

Blockchain



Contents

Module A - Blockchain



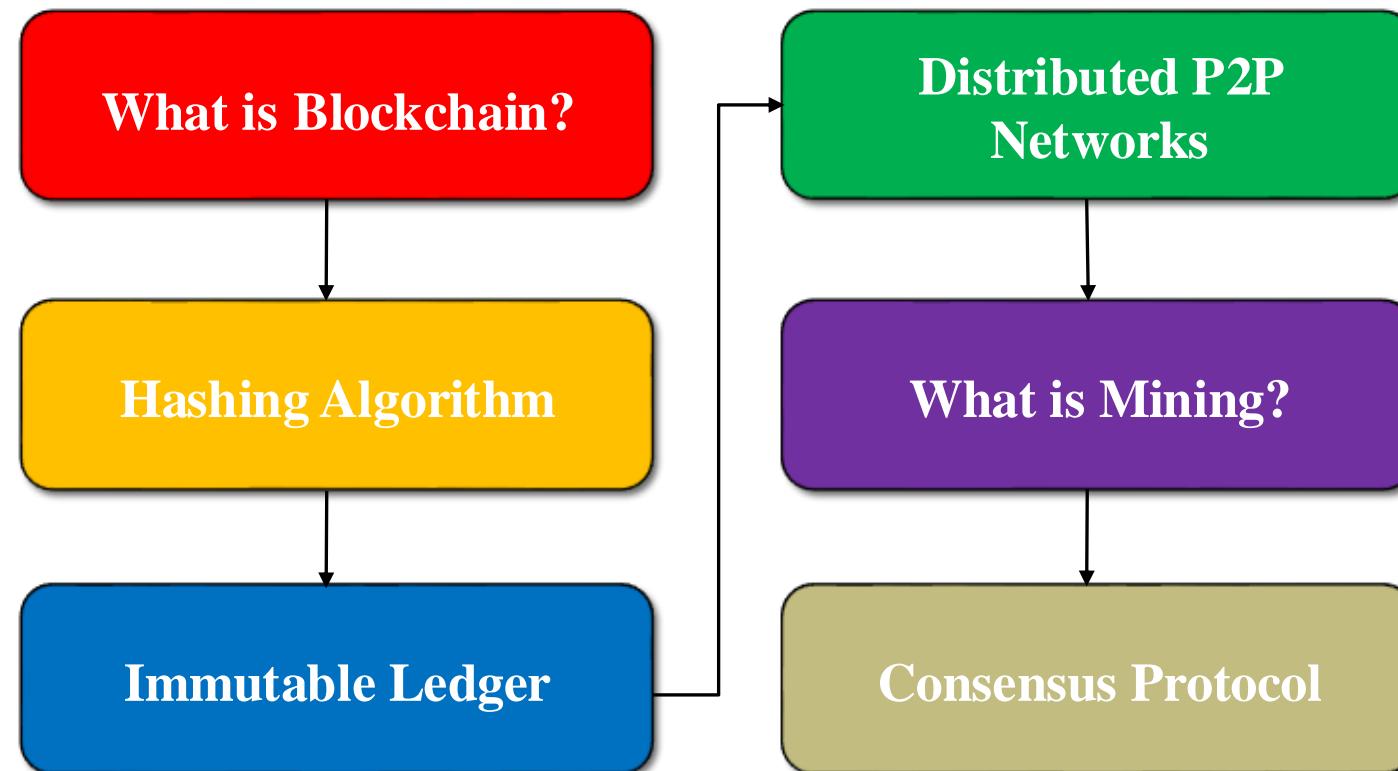
Module B - Cryptocurrency



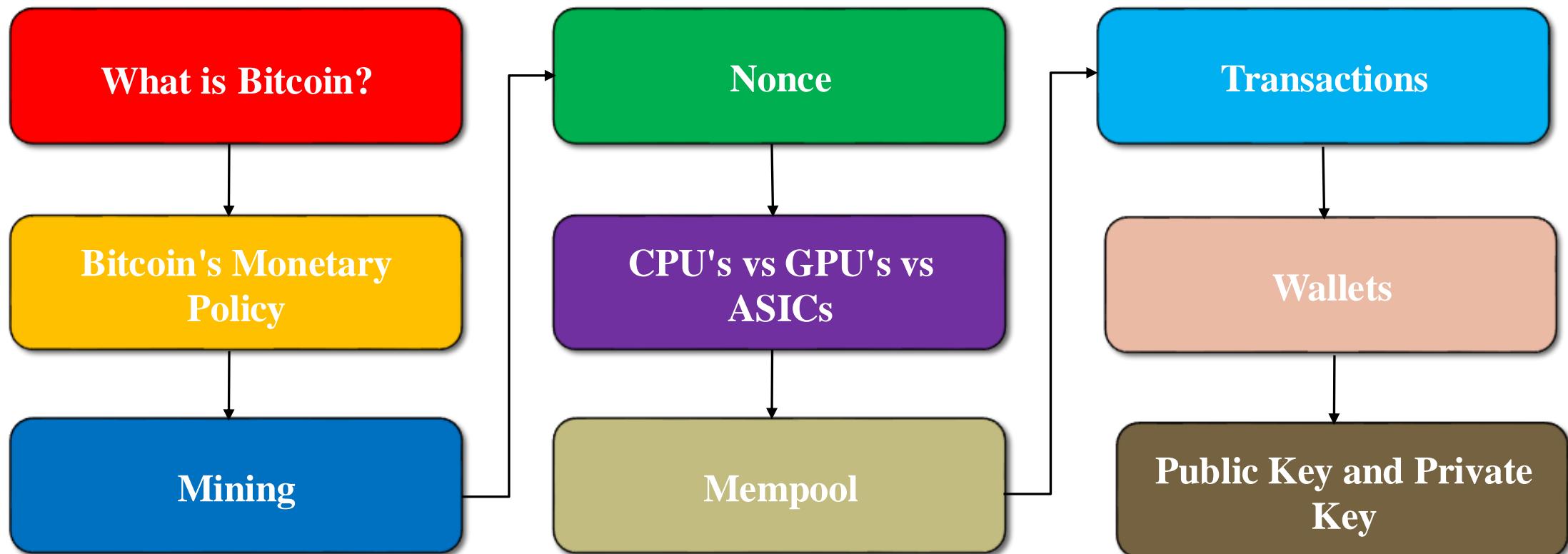
Module C – Smart Contract



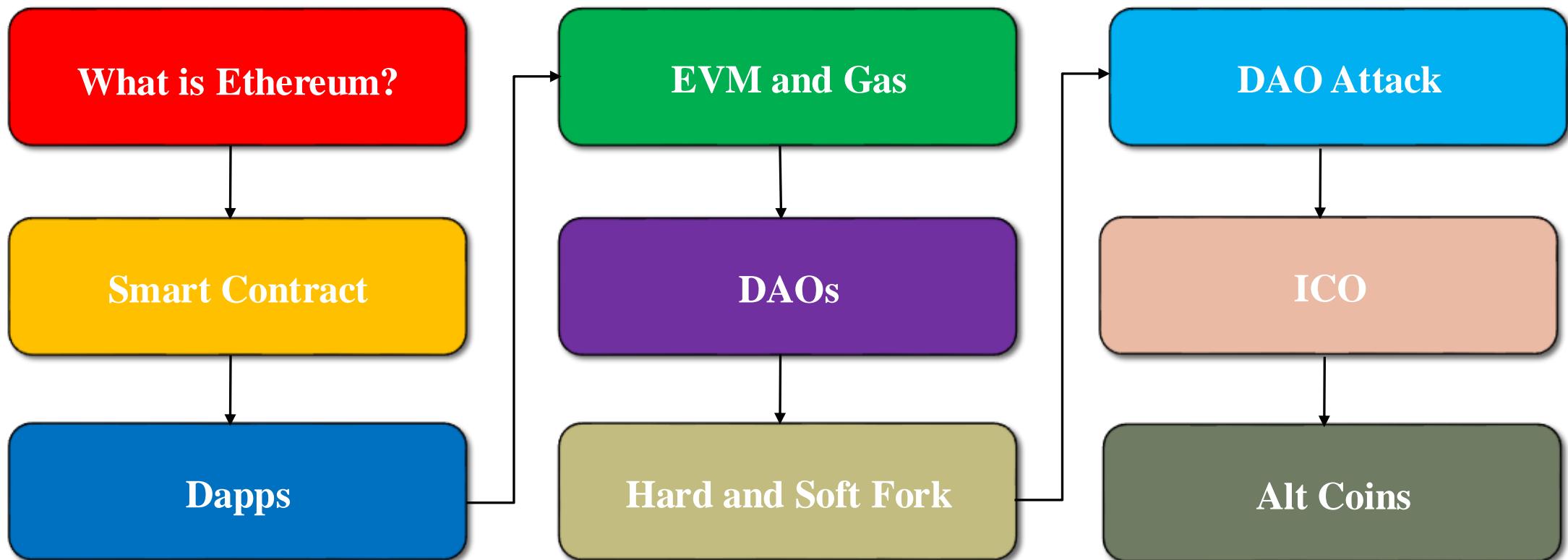
Contents – Module A



Contents – Module B

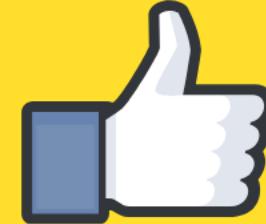


Contents – Module C



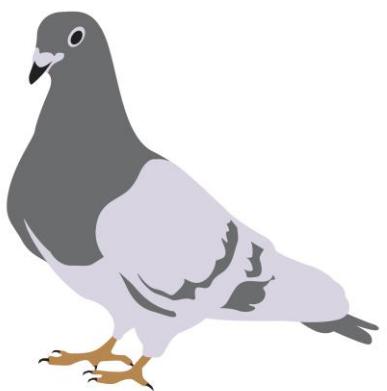
**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Why study blockchain ?

Story of internet



Story of internet



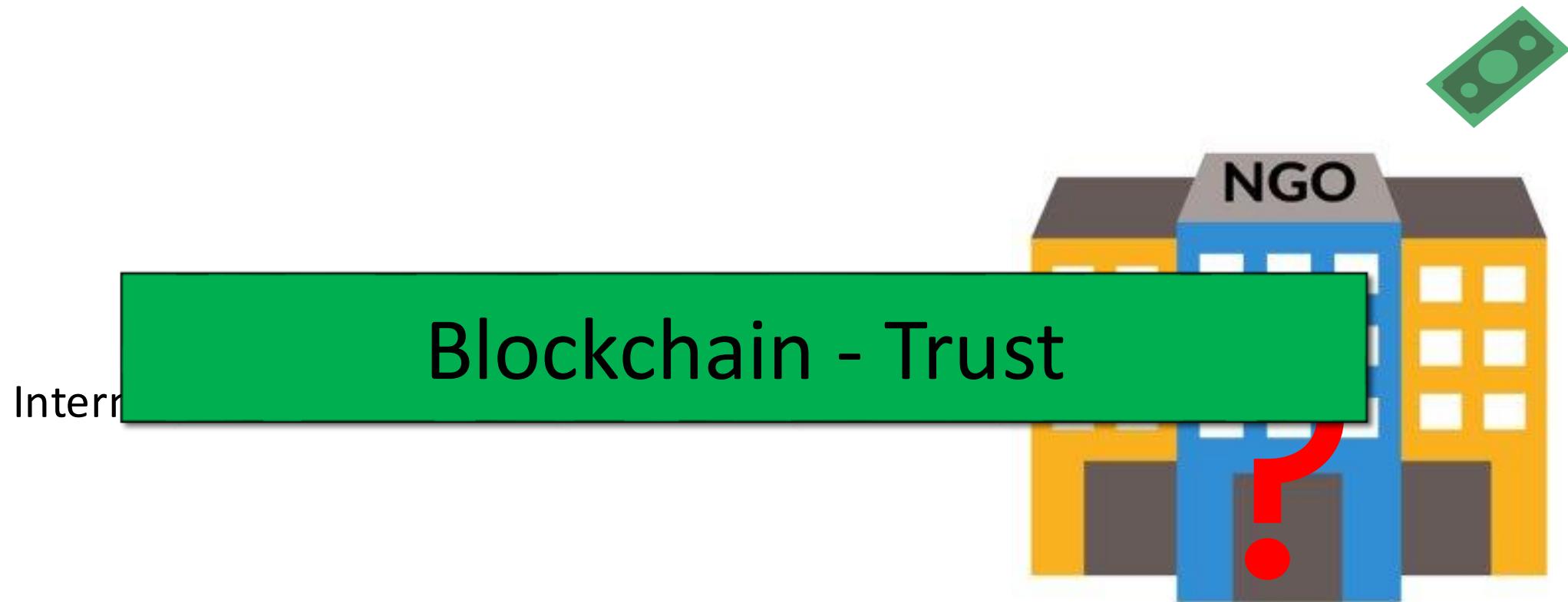
Trust

Story of internet

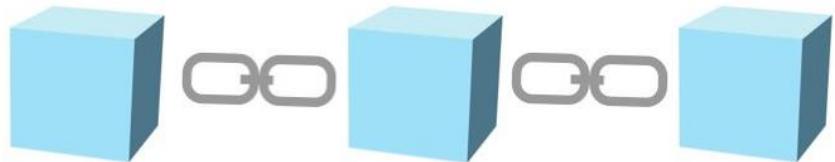
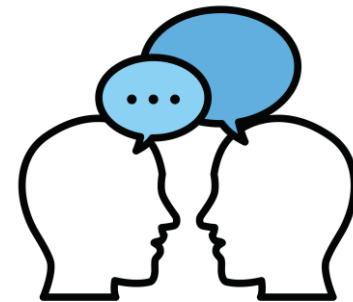
Internet Transaction

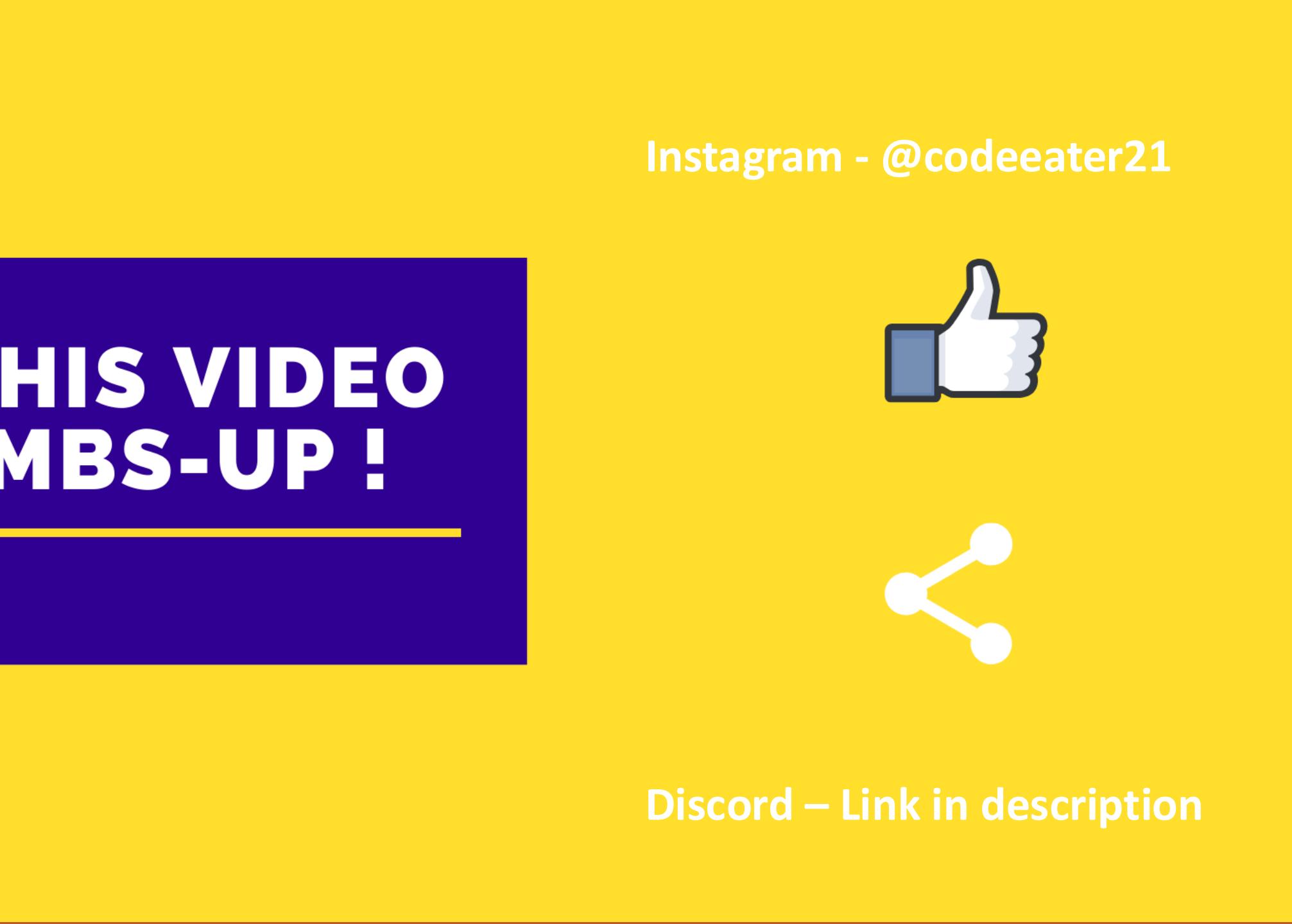


TRUST issues with internet



Disruptive Technology





GIVE THIS VIDEO A THUMBS-UP !

CODE EATER

Instagram - @codeeater21

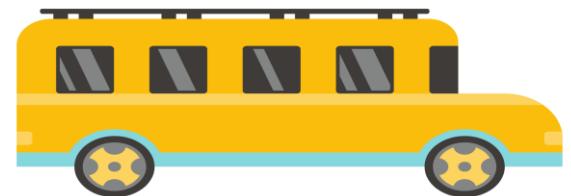


Discord – Link in description

Why should I study Blockchain?

- Because Blockchain is a disruptive technology.

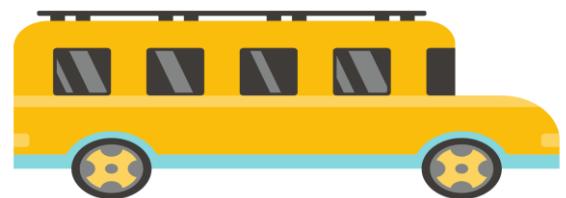
Q) What is a disruptive technology?



Why should I study Blockchain?

- Because Blockchain is a disruptive technology.

Q) What is a disruptive technology?

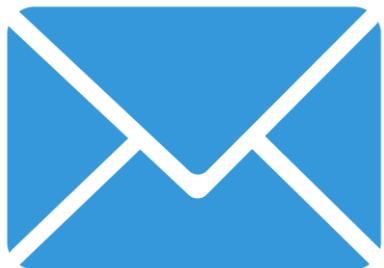


Why should I study Blockchain?

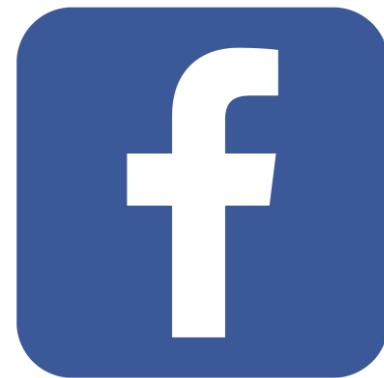


Why should I study Blockchain?

Internet:



Email



Social Media

Why should I study Blockchain?

Internet → Communication

Blockchain → Trust

Why should I study Blockchain?



Why should I study Blockchain?



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



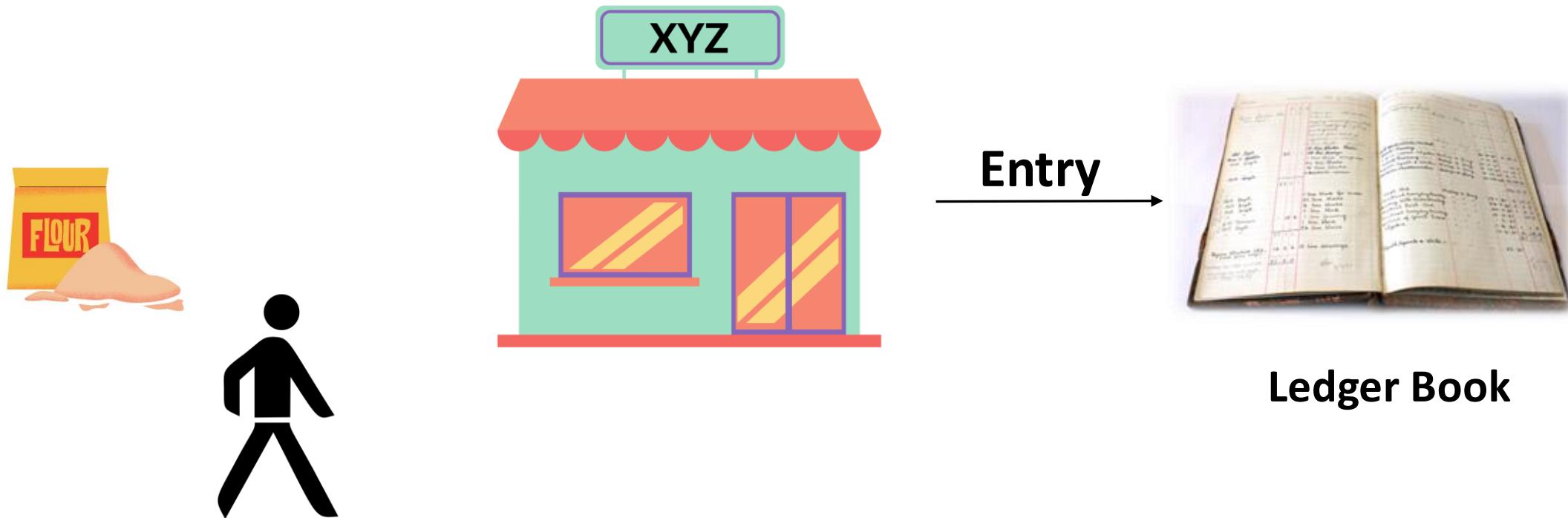


Stuart Haber

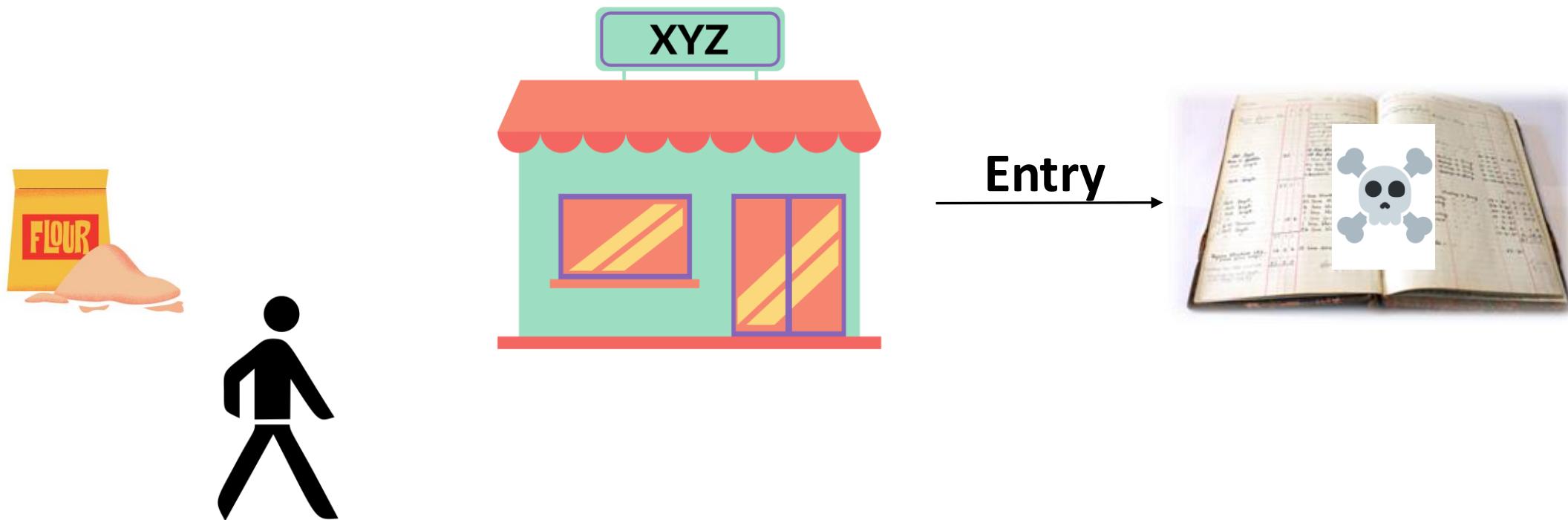


W. Scott Stornetta

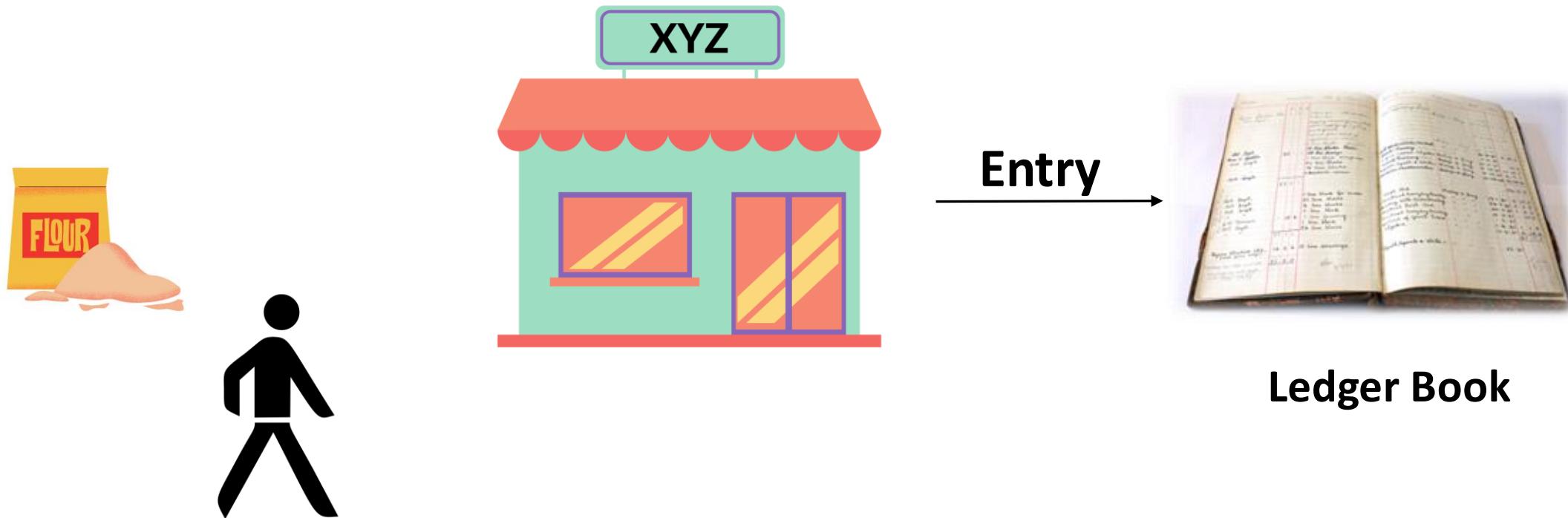
What is Blockchain?



