoW

- Bitcoin PoW is **computationally difficult** to break, but not **impossible**
- Attackers can deploy high power servers to do more work than the total work of the blockchain
- A known case of successful double-spending
  - (November 2013) "it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against *BetCoin Dice*, a gambling site" [Source: https://en.bitcoin.it/]

The Monopoly Problem

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work
- Monopoly can increase over time (*Tragedy of the Commons*)
  - Miners will get less reward over time
  - Users will get discouraged to join as the miner
  - Few miners with large computing resources may get control over the network

PoW Power Consumption



Source: https://www.planetblockcha.in/2018/03/27/bitcoin-is-dead/

Handling Monopoly and Power Consumption - Proof of Stake (PoS)

- Possibly proposed in 2011 by a Member in Bitcoin Forum - https://bitcointalk.org/index.php?topic=27787.0
  - Make a transition from PoW to PoS when bitcoins are widely distributed

- PoW vs PoS
  - PoW: Probability of mining a block depends on the work done by the miner
  - PoS: Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks.

Proof of Stake (PoS)

- Provides increased protection
  - Executing an attack is expensive, you need more Bitcoins
  - Reduced incentive for attack – the attacker needs to own a majority of bitcoins – an attack will have more affect on the attacker

- Variants of "stake"
  - Randomization in combination of the stake (*used in Nxt and BlackCoin*)
  - Coin-age: Number of coins multiplied by the number of days the coins have been held (*used in Peercoin*)

Proof of Burn (PoB)

- Miners should show proof that they have *burned* some coins
  - Sent them to a verifiably un-spendable address
  - Expensive just like PoW, but no external resources are used other than the burned coins
- PoW vs PoB – Real resource vs virtual/digital resource
- PoB works by burning PoW mined cryptocurrencies

PoW vs PoS vs PoB

PoW

- Do some work to mine a new block
- Consumes physical resources, like CPU power and time
- Power hungry

PoS

- Acquire sufficient stake to mine a new block
- Consumes no external resource, but participate in transactions
- Power efficient

PoB

- Burn some wealth to mine a new block
- Consumes virtual or digital resources, like the coins
- Power efficient

Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications

- **Basic idea:**
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

PoET over Trusted Environments

- How will one verify that the proposer has **really waited** for a **random amount of time**?
  - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform
  - The trusted code is private to the rest of the application
  - The specialized hardware provides an attestation that the trusted code has been set up correctly