What is Blockchain?



What is Blockchain?





What is Blockchain?

Inventors Of Blockchain

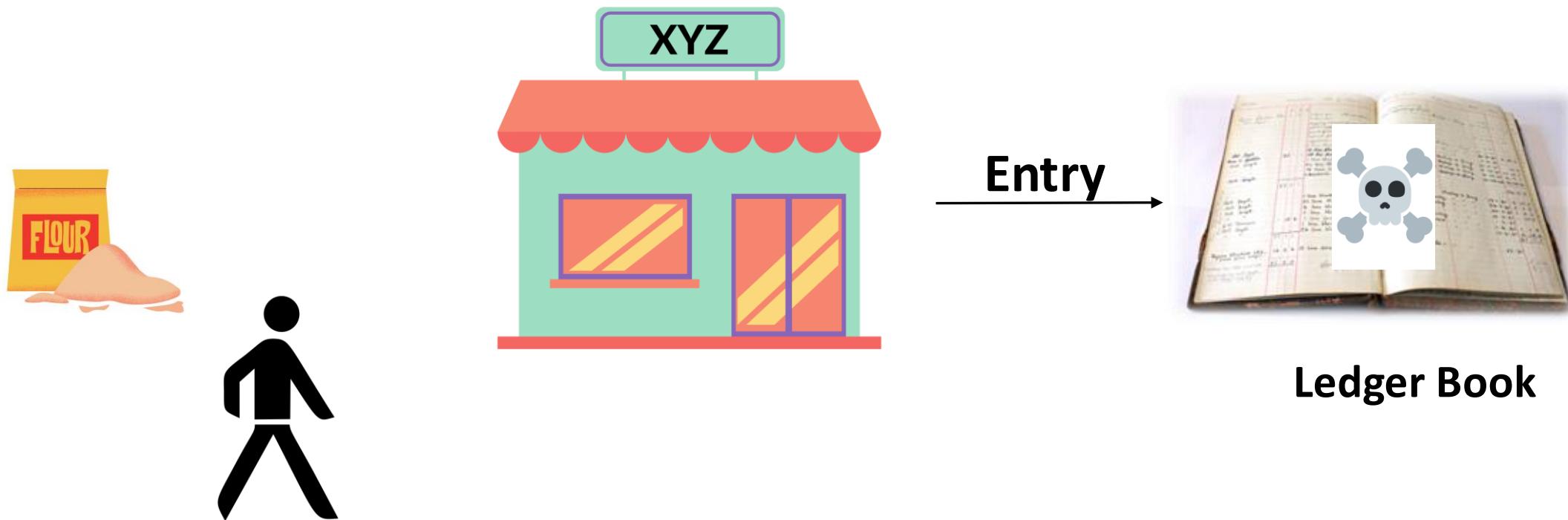


Stuart Haber



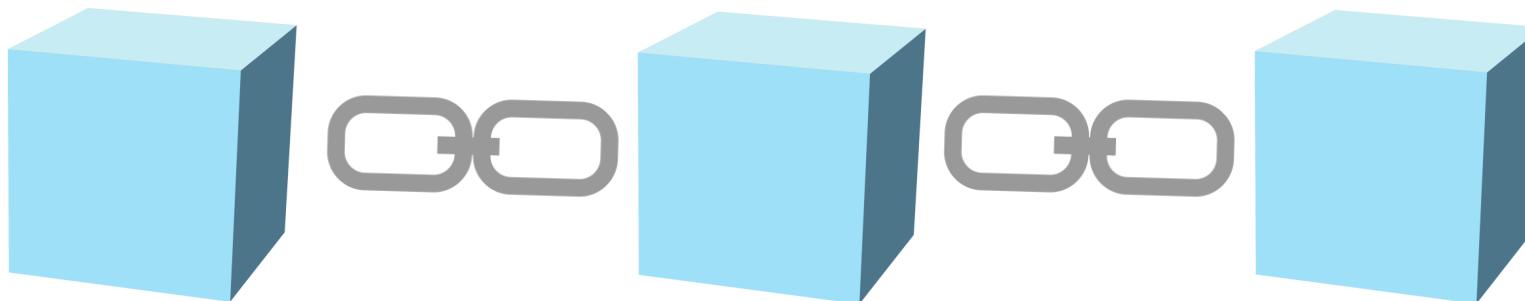
W. Scott Stornetta

What is Blockchain?

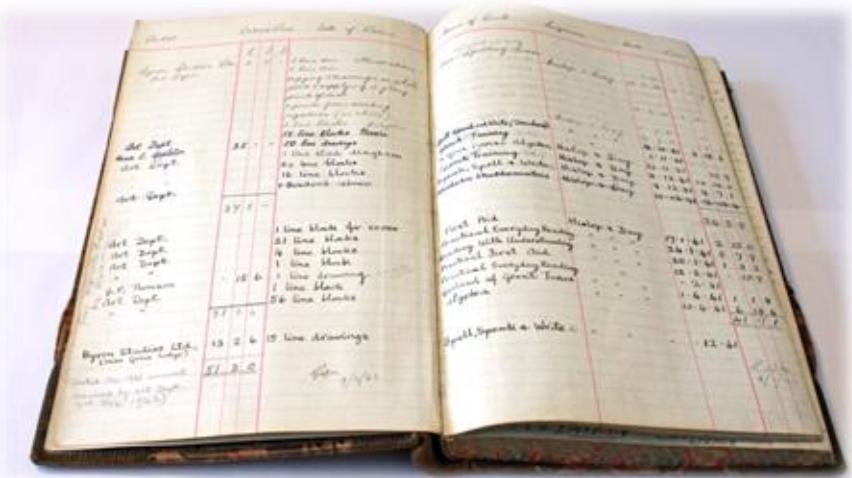


What is Blockchain?

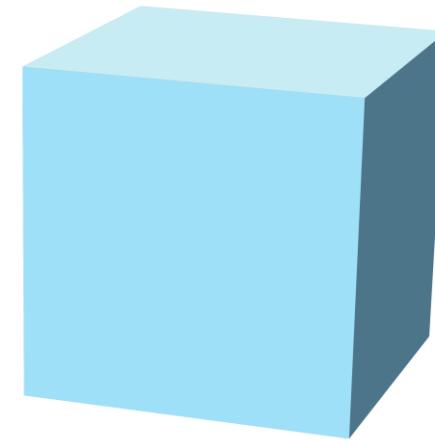
Blockchain is a **distributed immutable ledger** which is completely **transparent**.



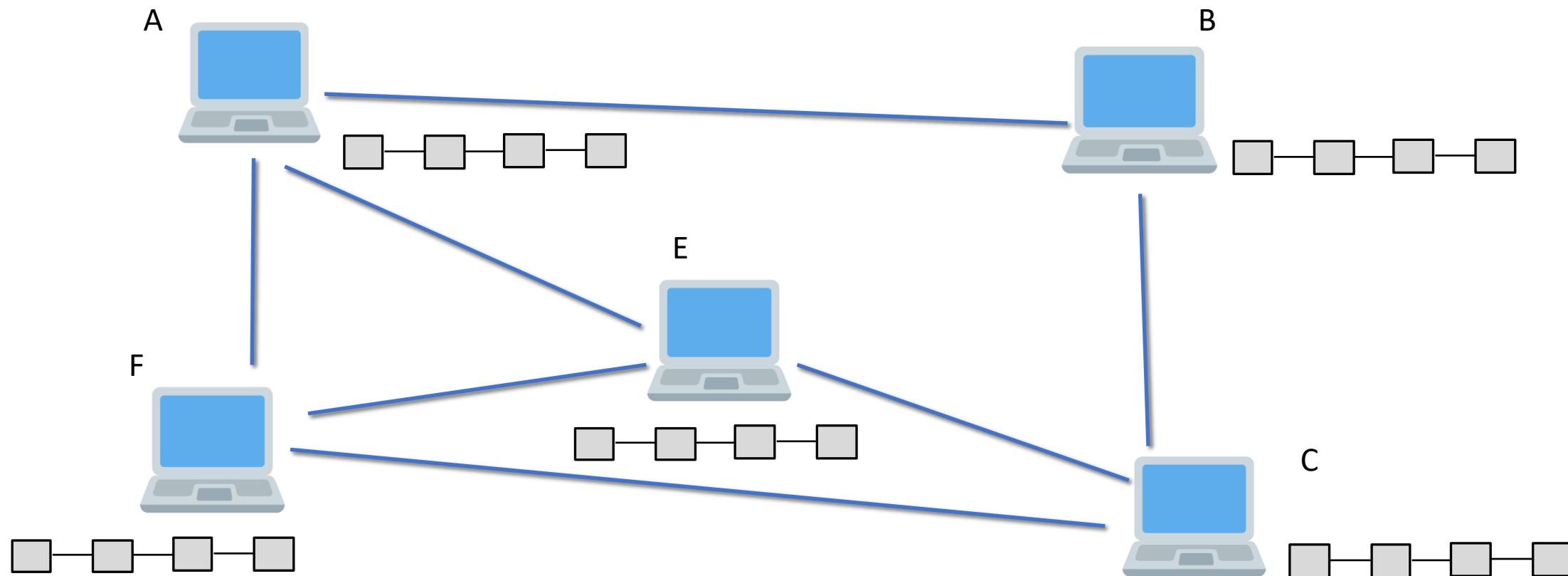
What is Blockchain?

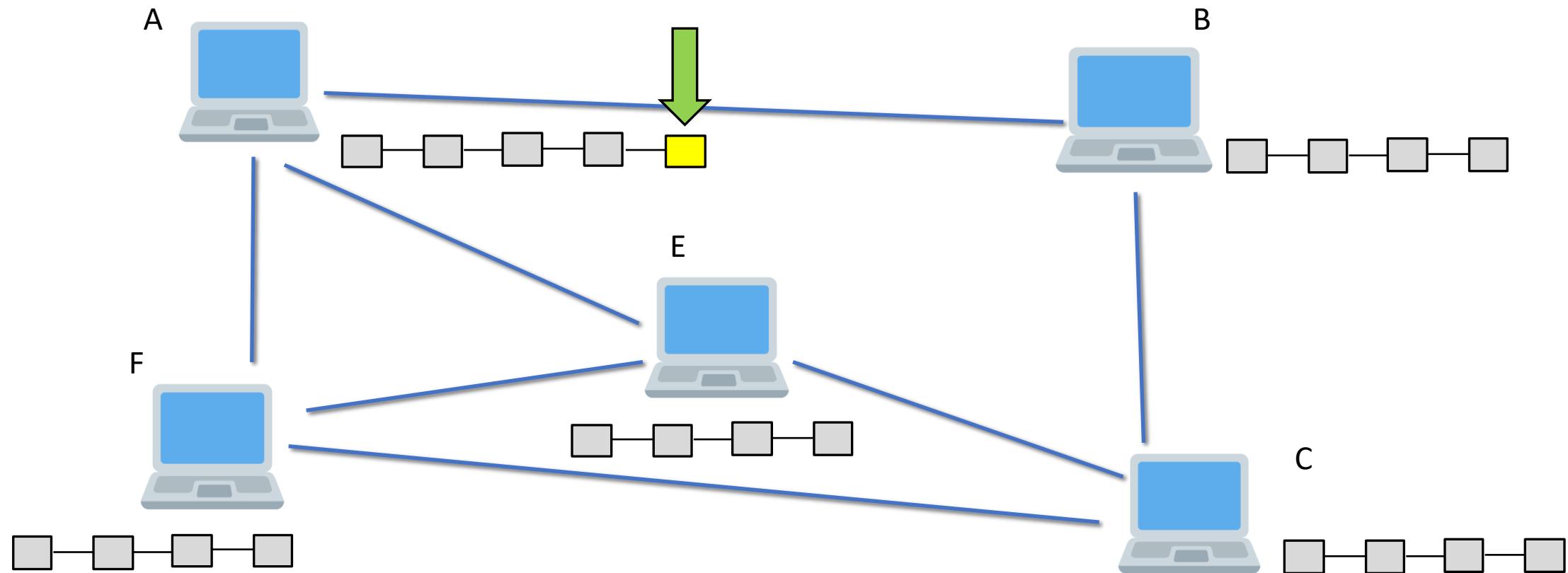


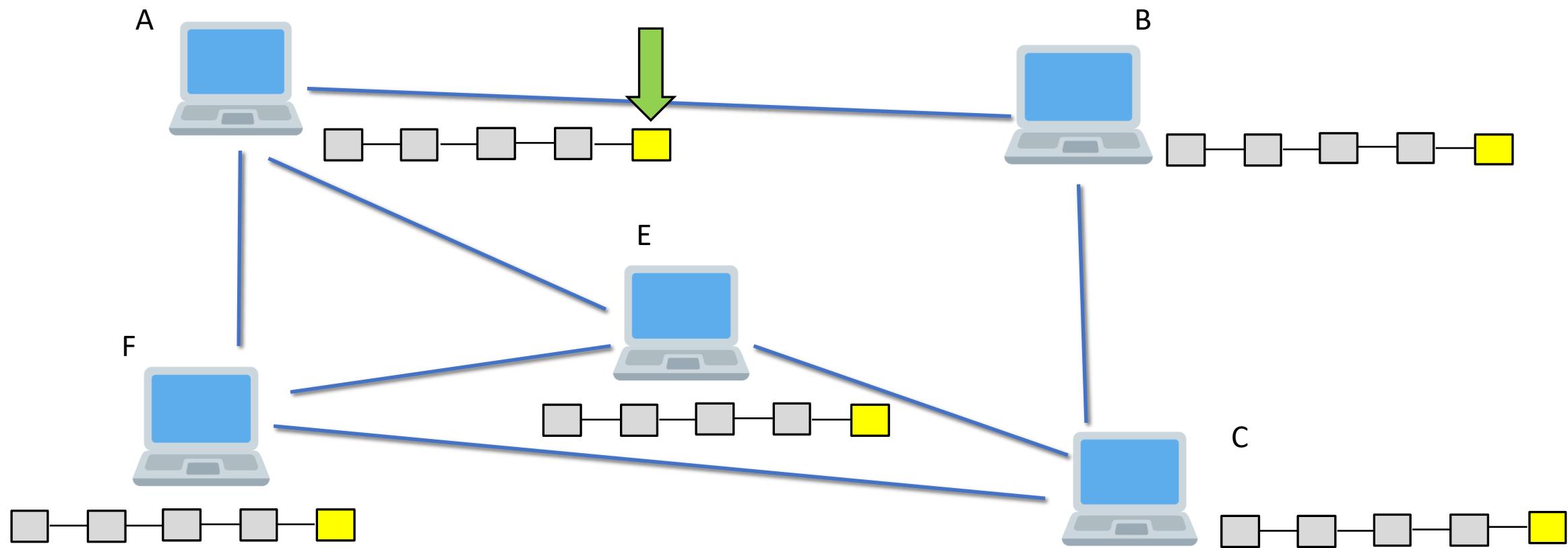
Ledger Book



Block





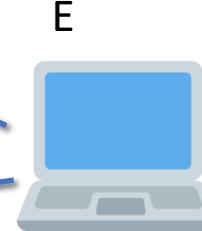




A



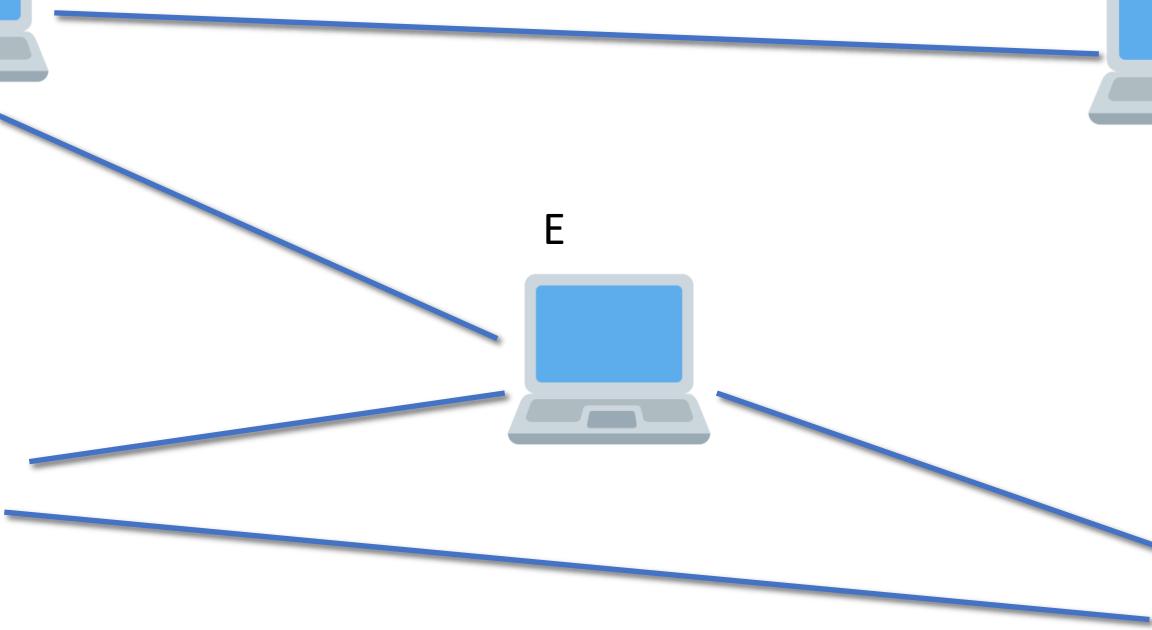
B

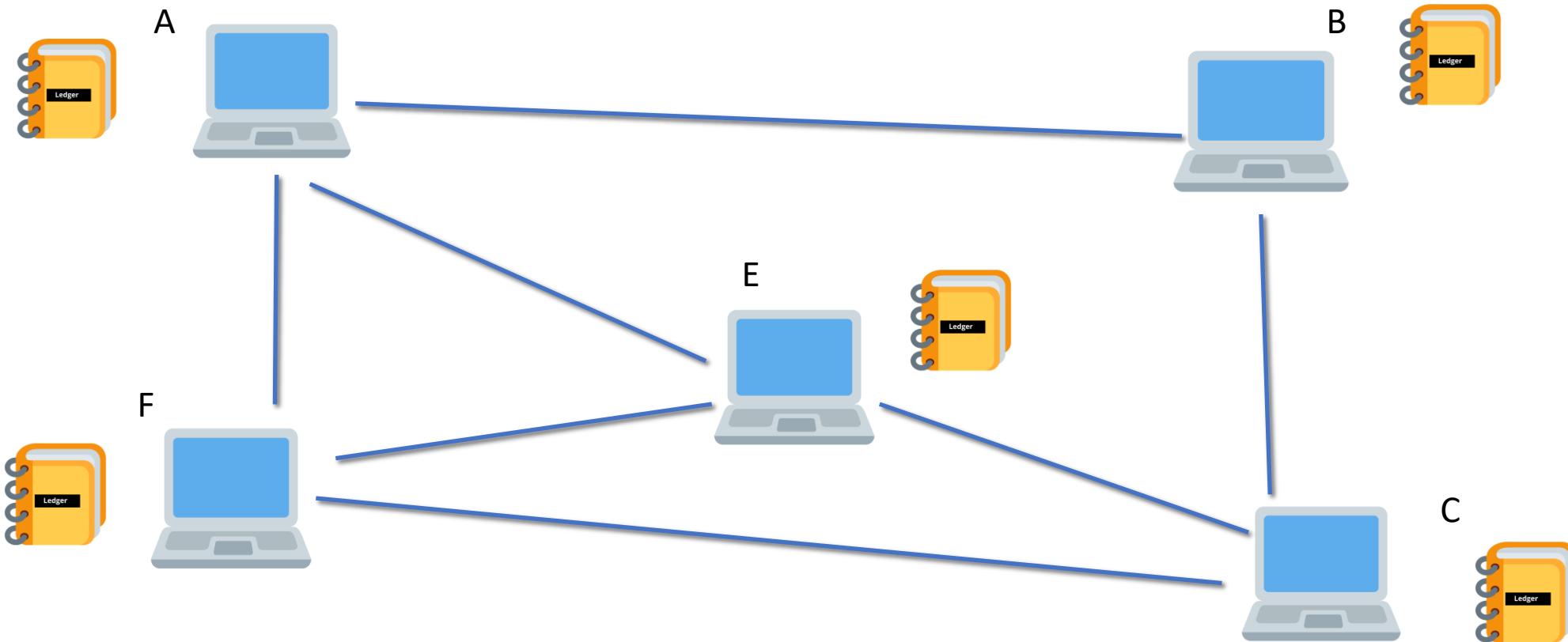


F



C





**GIVE THIS VIDEO
A THUMBS-UP !**

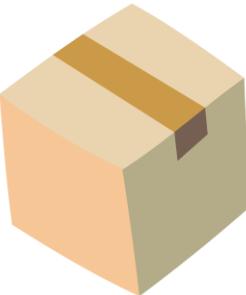
CODE EATER



Applications of Blockchain

Applications of Blockchain

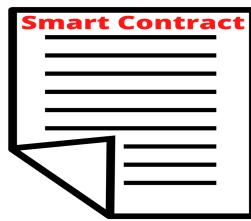
Product Tracking



Healthcare System



Smart Contracts



International Wire Transfer

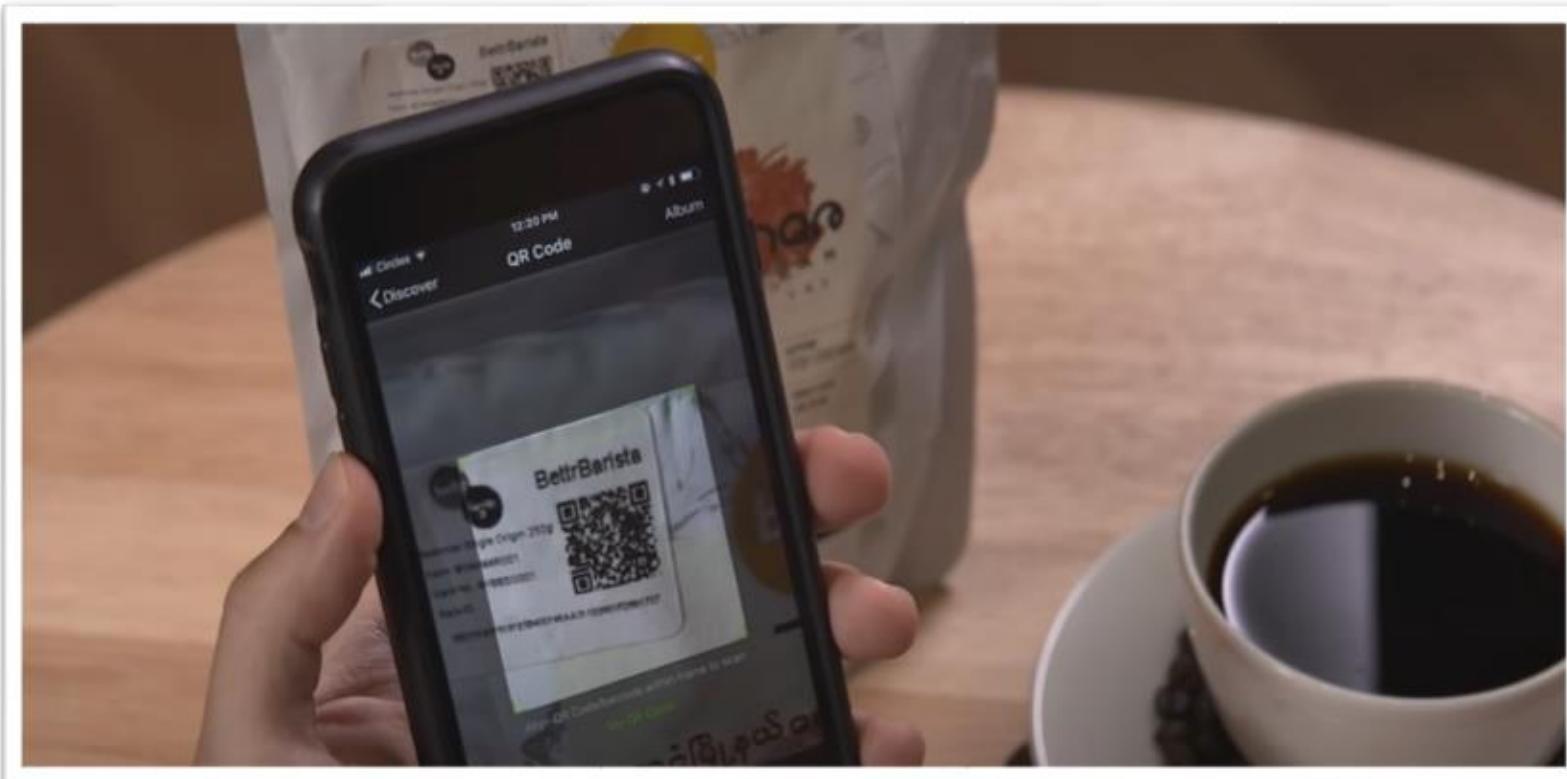


Product Tracking



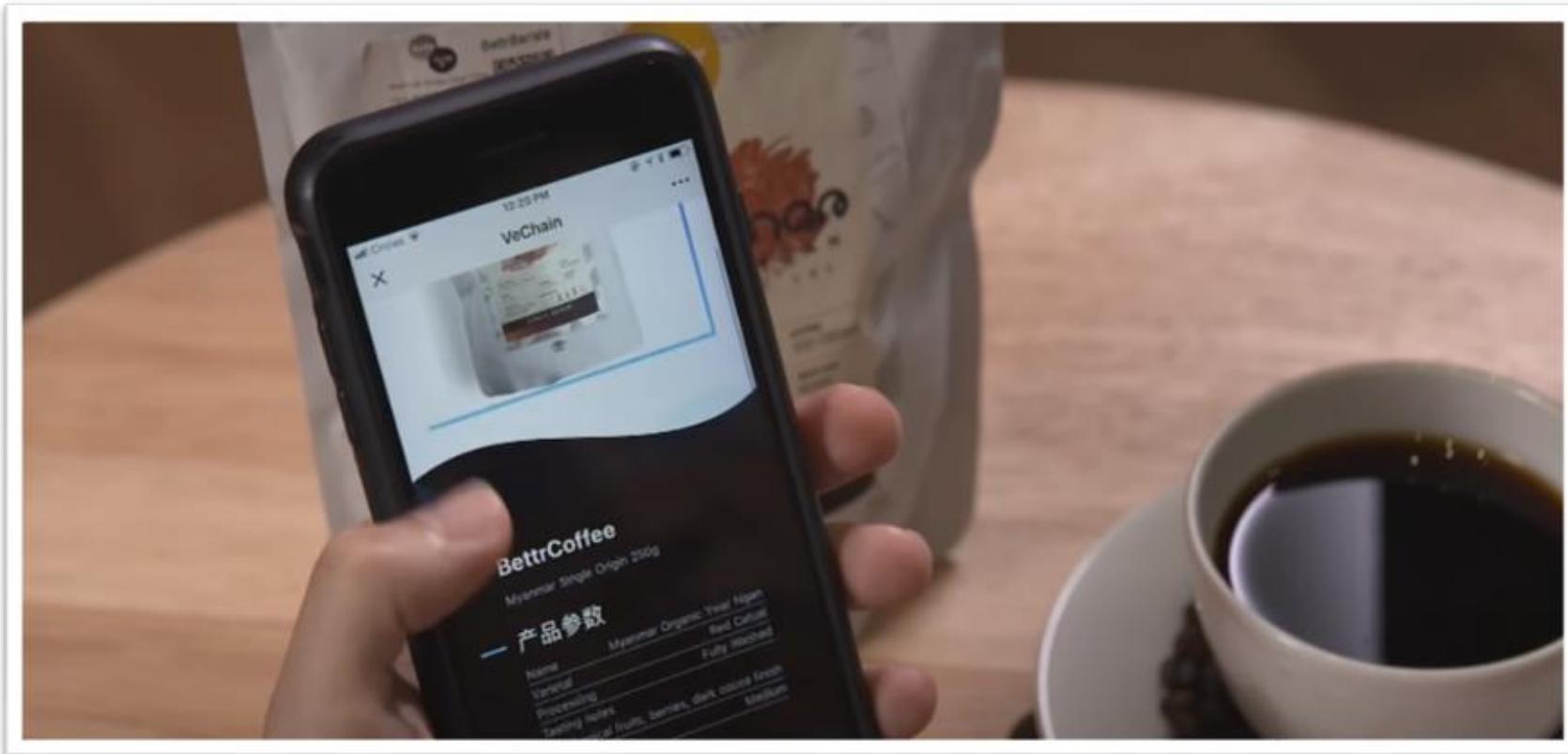
Coffee

Product Tracking



Scan Barcode

Product Tracking



Product Tracking



Applications of Blockchain

Smart Contract

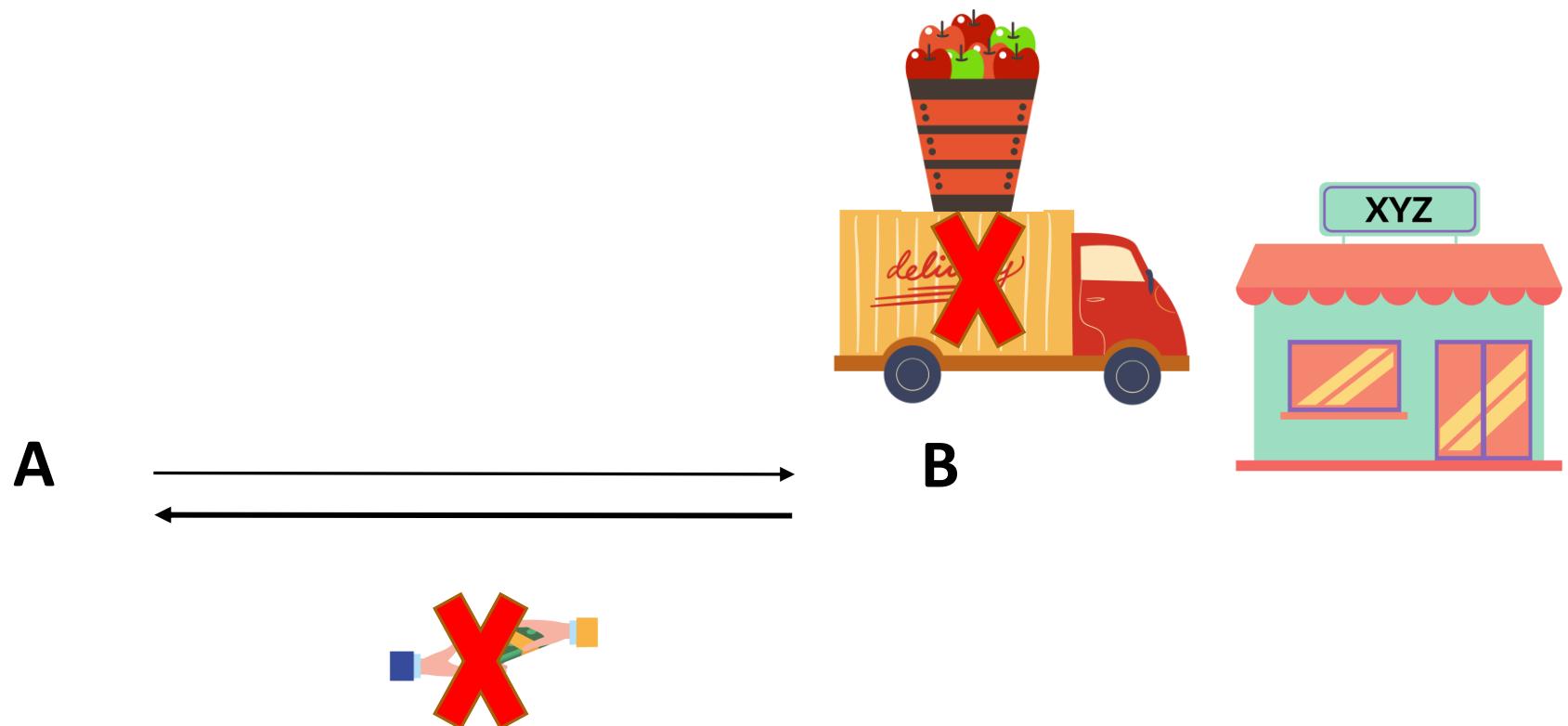


A

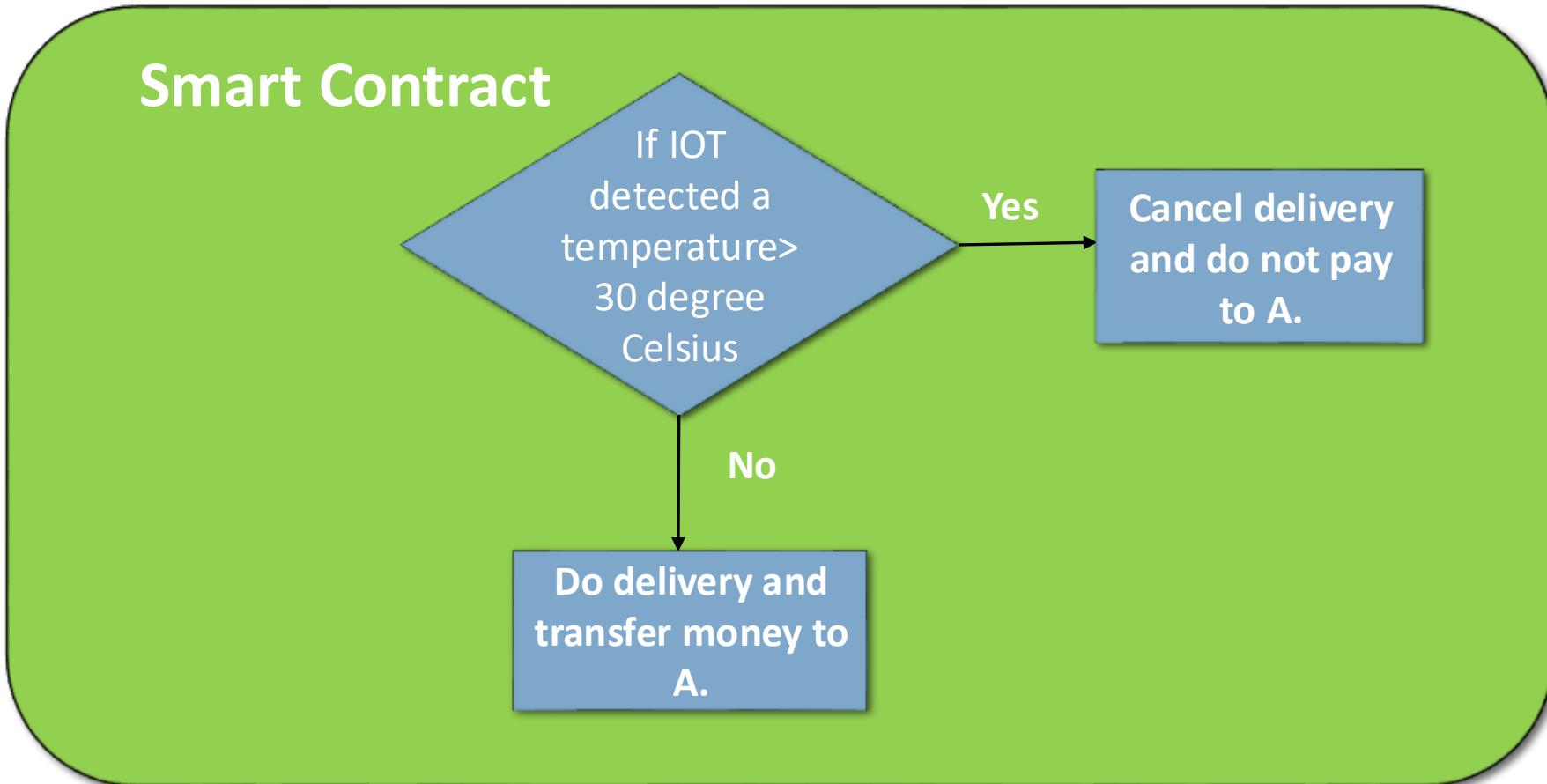


B

Smart Contract

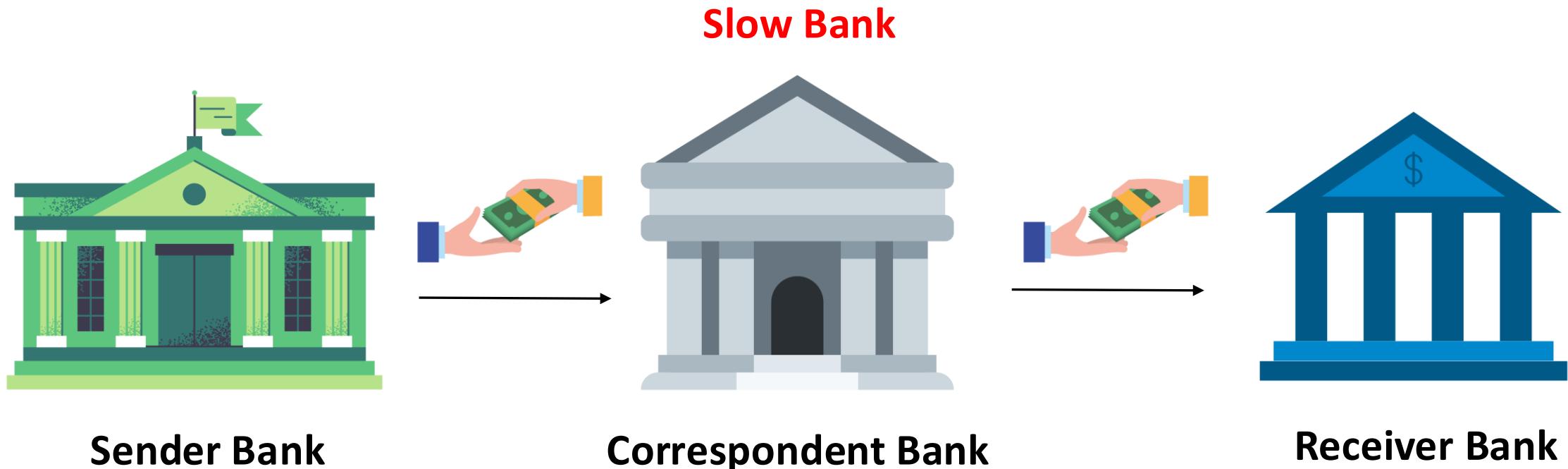


Smart Contract

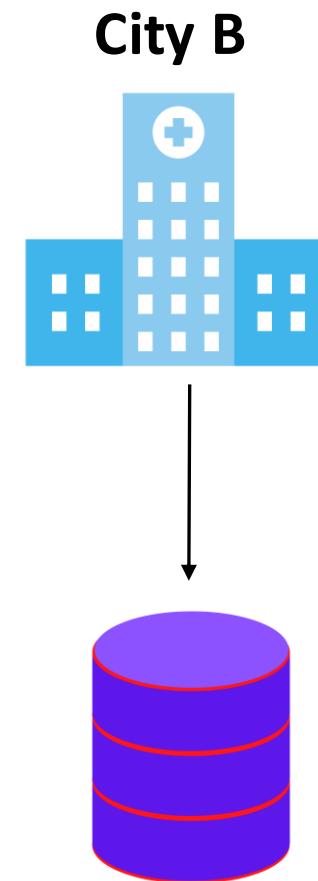
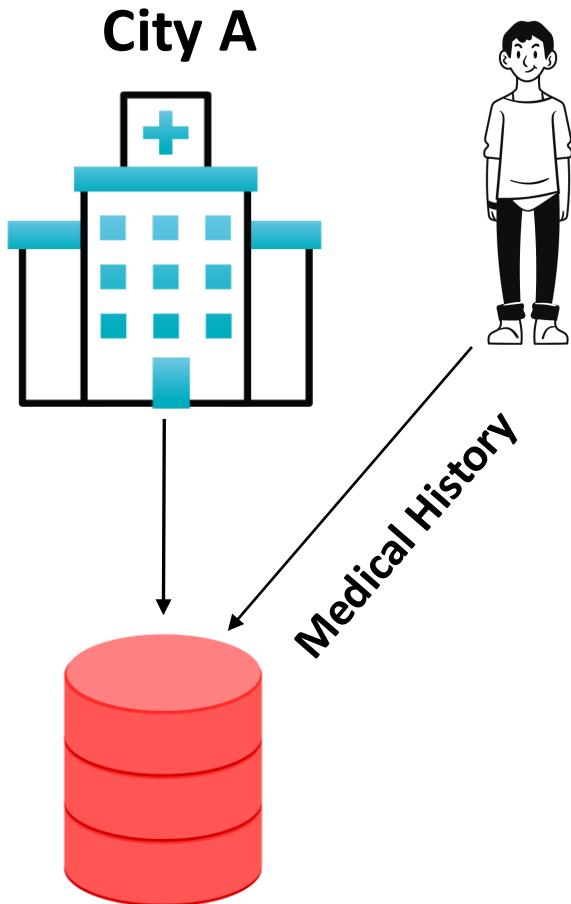


Note-Assuming optimum temperature < 30 degree Celsius.

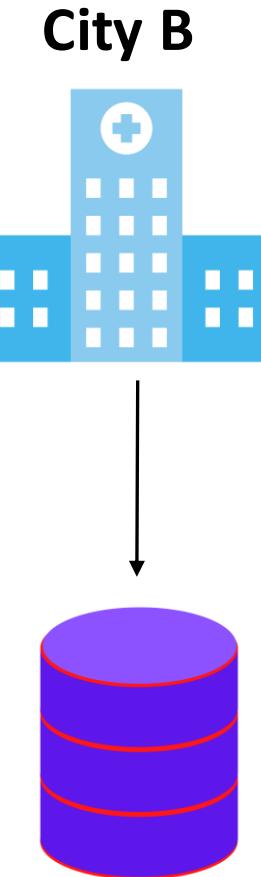
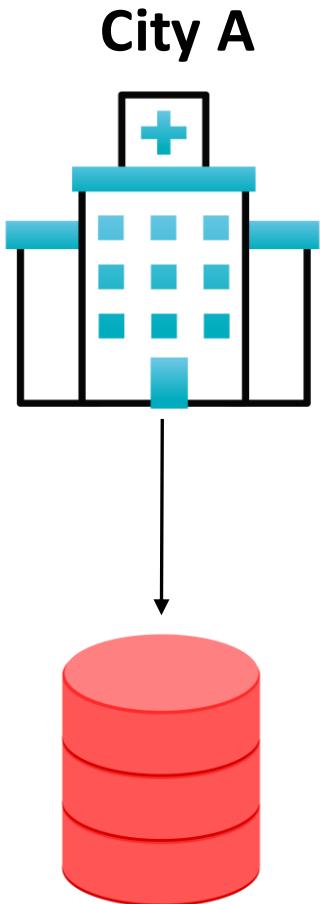
International Wire Transfer



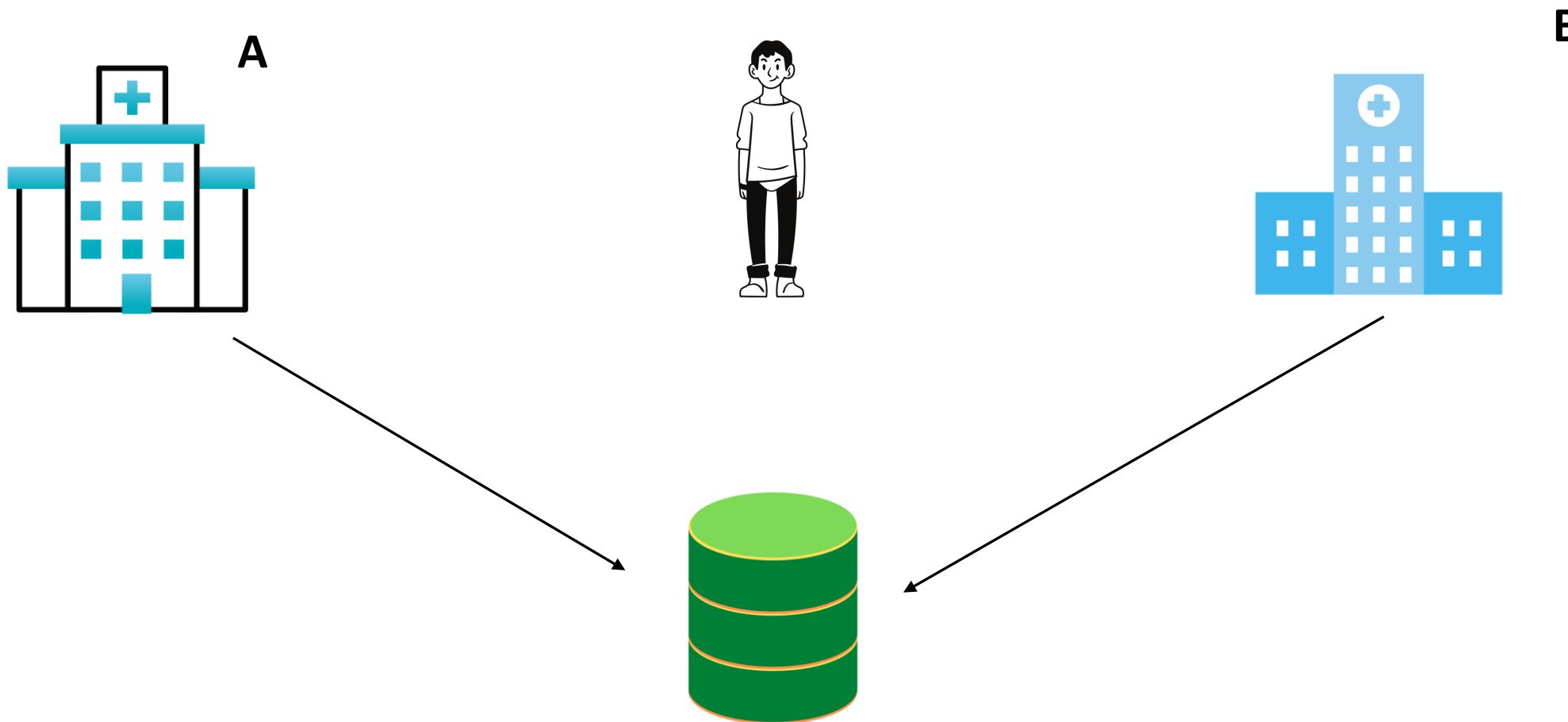
Healthcare System



Healthcare System

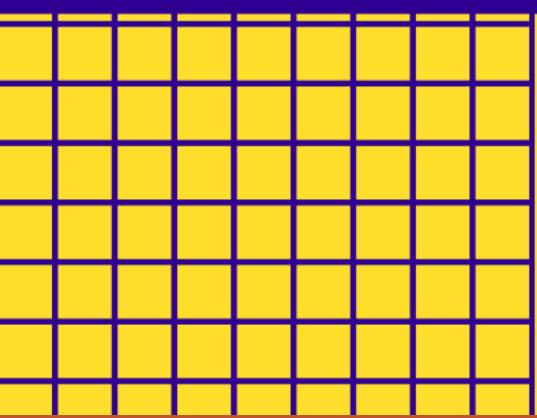
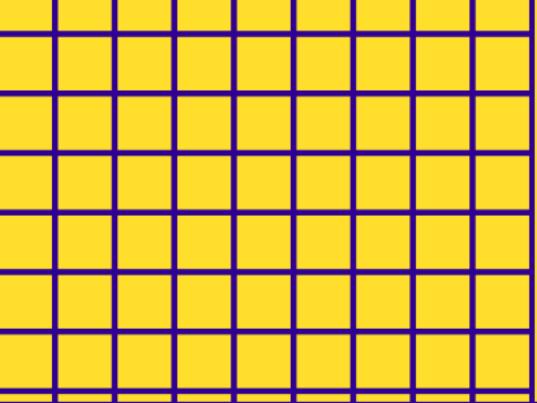


Healthcare System



Homework Time





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

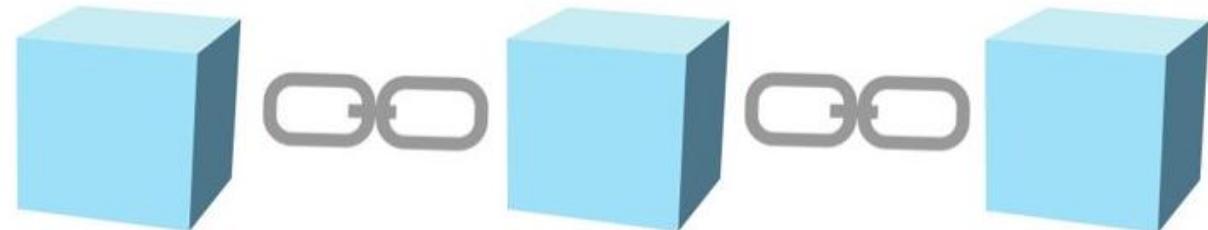
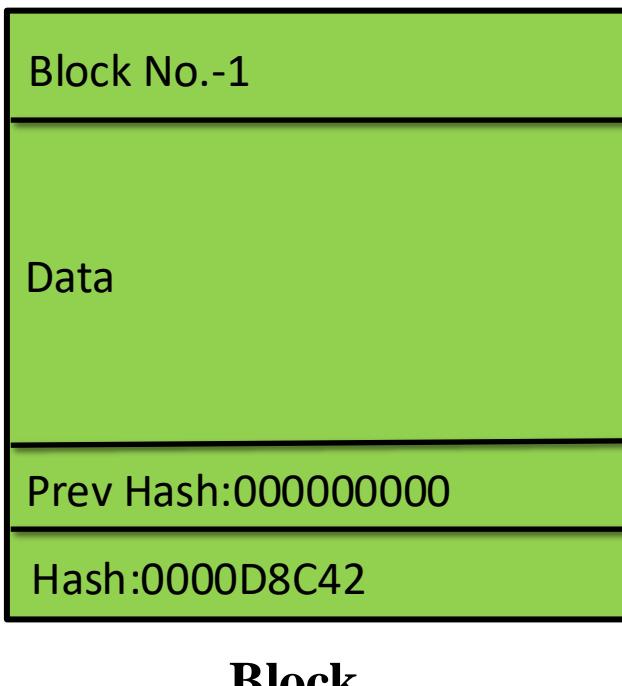
Hashing Algorithm



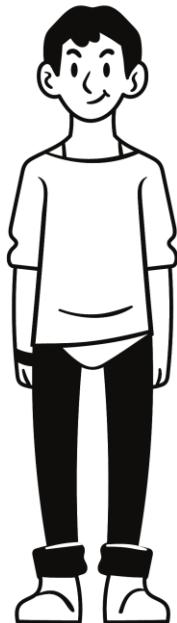
Hashing Algorithm

Hashing Algorithm

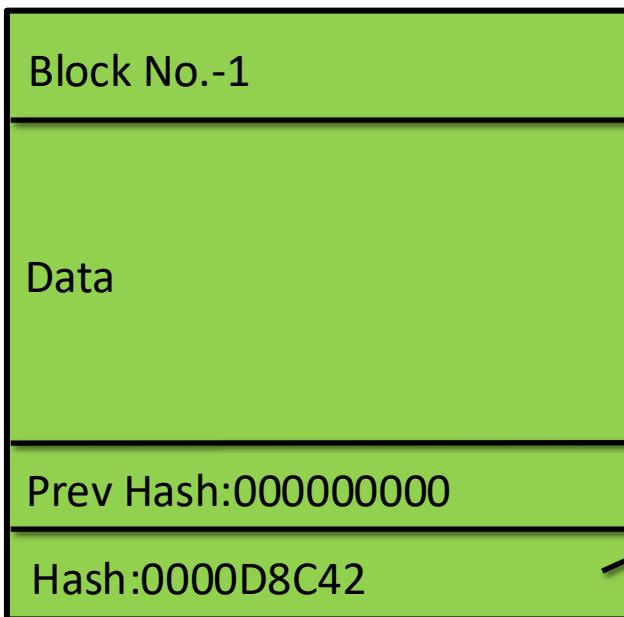
Hashing Algorithm



Hashing Algorithm



Hashing Algorithm

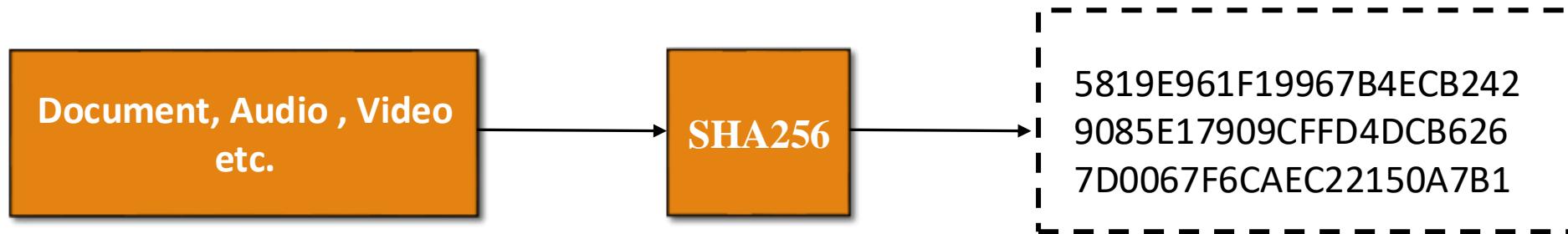


Block



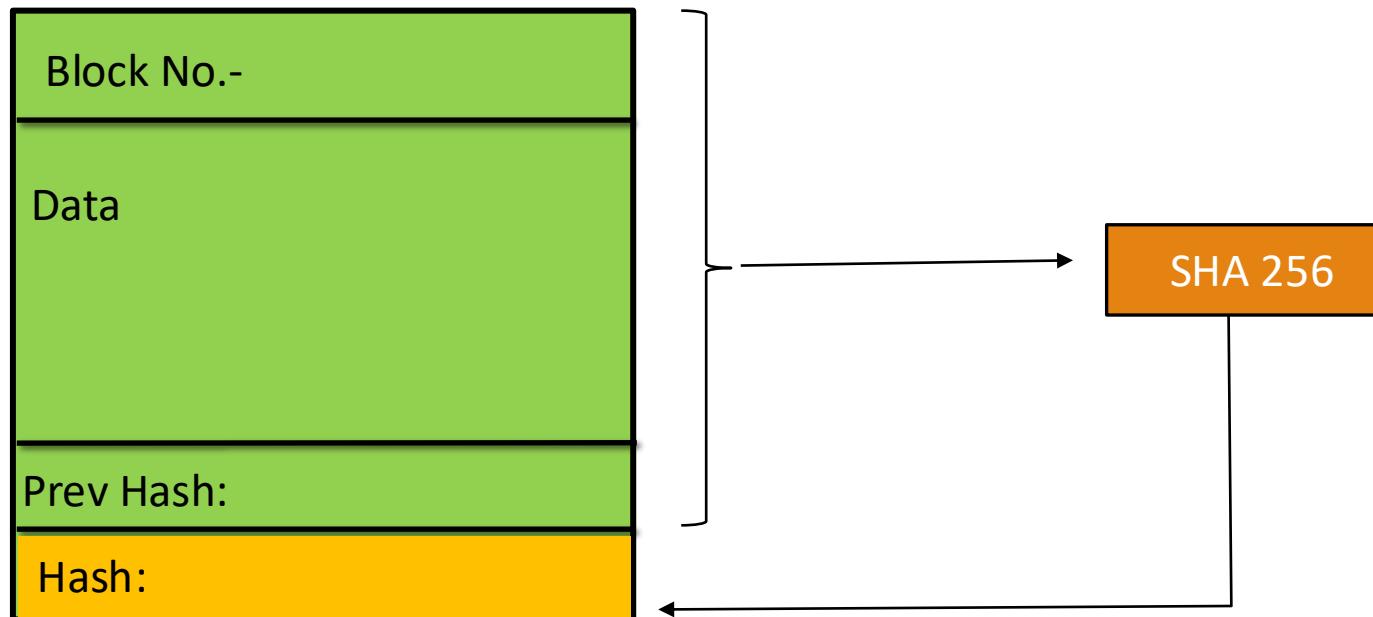
Fingerprint

Hashing Algorithm

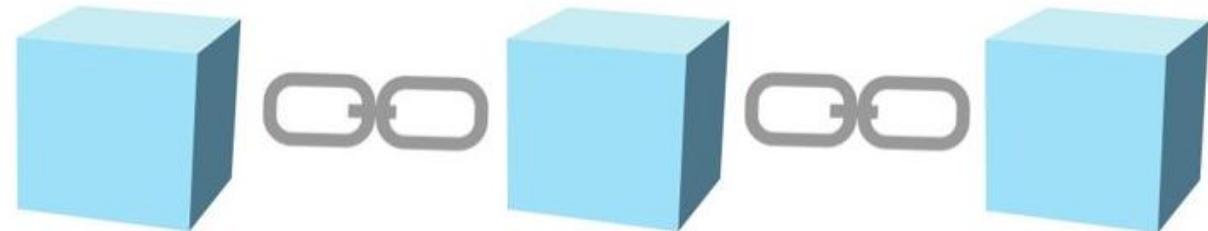
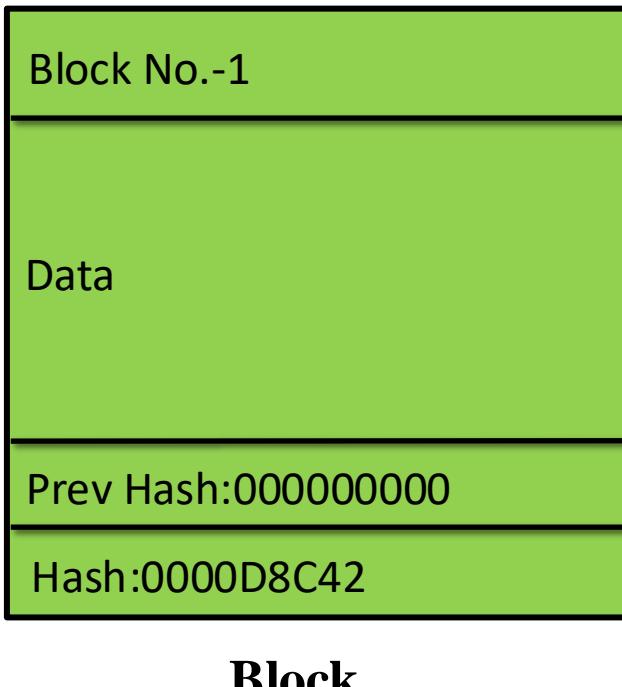


This has **64 hexadecimal characters**.
Each character is of **4 bits**.
So in total it has $64 * 4$ bits i.e. **256 bits**.

Hashing Algorithm



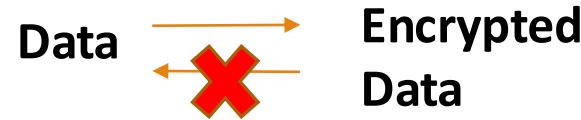
Hashing Algorithm



Hashing Algorithm

The five requirements of Hash Algorithm-

One Way



Withstand Collisions

Deterministic

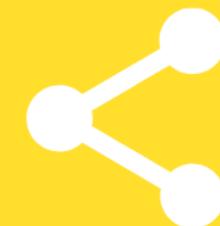


Avalanche Effect

Fast Computation

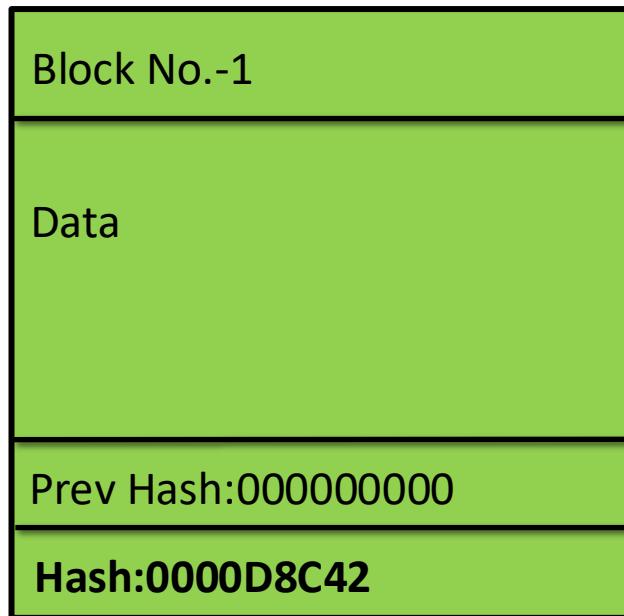
**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

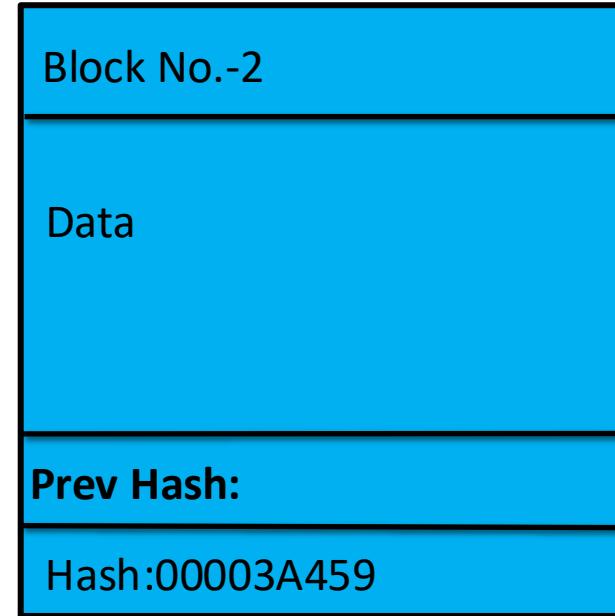
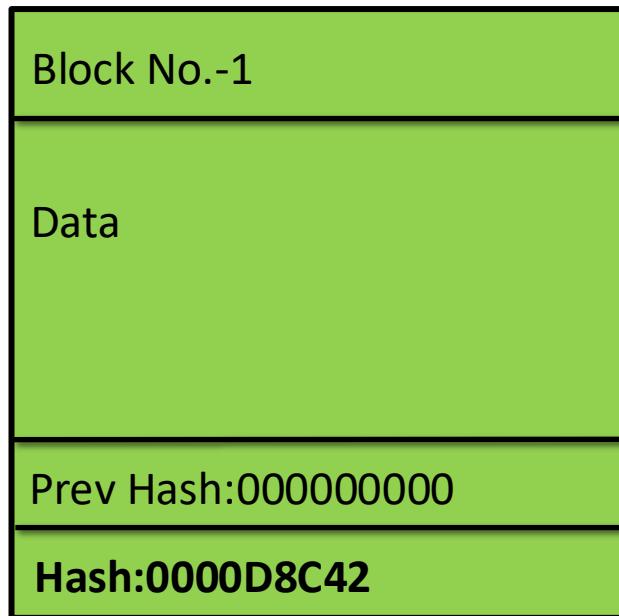


Blockchain Formation

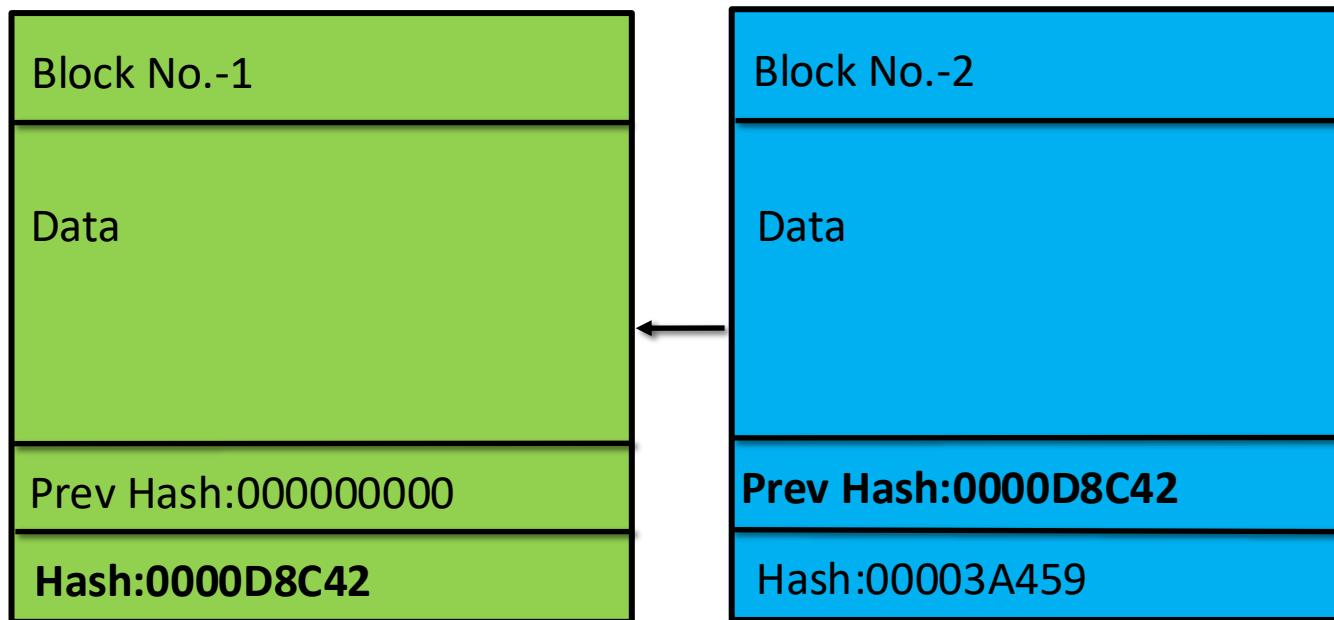
Hashing Algorithm



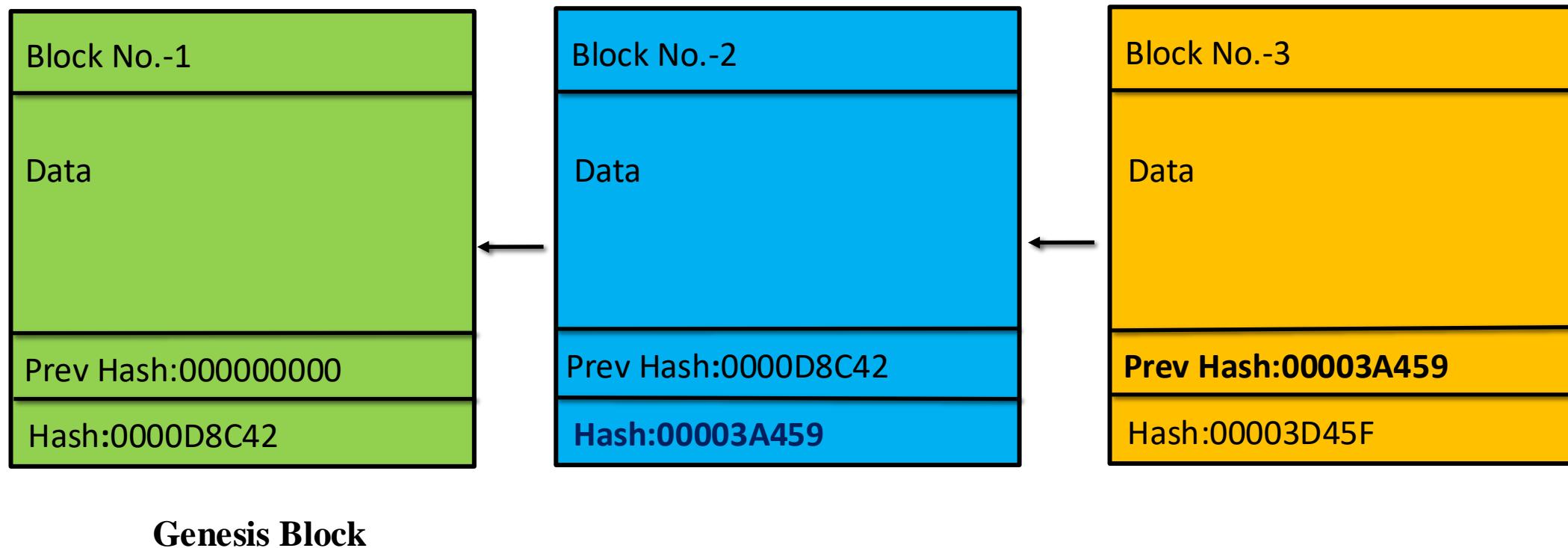
Hashing Algorithm



Hashing Algorithm

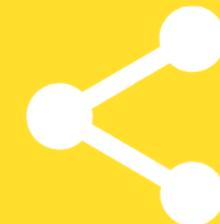


Hashing Algorithm



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Immutable Ledger

Immutable Ledger



You



Money



Sales Deed

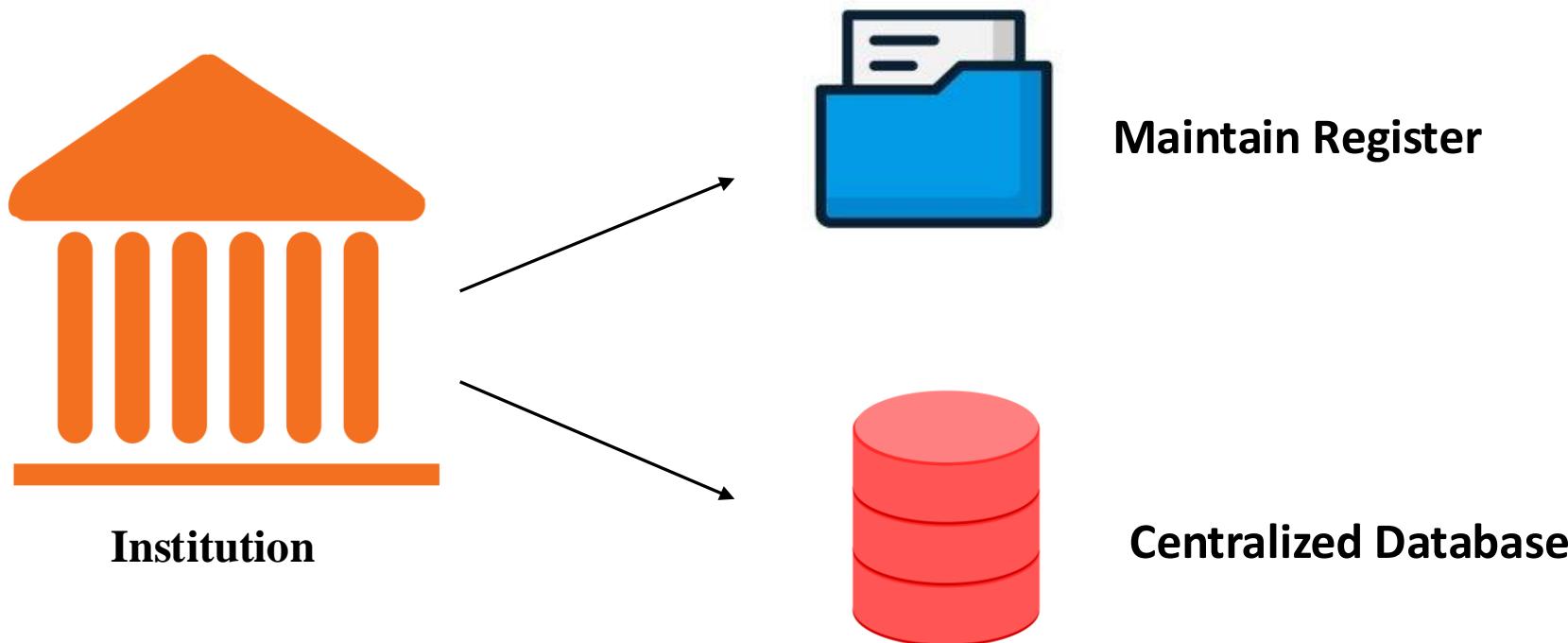


Institution

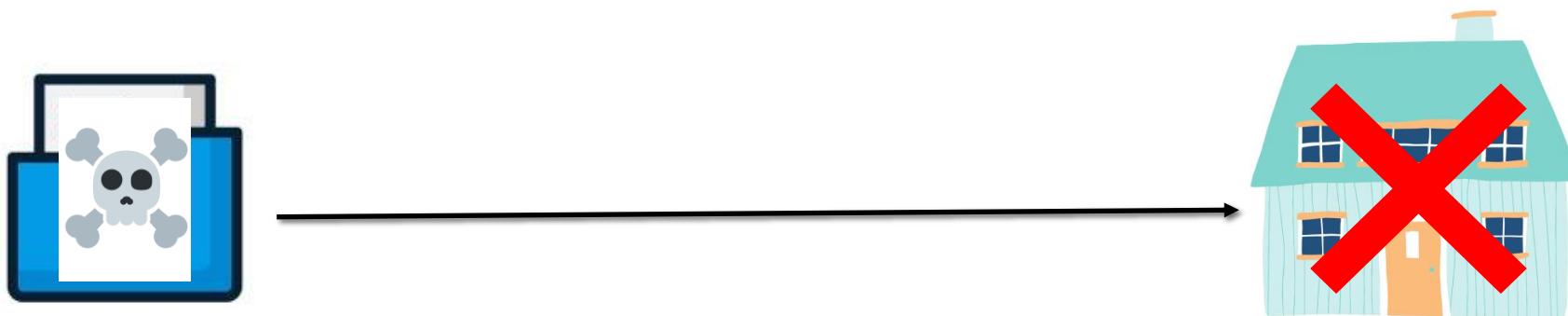


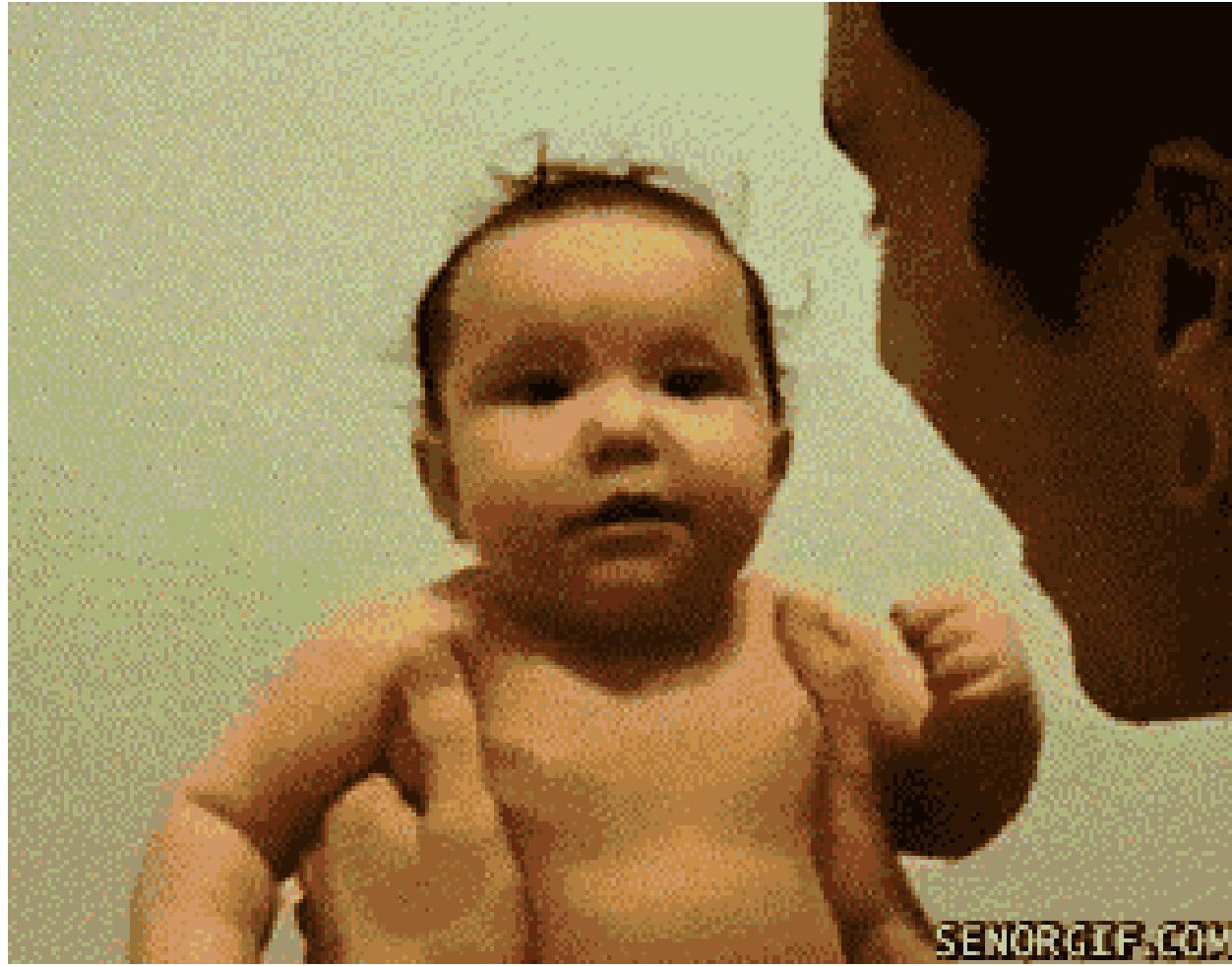
House

Immutable Ledger



Immutable Ledger



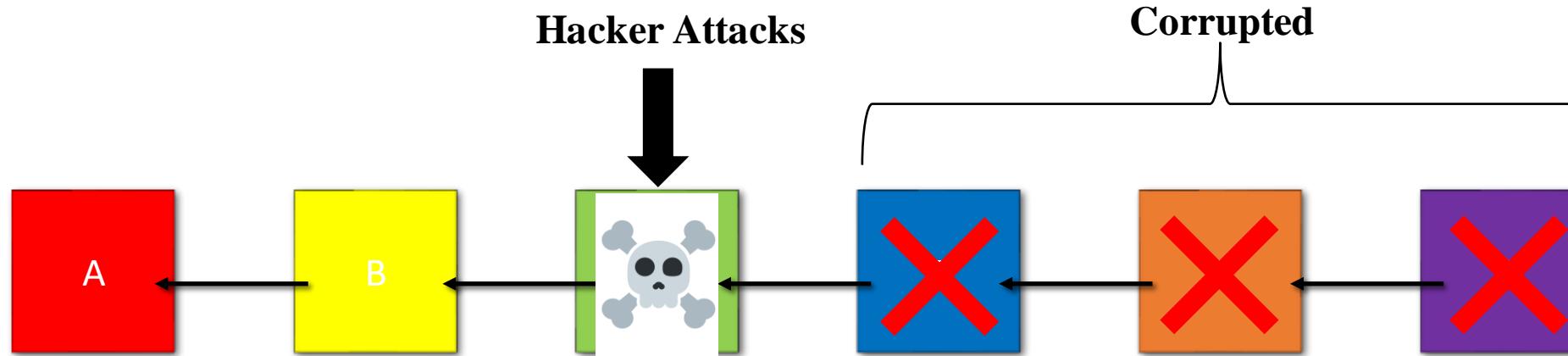


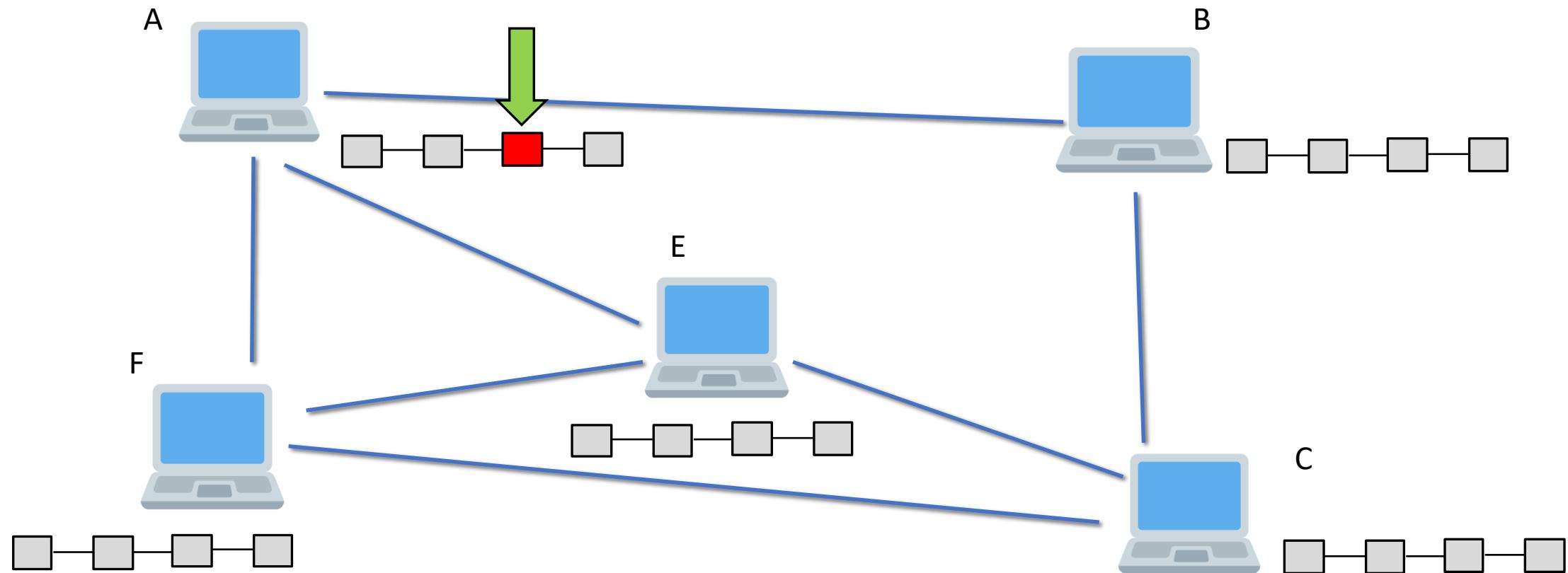
SENRGIF.COM

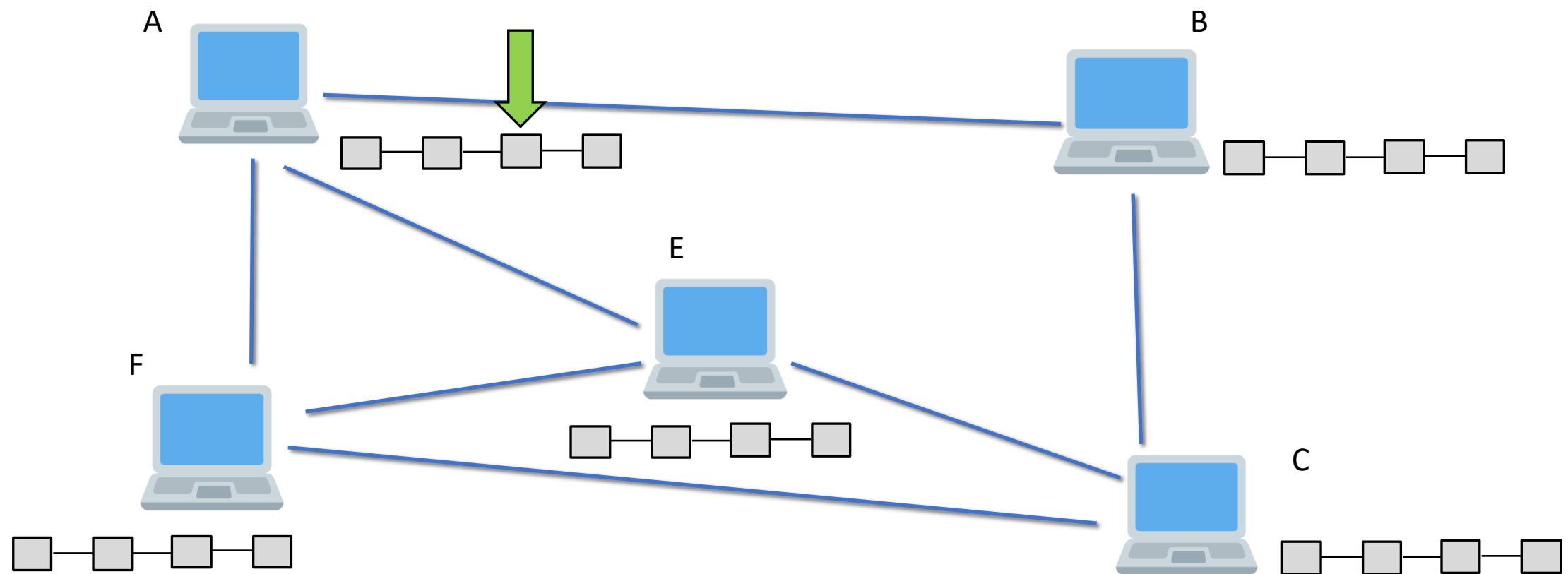
Immutable Ledger

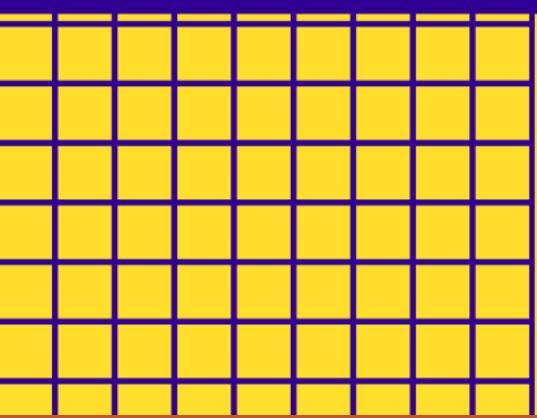
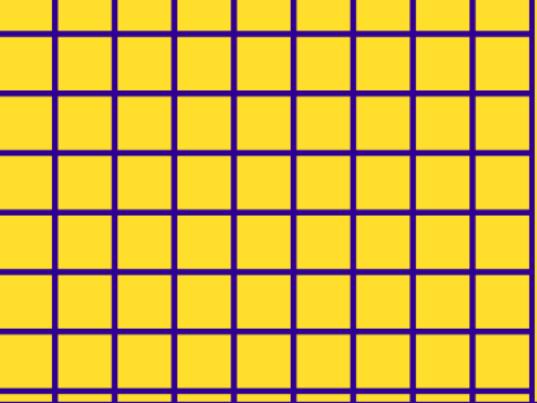


From previous lecture..









Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



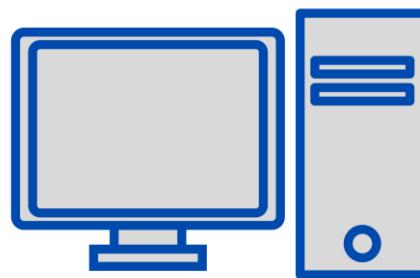
Discord – Link in description



What is a P2P network?

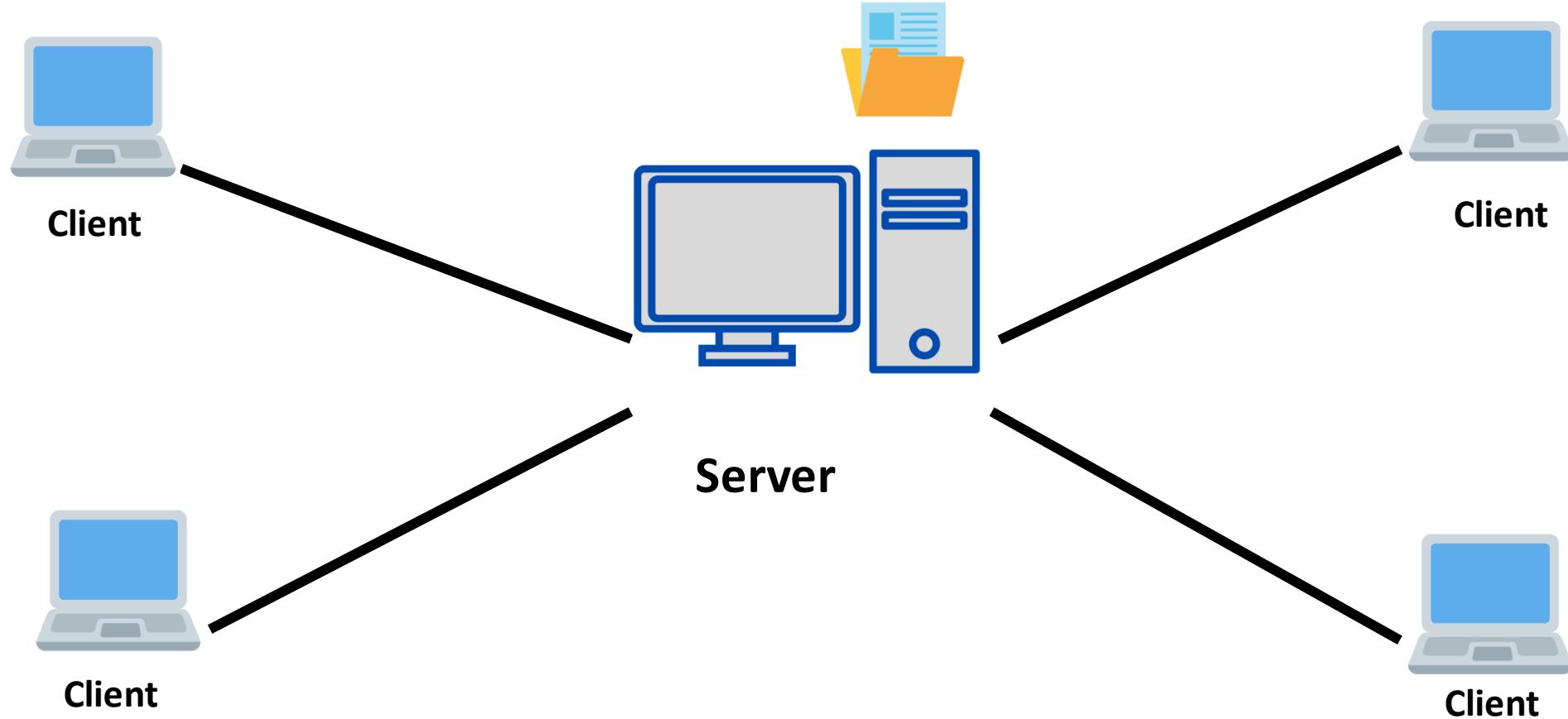
What is a centralized network?

What is a centralized network?

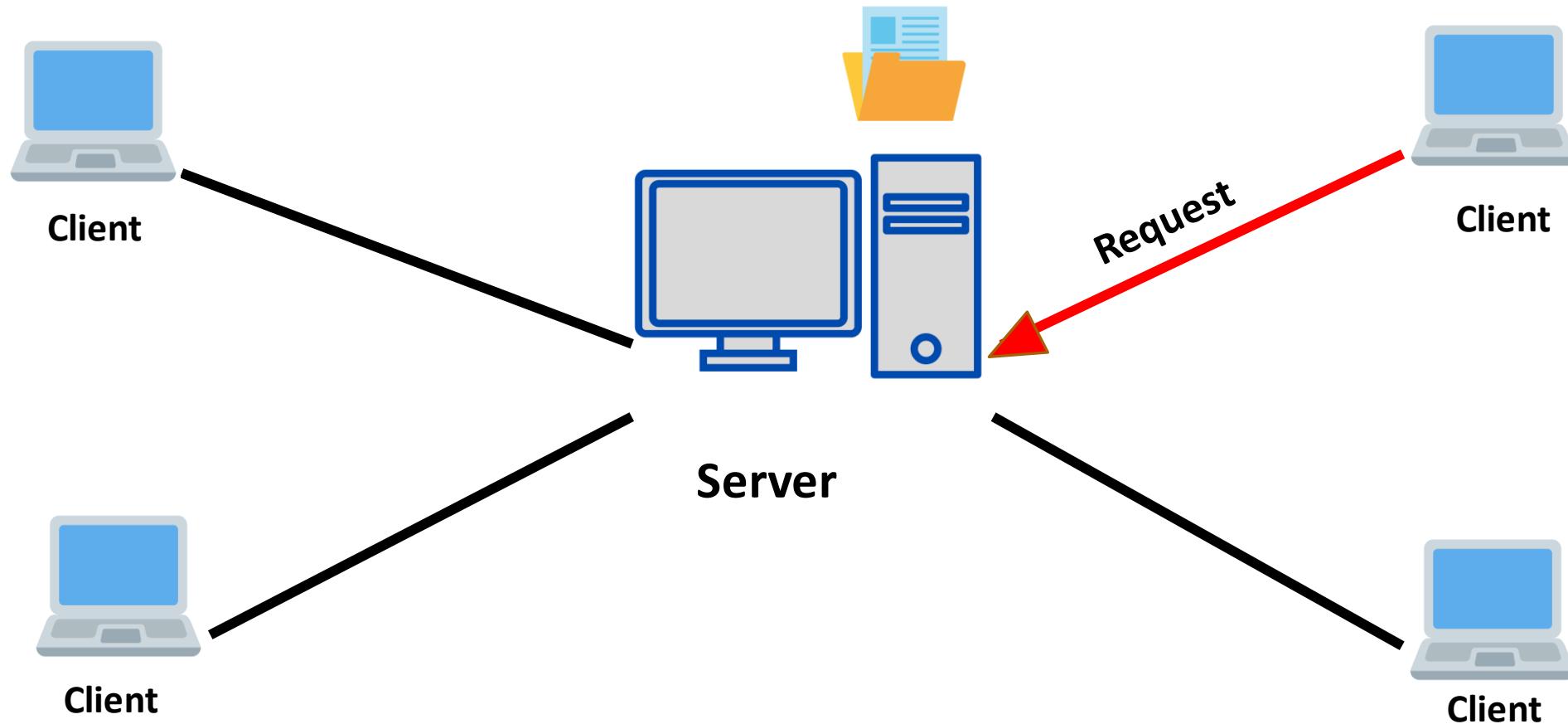


Server

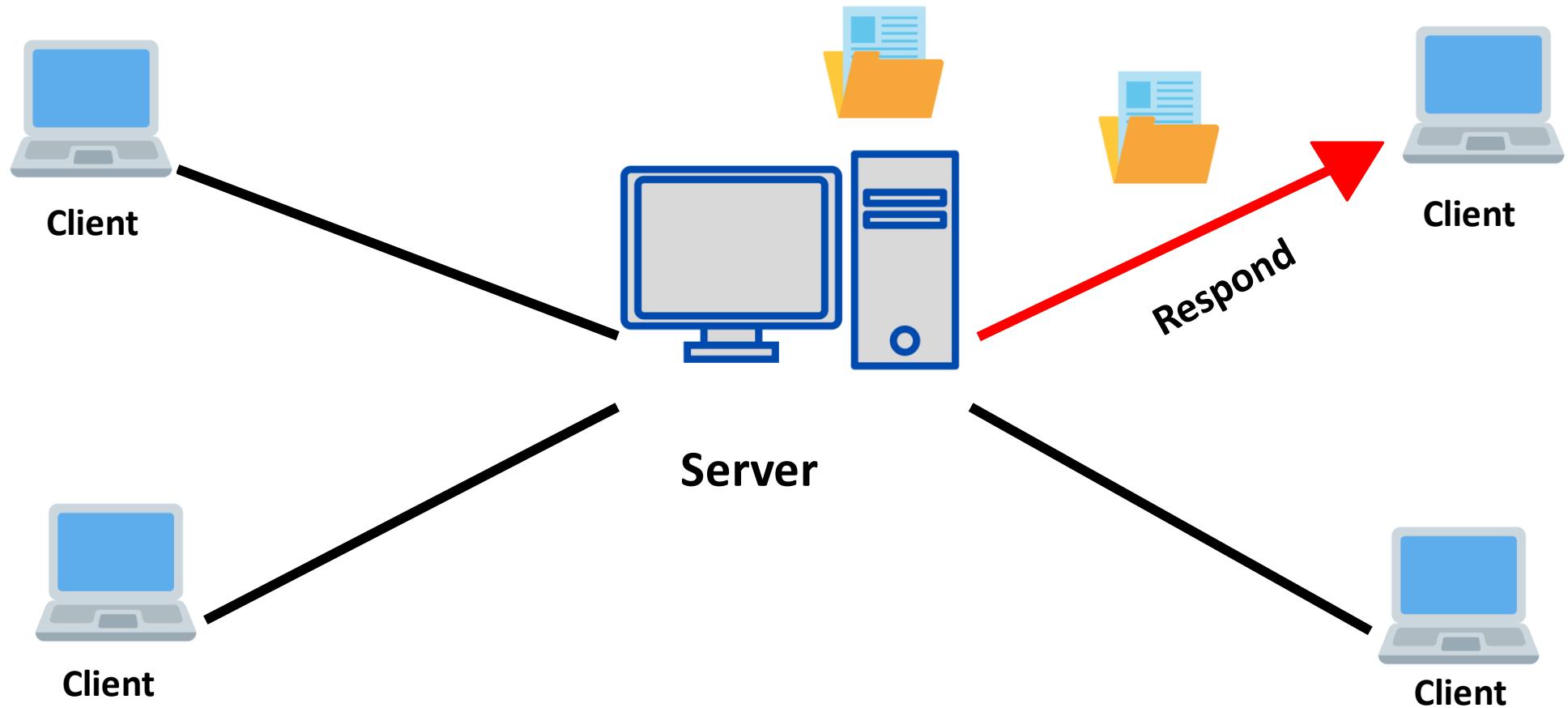
What is a centralized network?



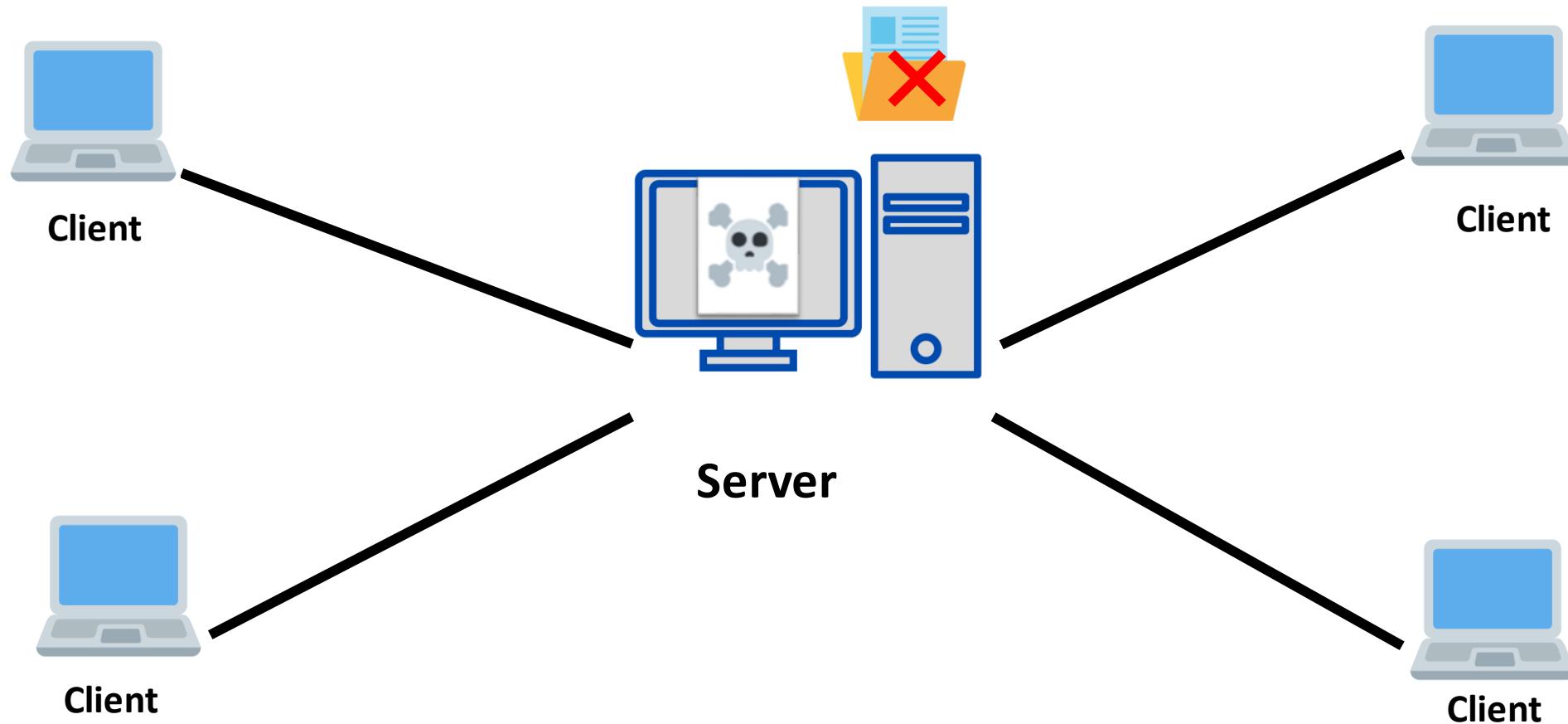
What is a centralized network?



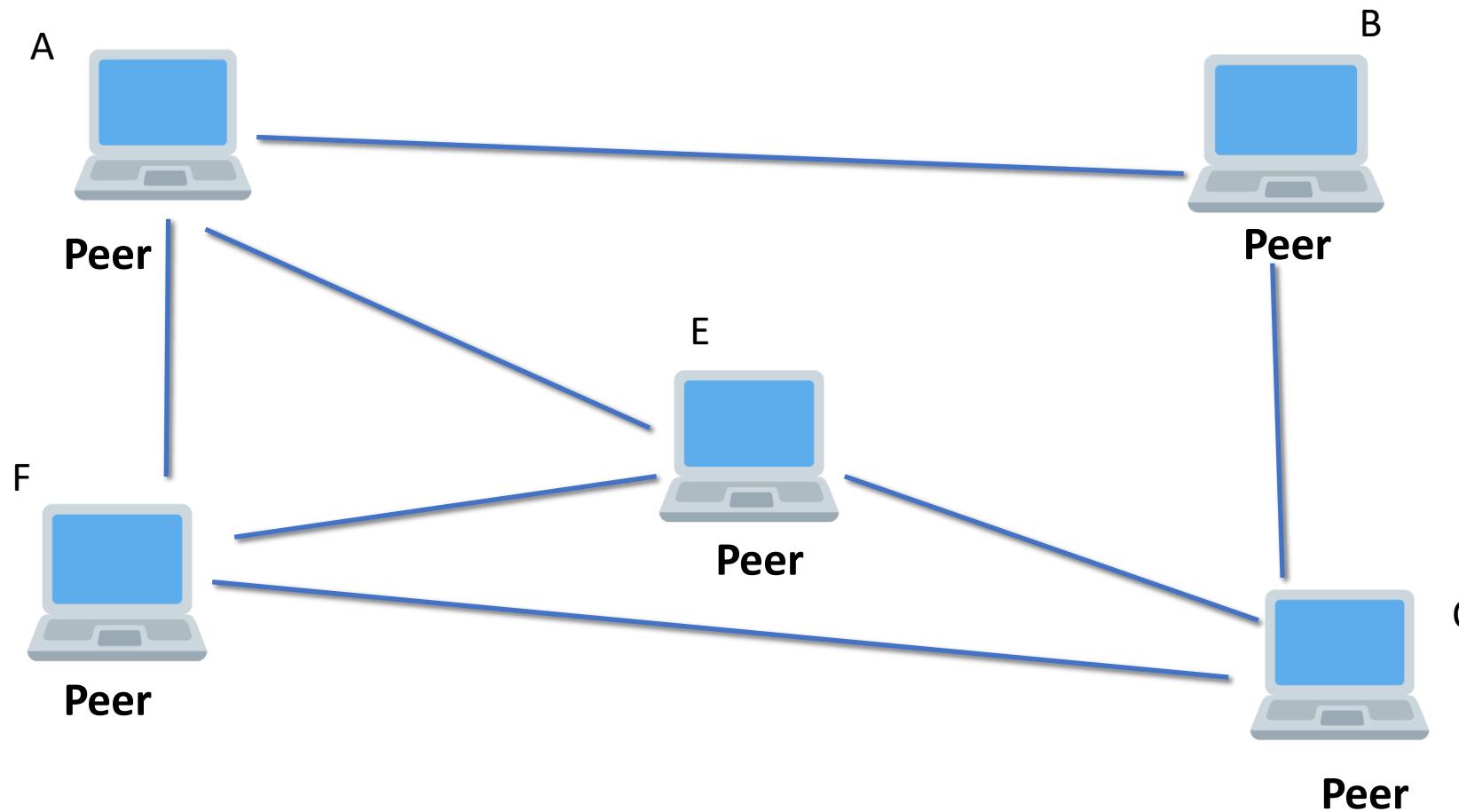
What is a centralized network?



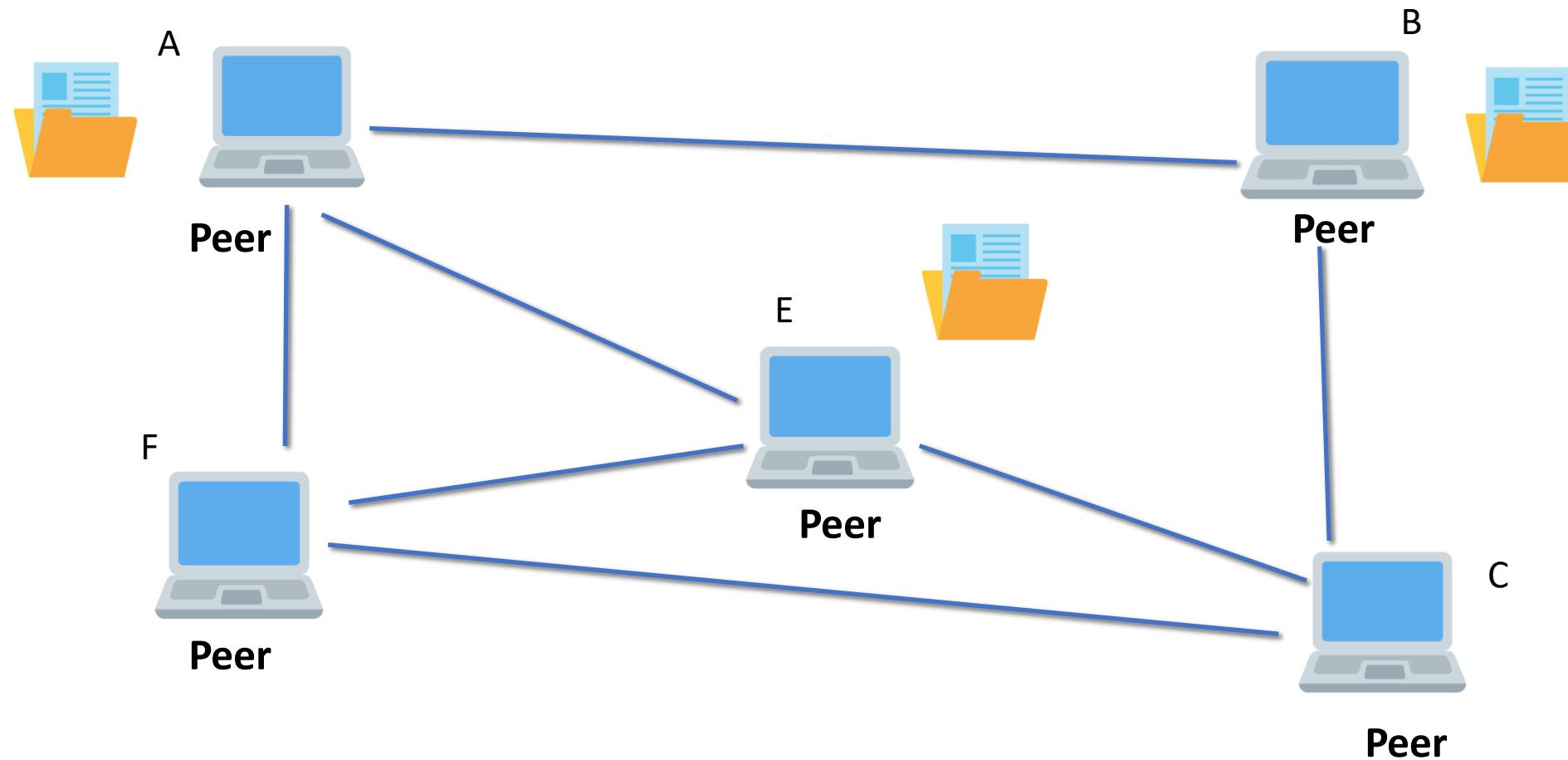
What is a centralized network?

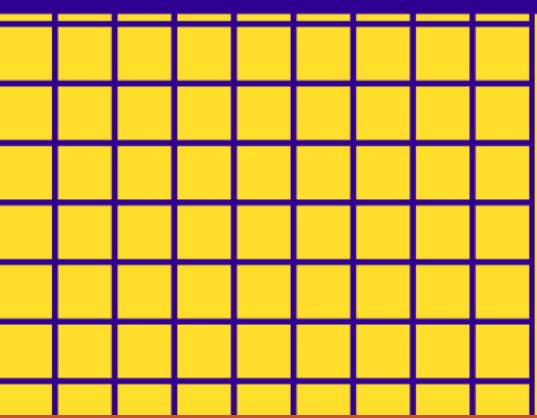
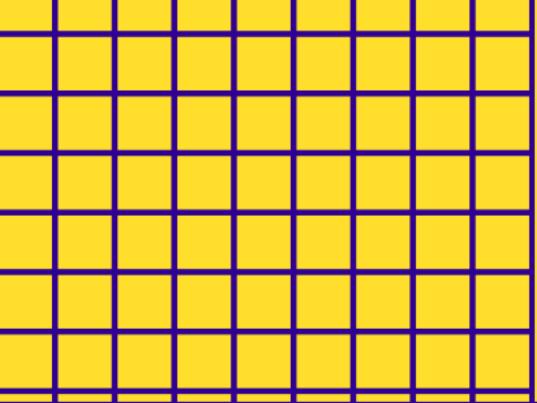


Distributed P2P network



Distributed P2P network





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

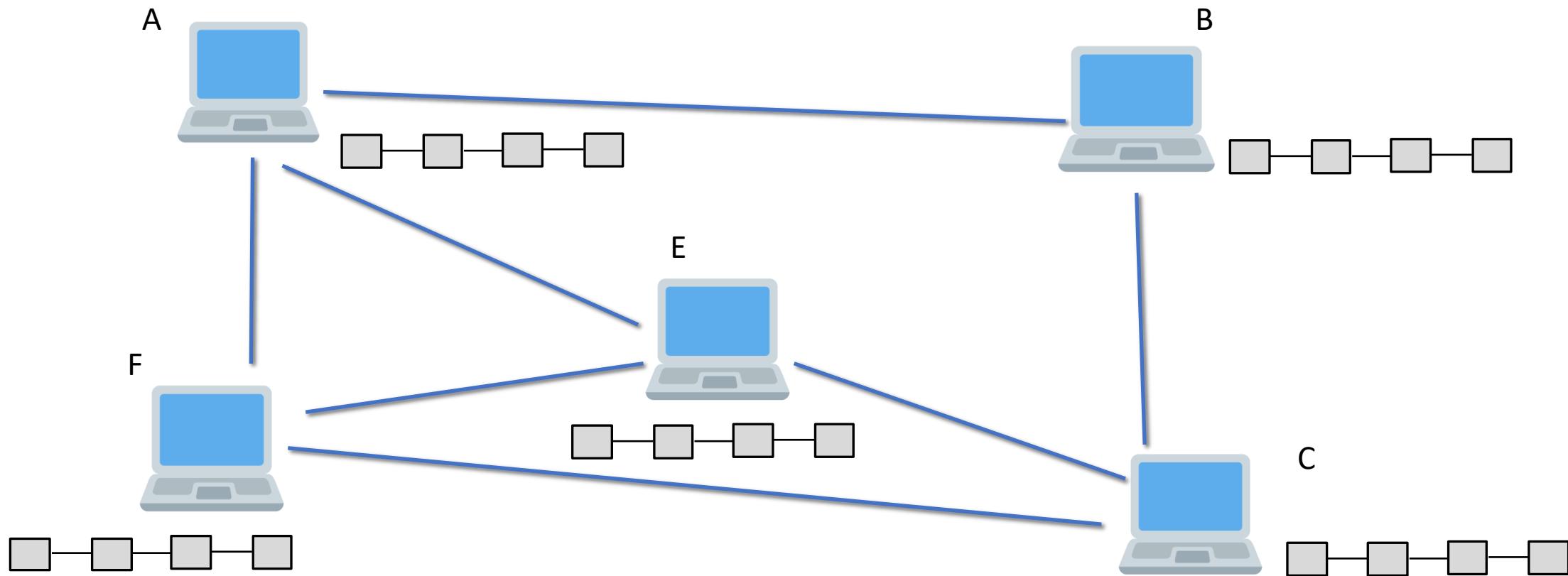


Discord – Link in description

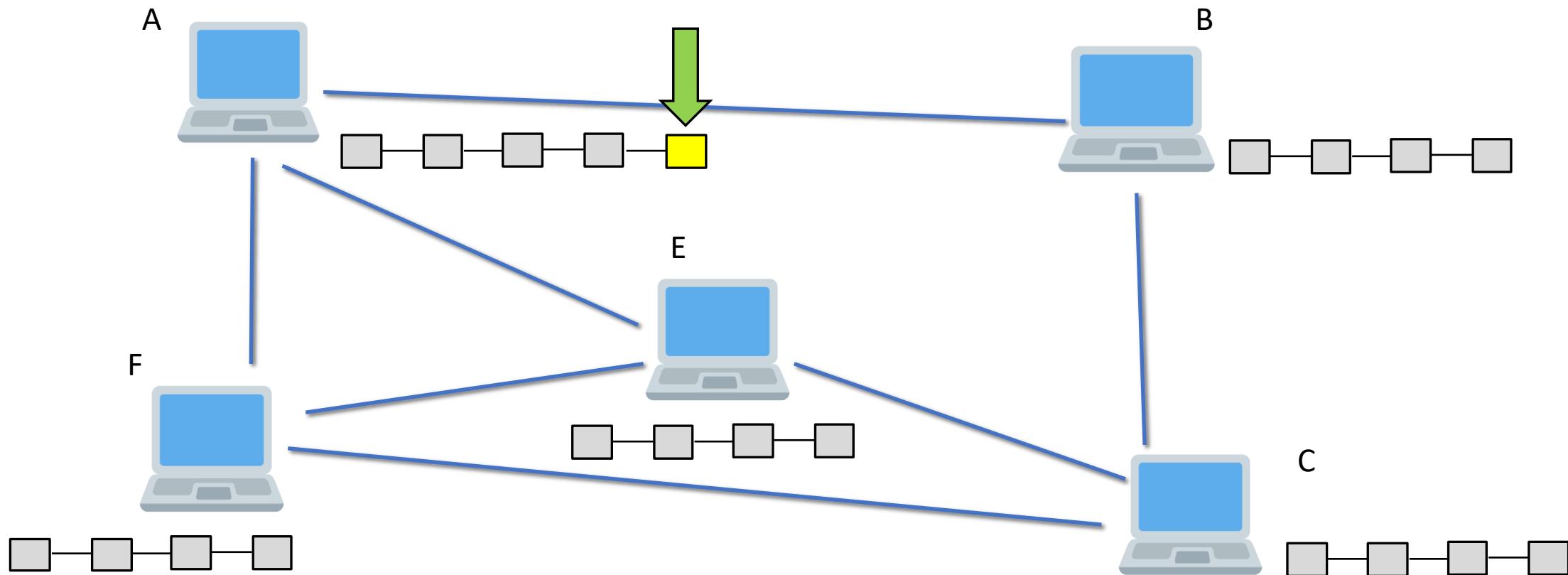
A complex, abstract digital background composed of a grid of blue and white squares. Overlaid on this grid are several concentric, semi-transparent circles in shades of blue and cyan. The circles appear to be rotating or pulsating. Interspersed throughout the grid are numerous binary digits (0s and 1s) in a light blue color, some of which are contained within small, dashed rectangular boxes. The overall effect is one of a high-tech, digital environment.

Distributed P2P network in Blockchain

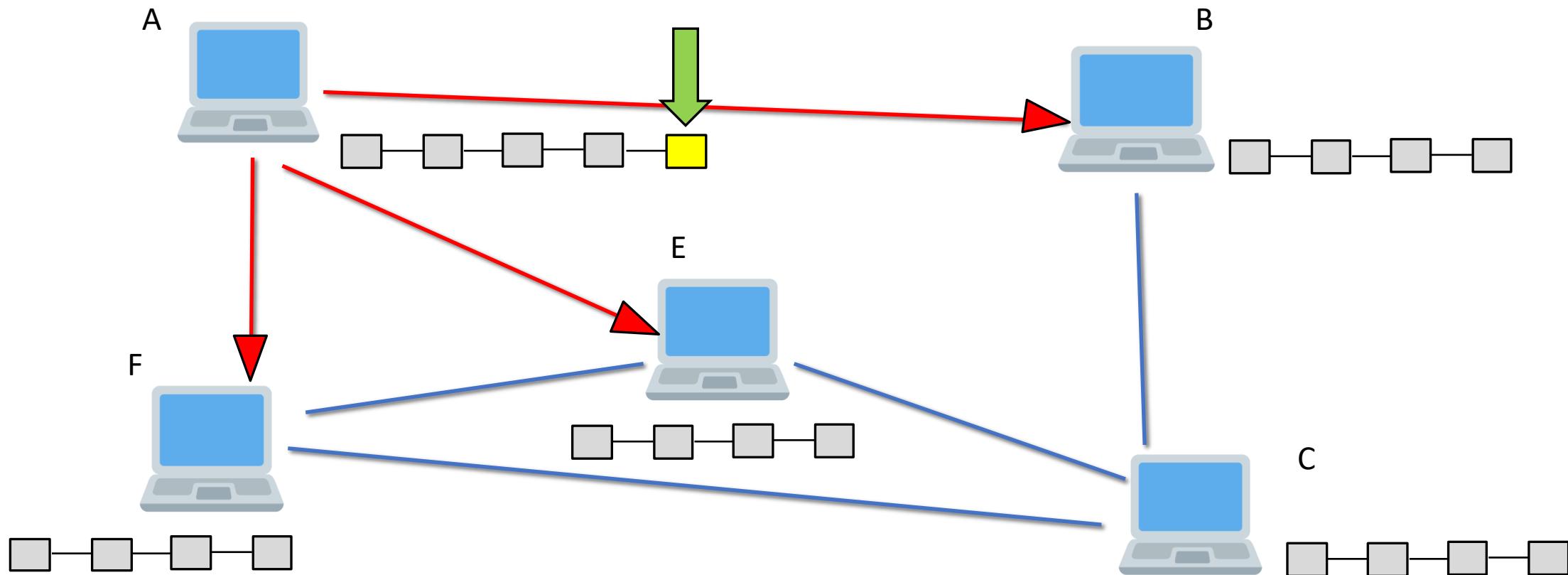
Distributed P2P network



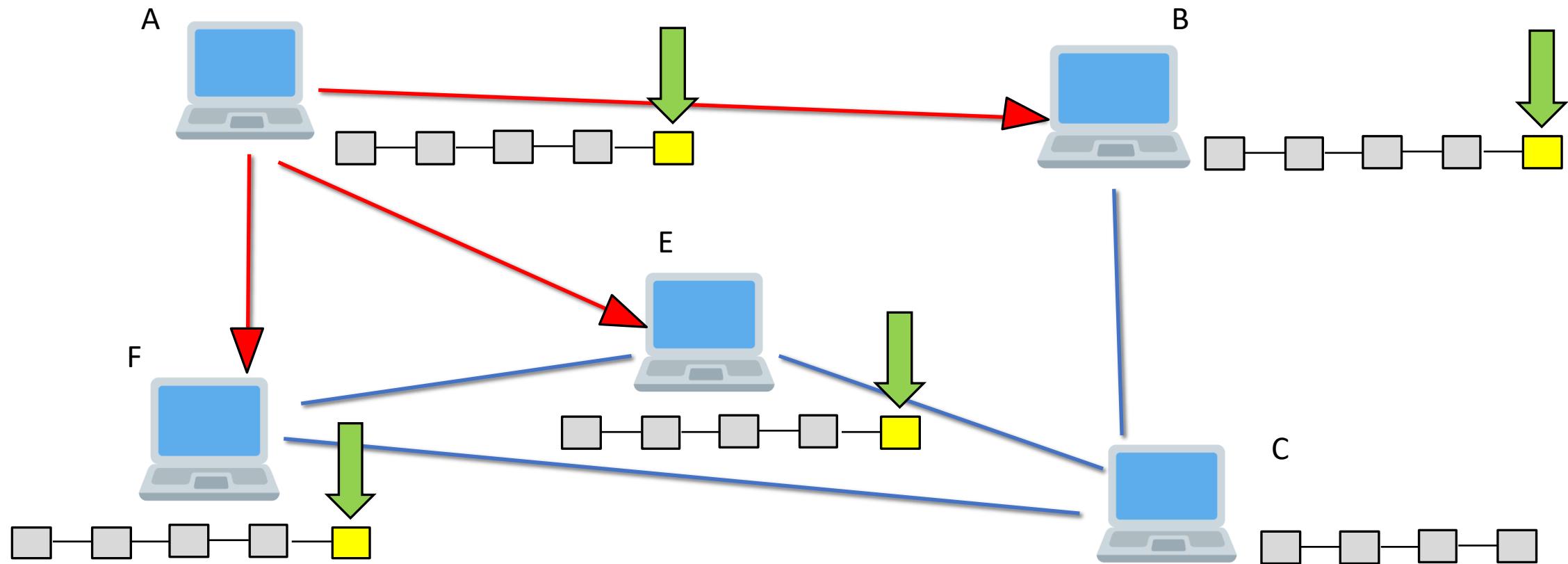
Distributed P2P network



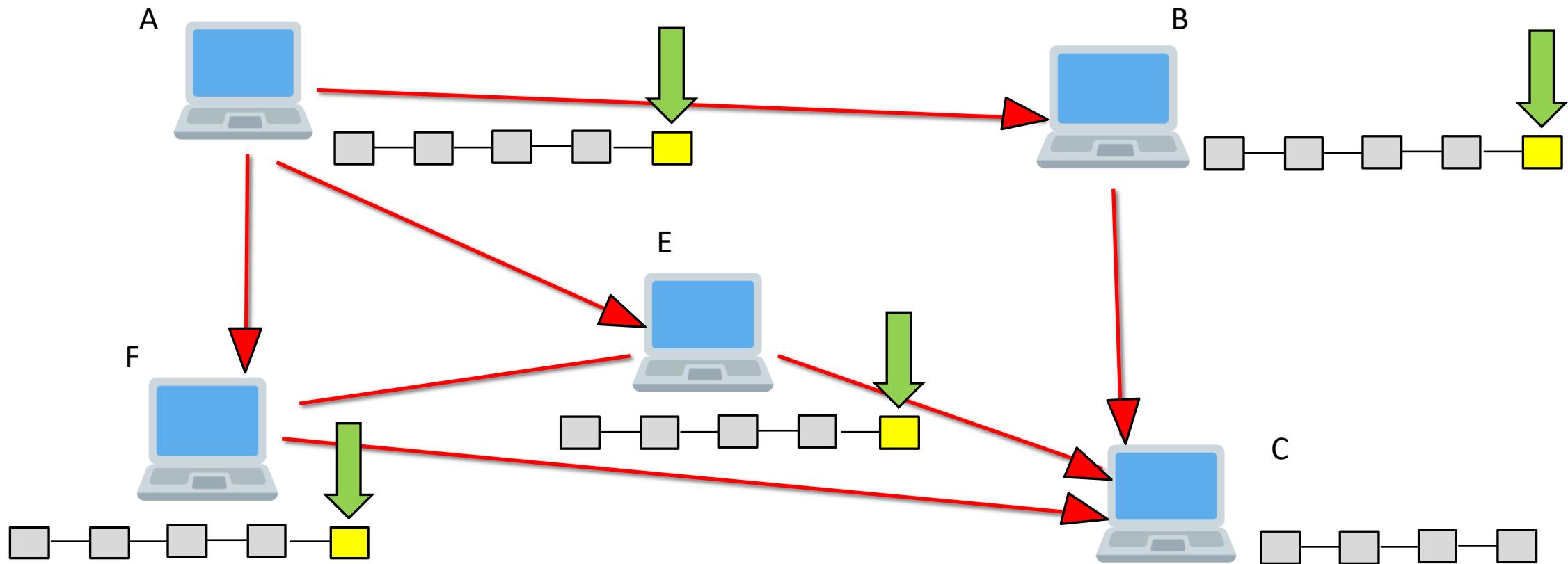
Distributed P2P network



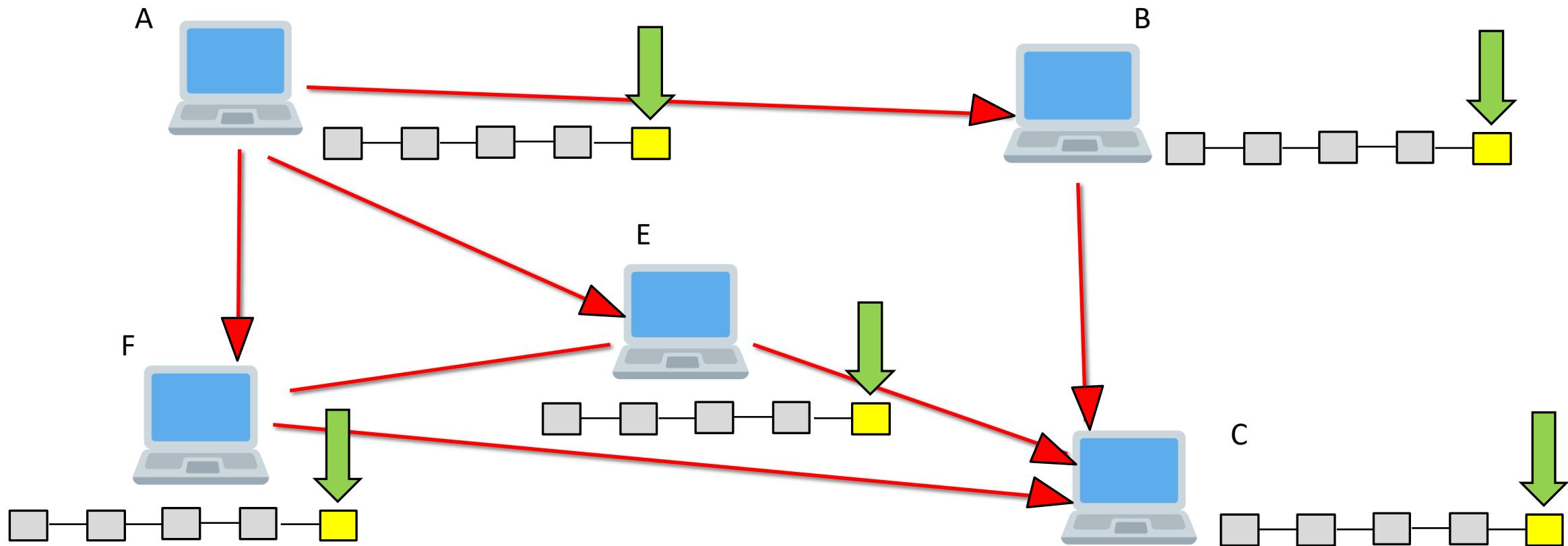
Distributed P2P network



Distributed P2P network



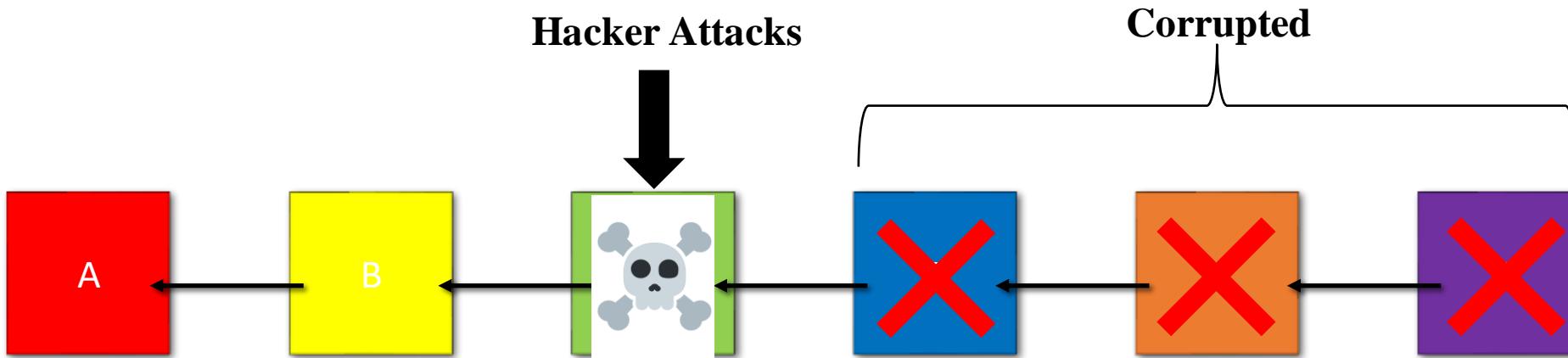
Distributed P2P network



Distributed P2P network

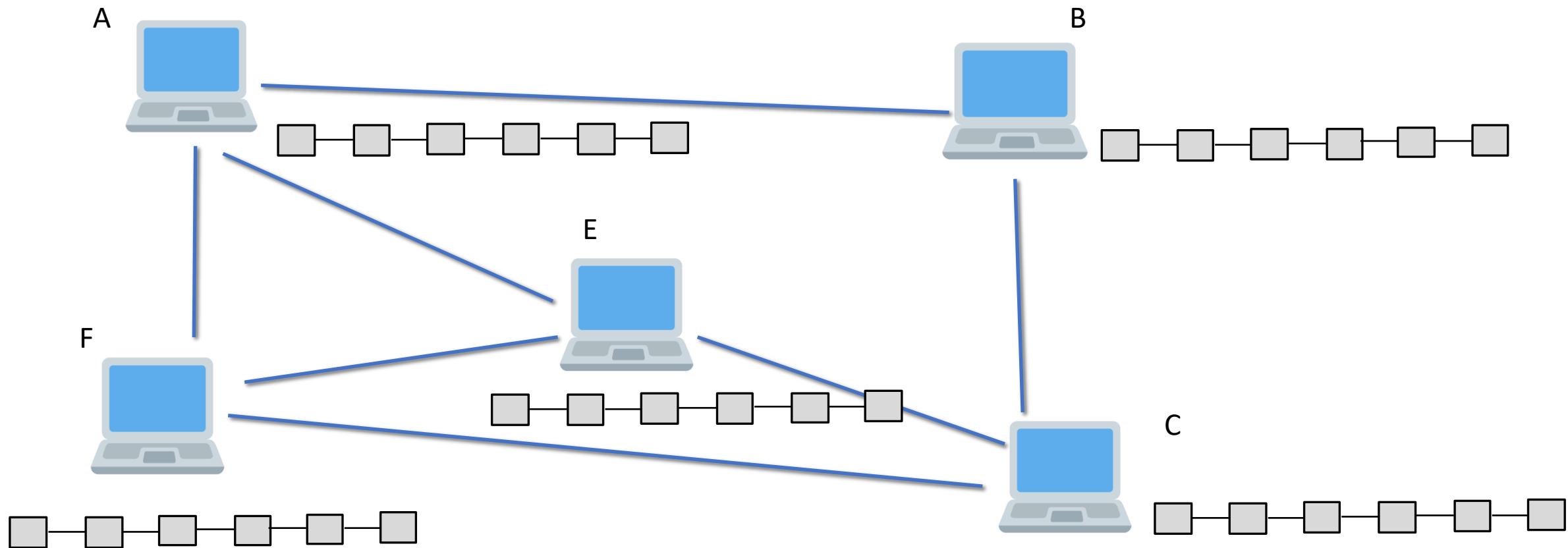
Q)Why we need Distributed P2P network in Blockchain?

Distributed P2P network

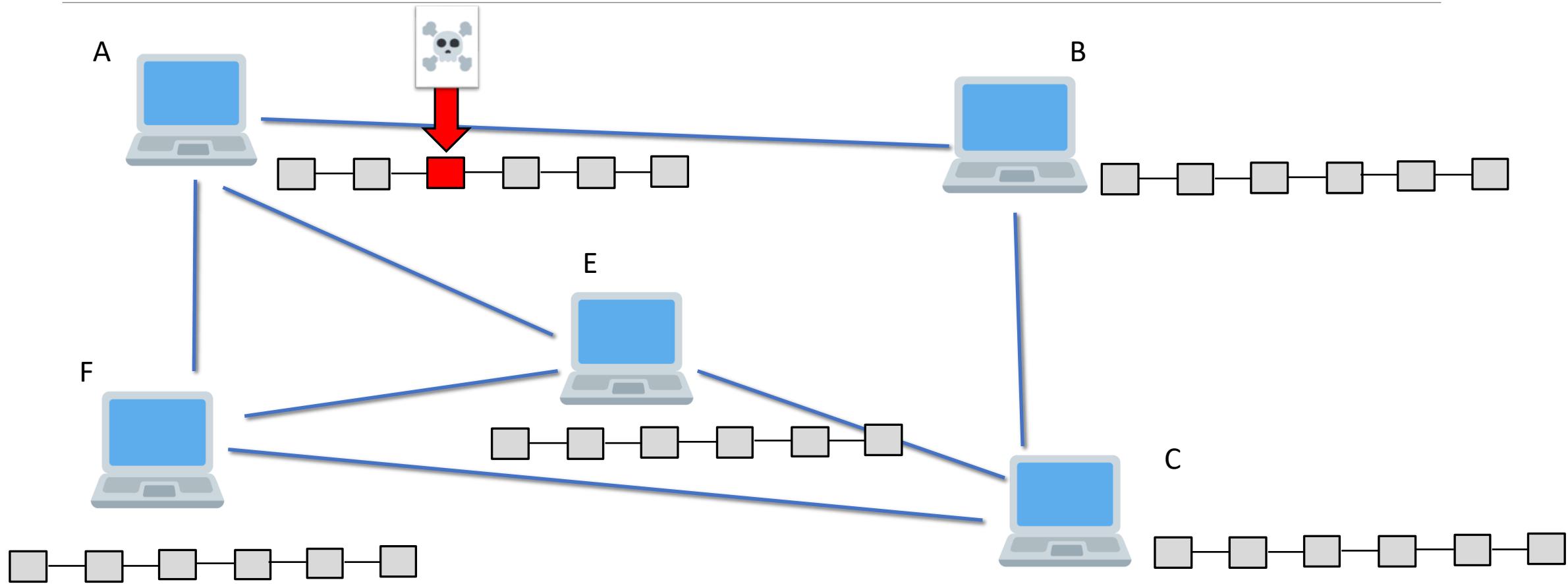


Concept of Immutability

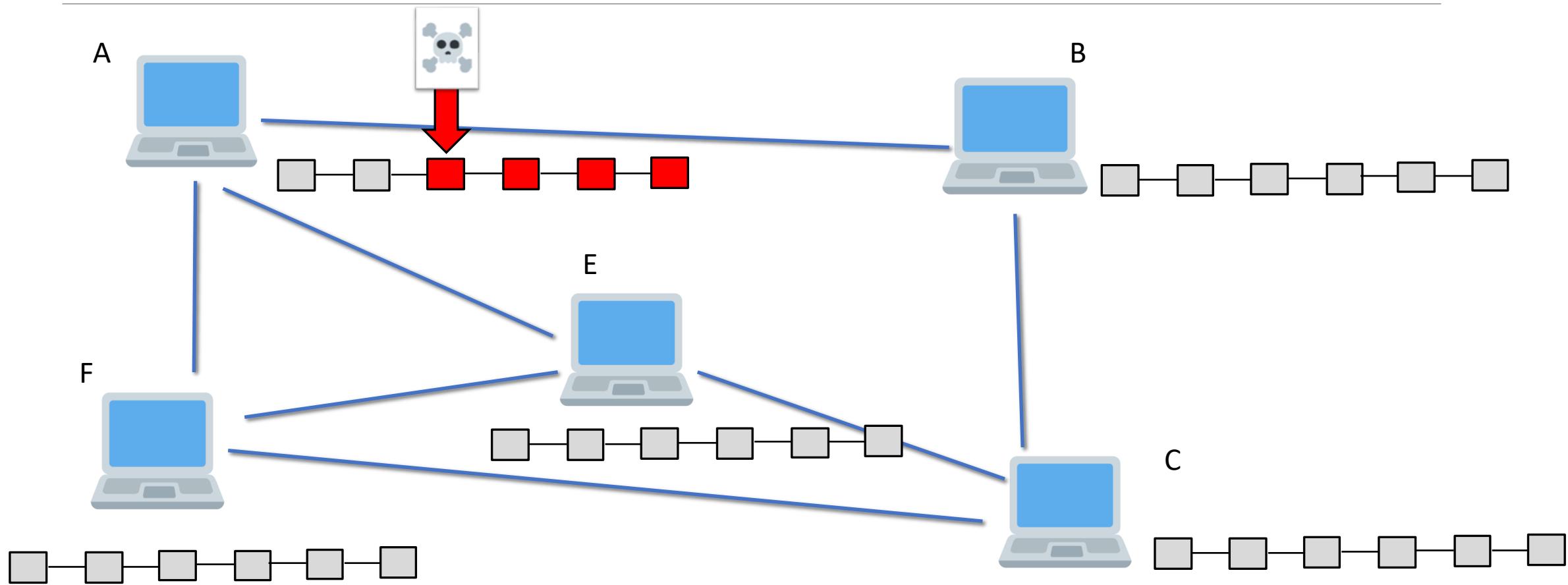
Distributed P2P network



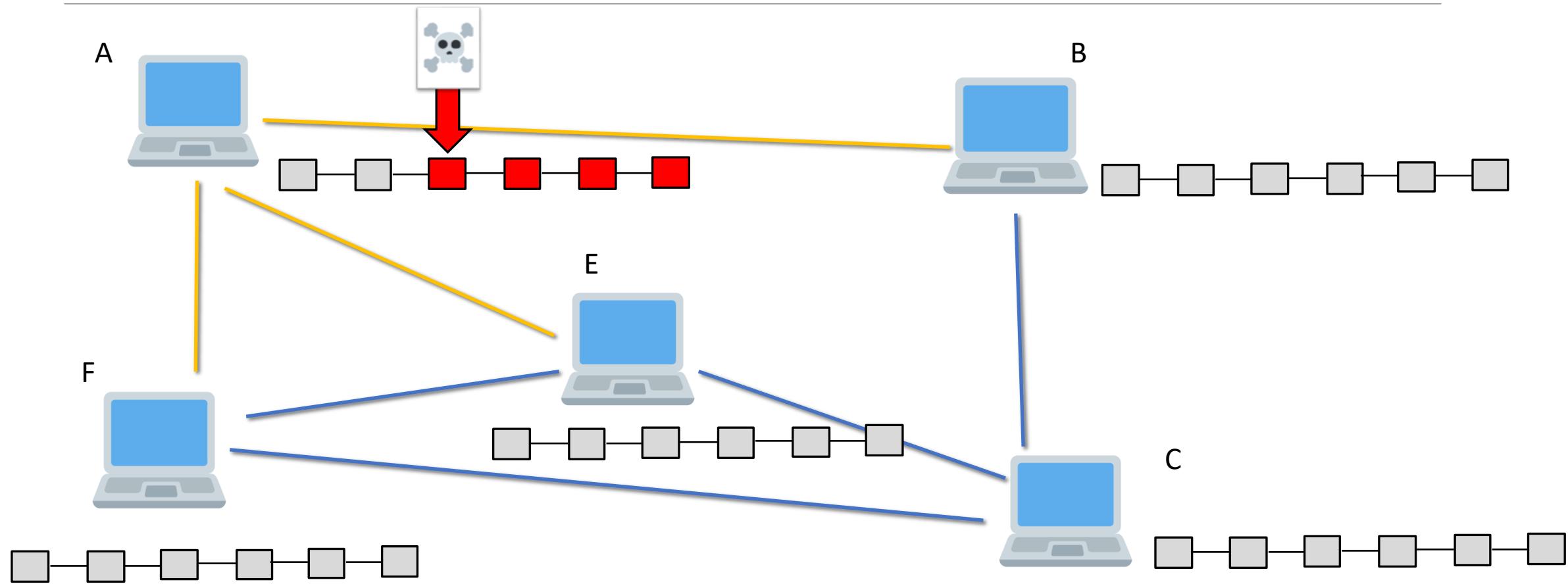
Distributed P2P network



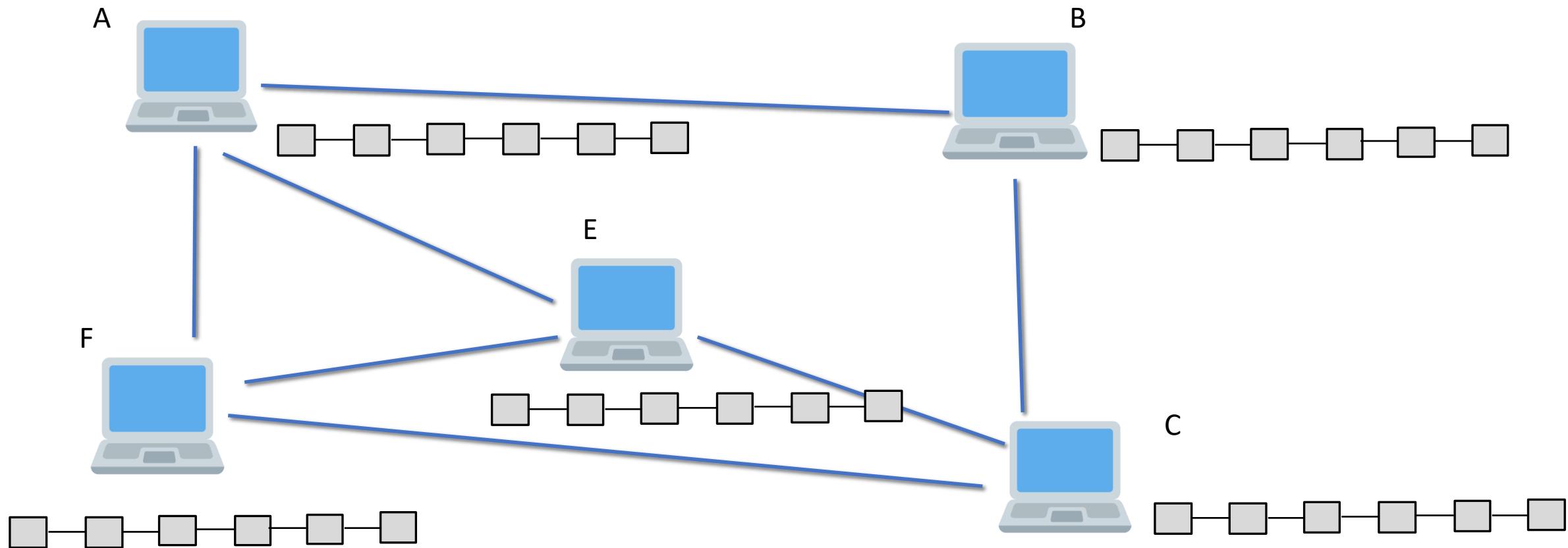
Distributed P2P network

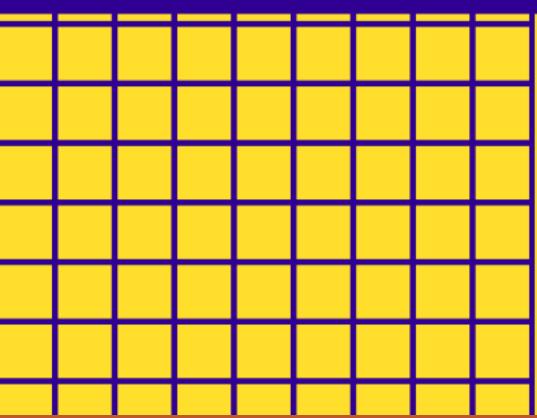
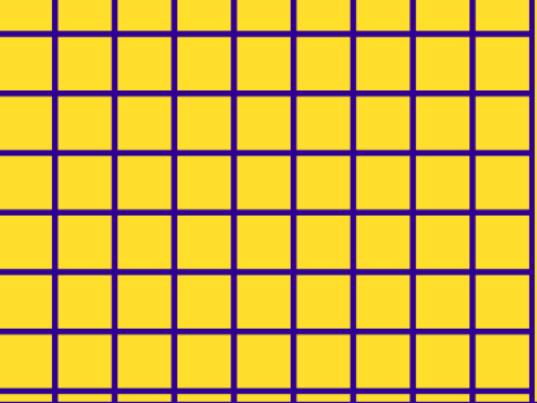


Distributed P2P network



Distributed P2P network





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

**GIVE THIS VIDEO
A THUMBS-UP !**

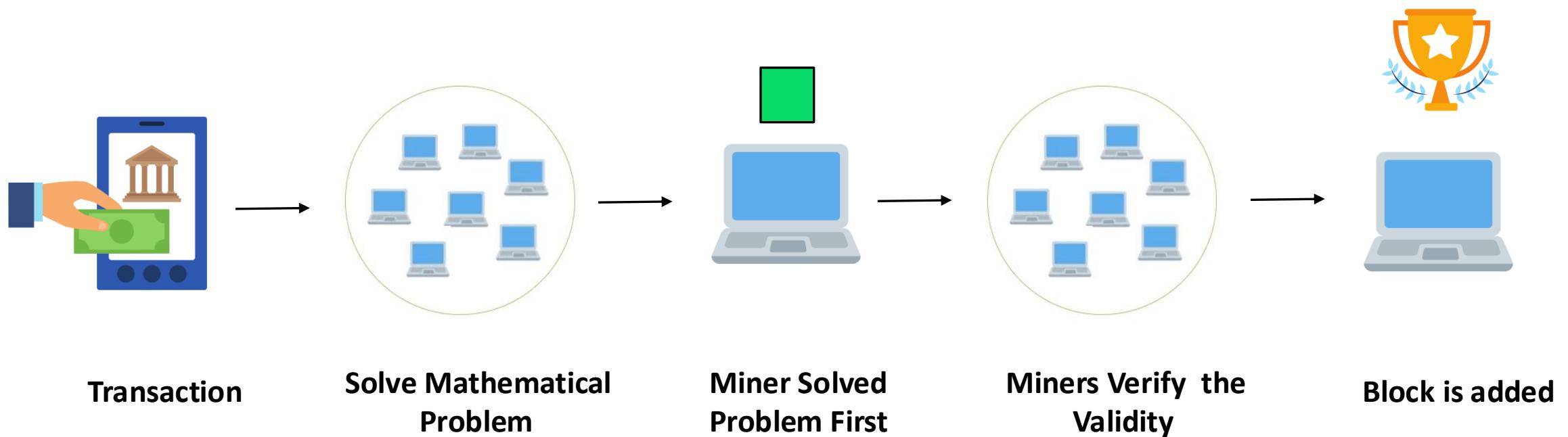
CODE EATER

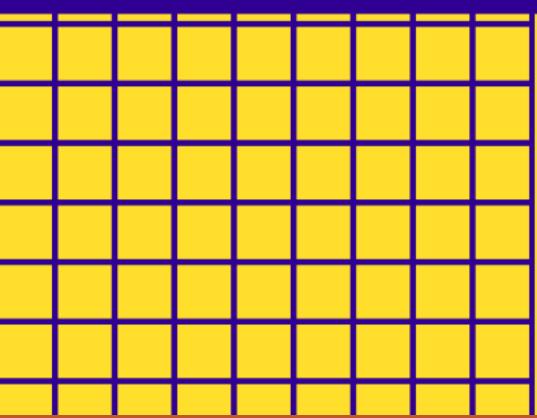
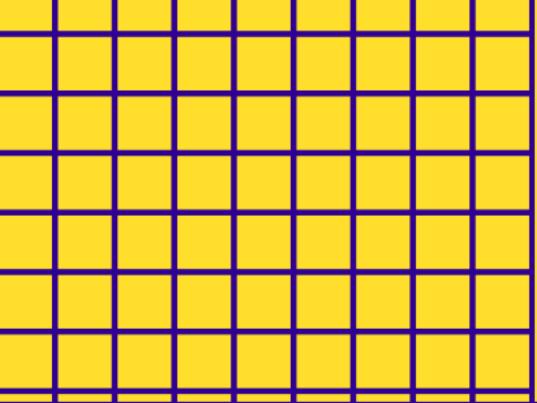


A complex, abstract digital background on the left side of the slide. It features a grid pattern with various shades of blue. Overlaid on the grid are several concentric, semi-transparent circles and arcs in different shades of blue and white. Small, white binary digits (0s and 1s) are scattered across the entire background, appearing both within the circular patterns and outside them. The overall effect is futuristic and technological.

Blockchain Mining

Blockchain Mining





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



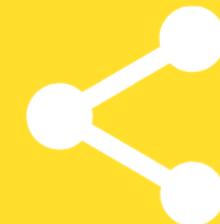
Discord – Link in description

Blockchain Mining

Trust, secure,

**GIVE THIS VIDEO
A THUMBS-UP !**

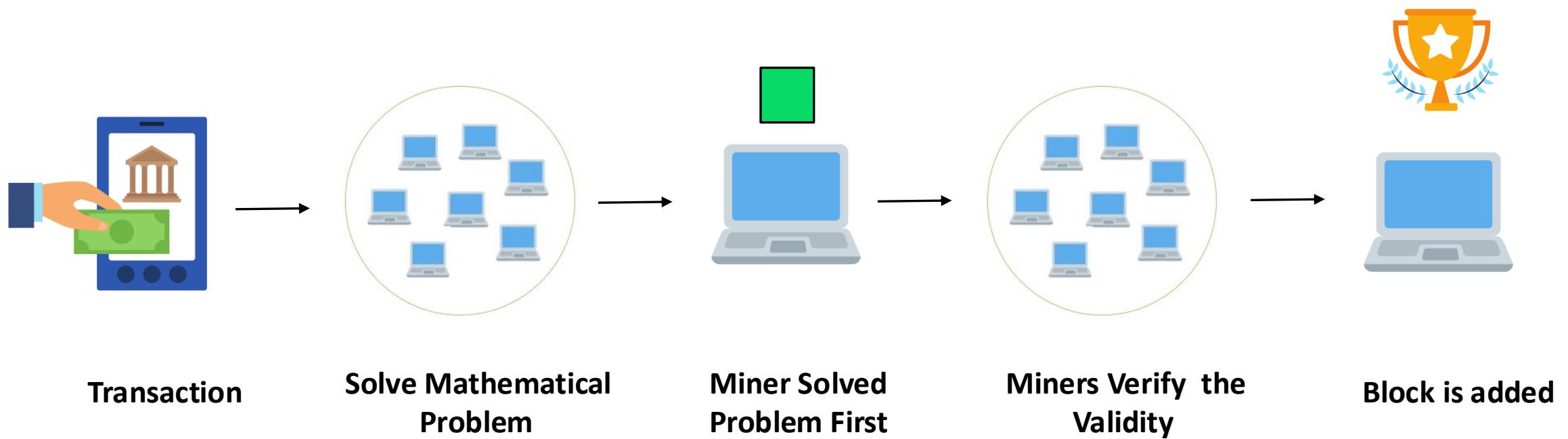
CODE EATER



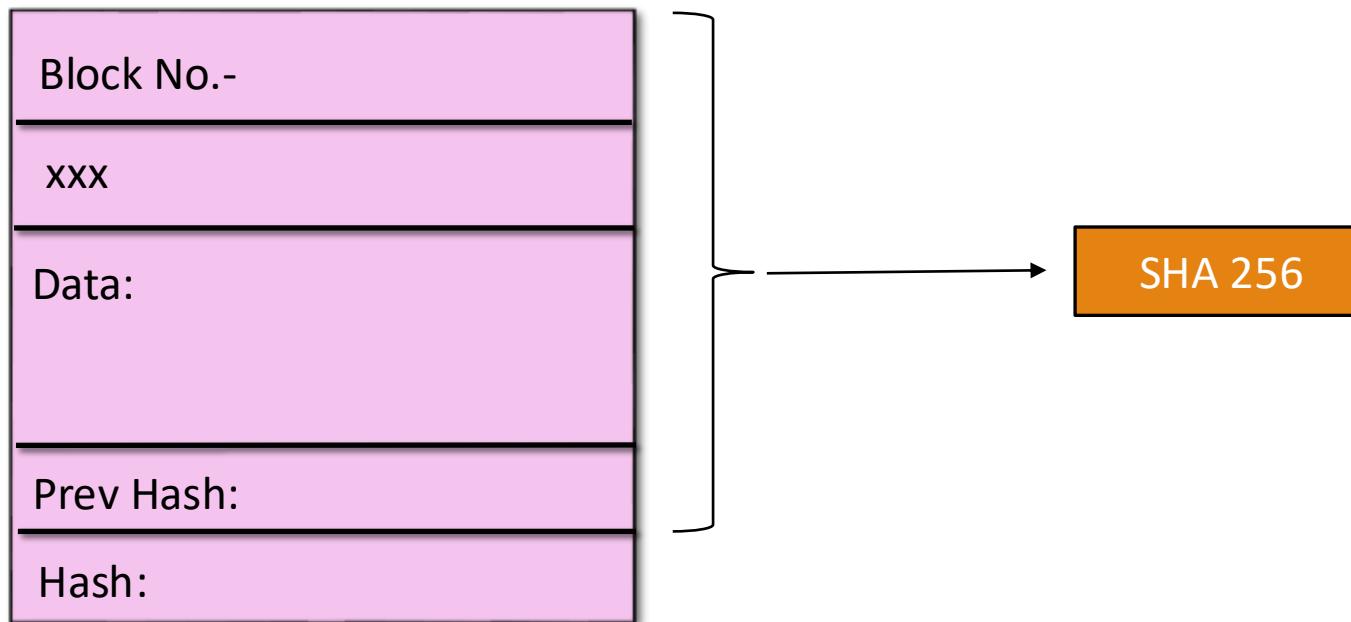


How Mining works: The Nonce

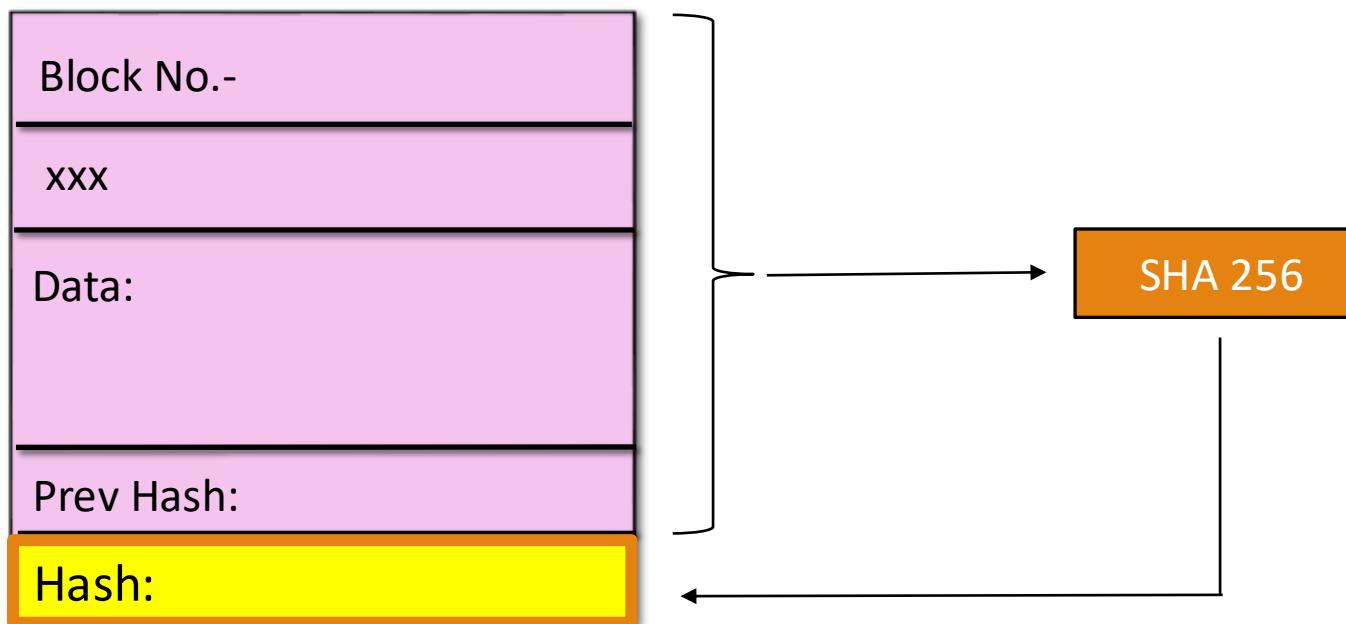
Blockchain Mining



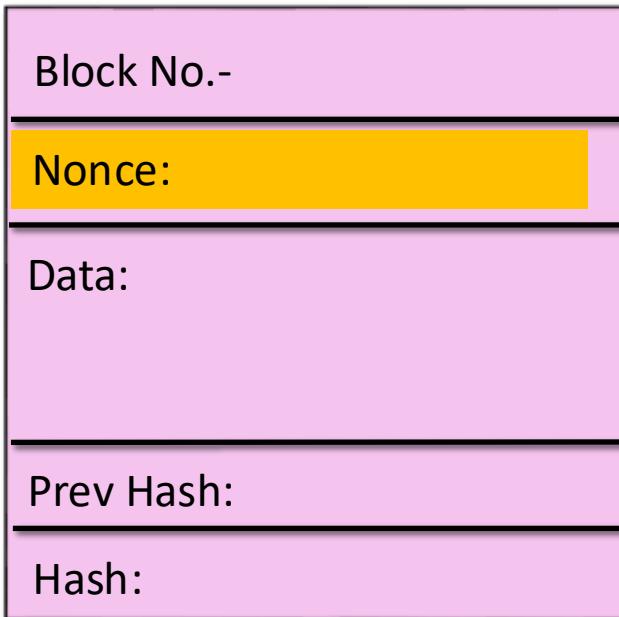
TheNonce



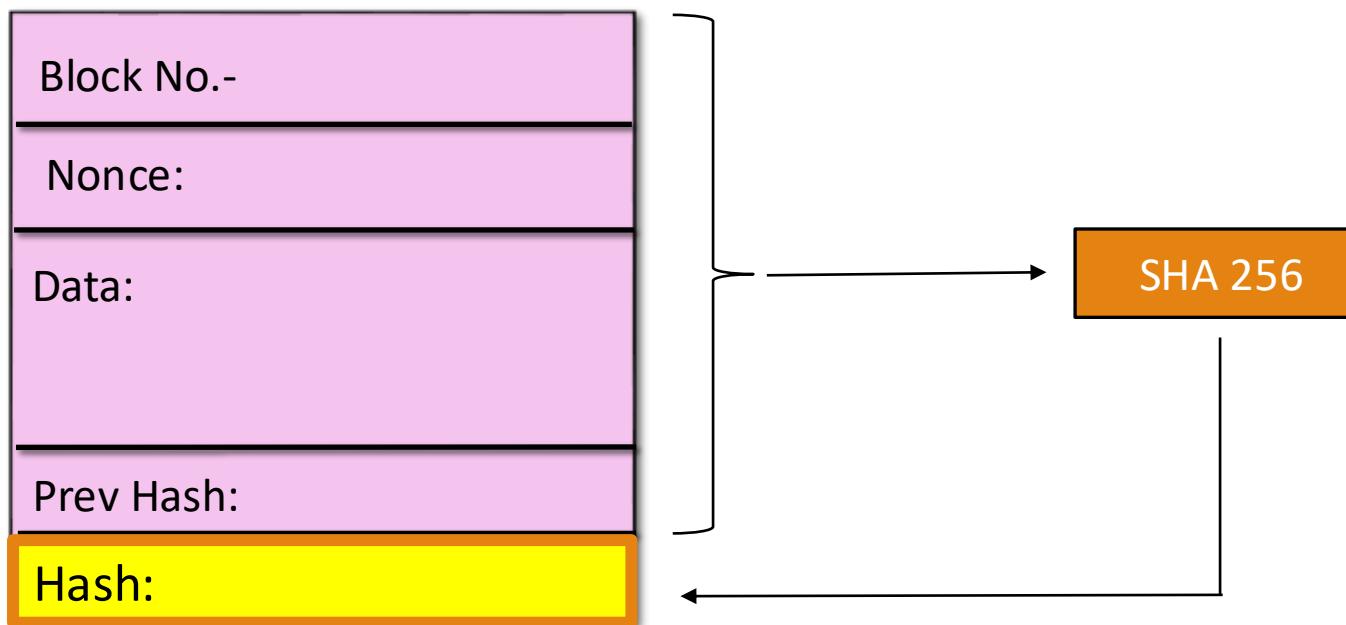
TheNonce



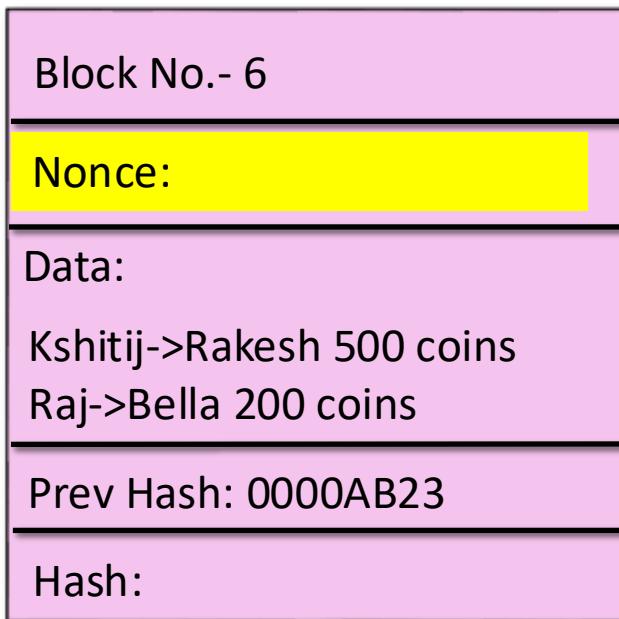
TheNonce



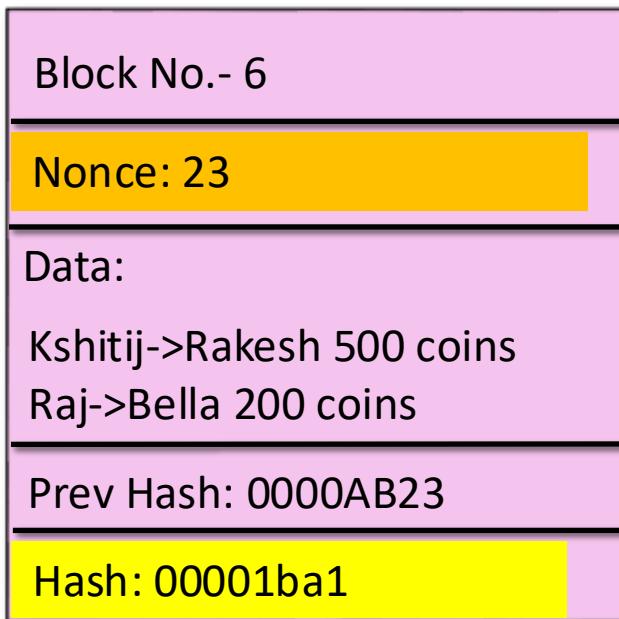
The Nonce



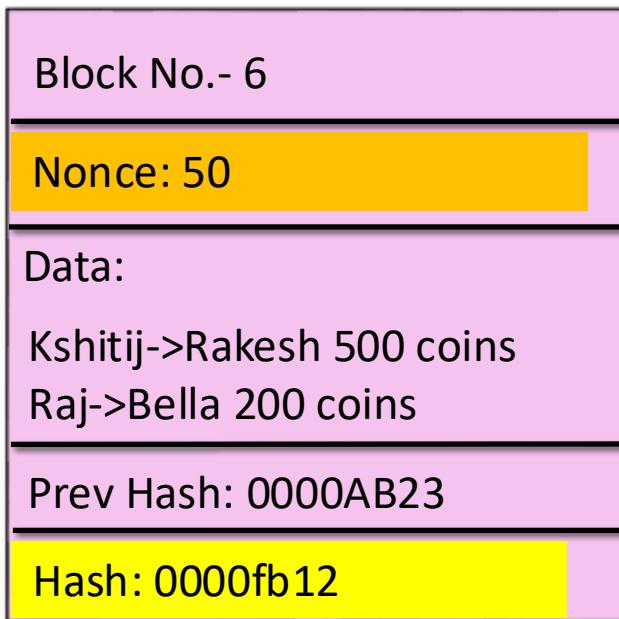
TheNonce



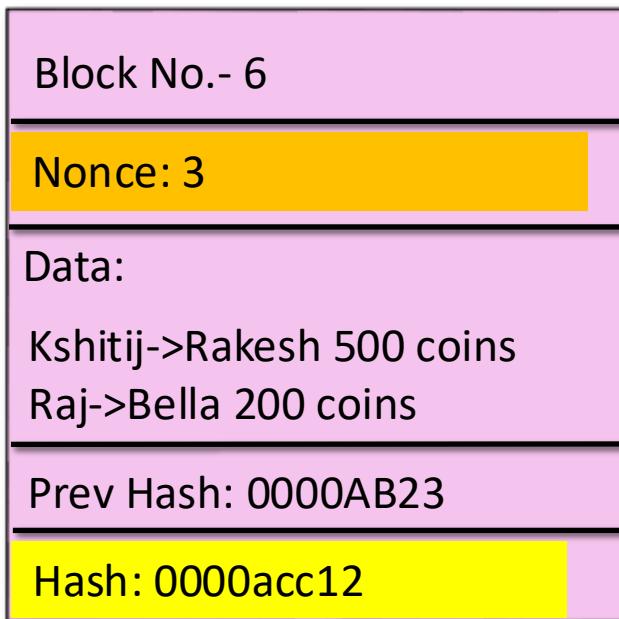
TheNonce



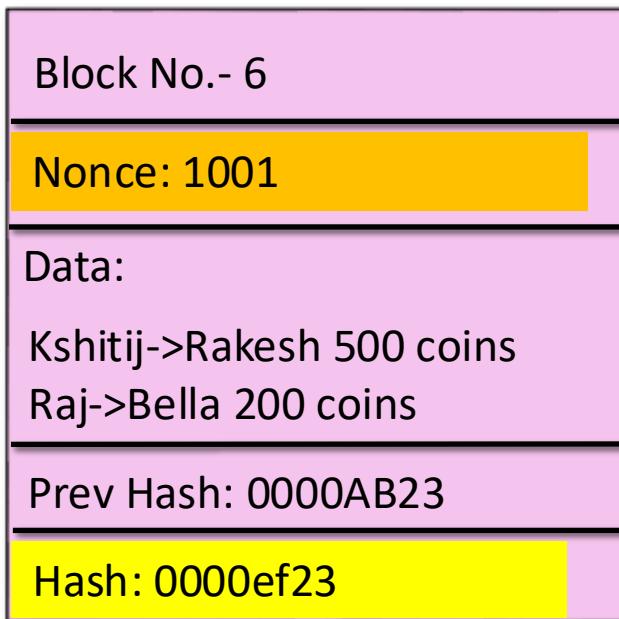
TheNonce



TheNonce

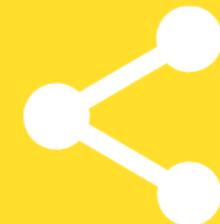


TheNonce



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





How Mining works: The Nonce

How Mining Works ?

Nonce

Target

How Mining Works ?

Nonce:

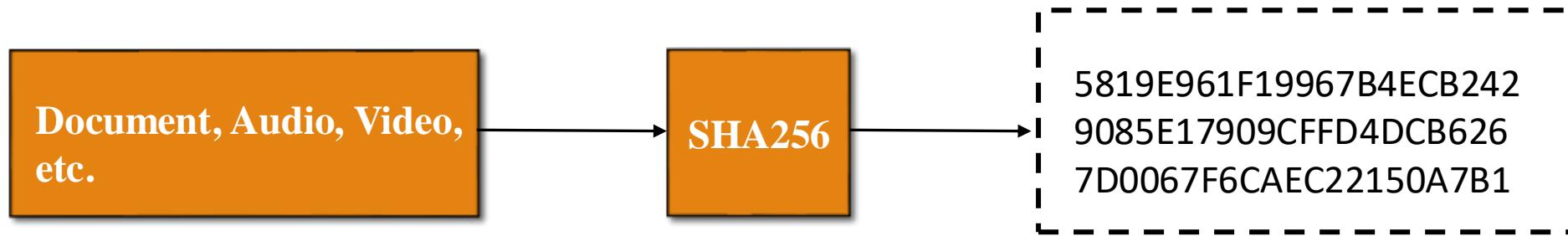
- The nonce is a number that blockchain miners are solving for.

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.

Hashing Algorithm



This has **64 hexadecimal characters**.
Each character is of **4 bits**.
So in total it has $64 * 4$ bits i.e. **256 bits**.

How Mining Works ?

Hexadecimal Numbers

Decimal	Hexadecimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A

Decimal	Hexadecimal
11	B
12	C
13	D
14	E
15	F

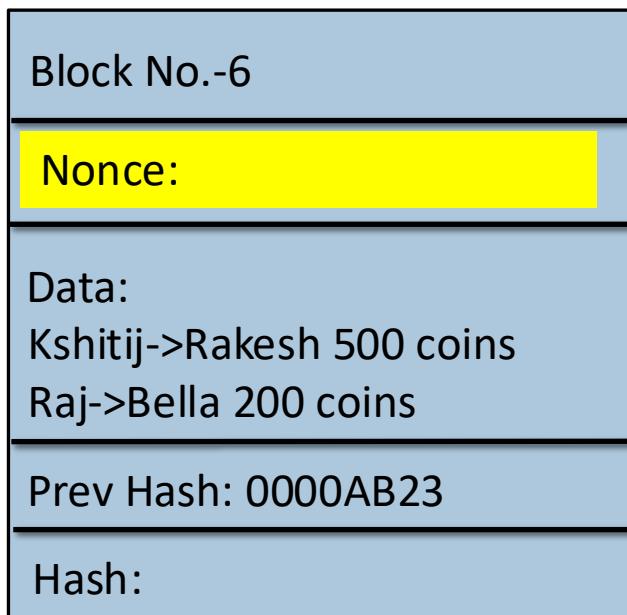
How Mining Works ?

- d2fd3930d274b202fe8e7cb431e38a8b64ec396e15f5717e60493234b0de210a
- 52d095795c1dc87ff2f6b4d9b005a1fe2cfed01103763c9443f6d4496df8e800
- 0000005432d9f64f6e05c019f9302162100163b6cdba06bd72eee35cd19aebf

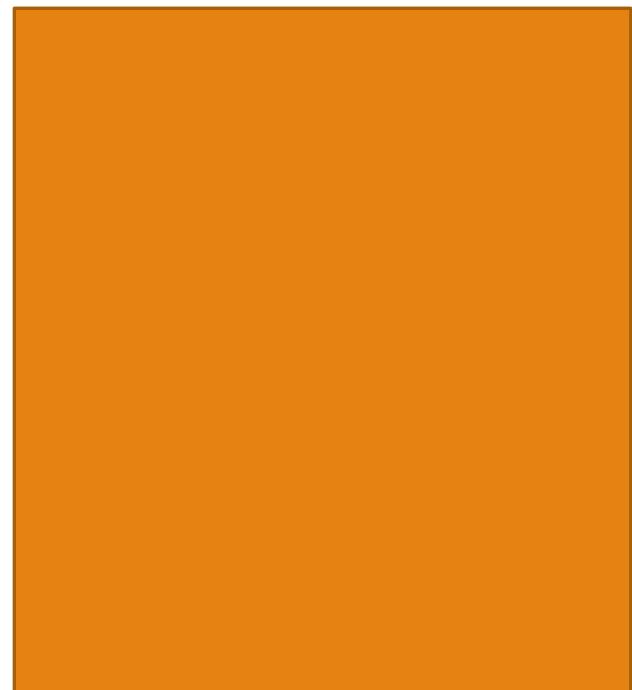
Smallest- 0000000.....0

Largest- ffffffff.....f

How Mining Works ?

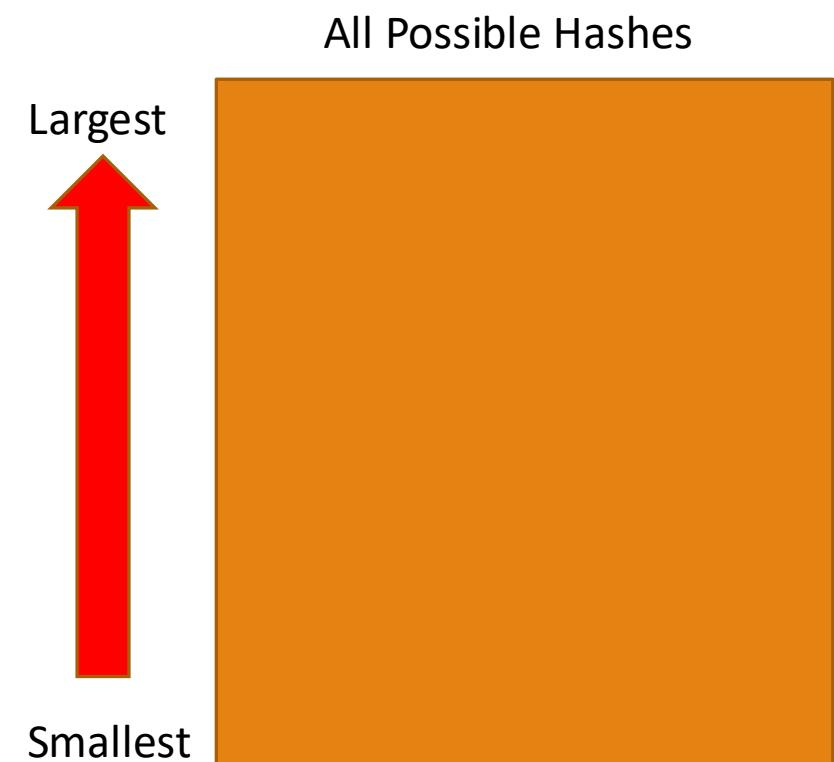


All Possible Hashes



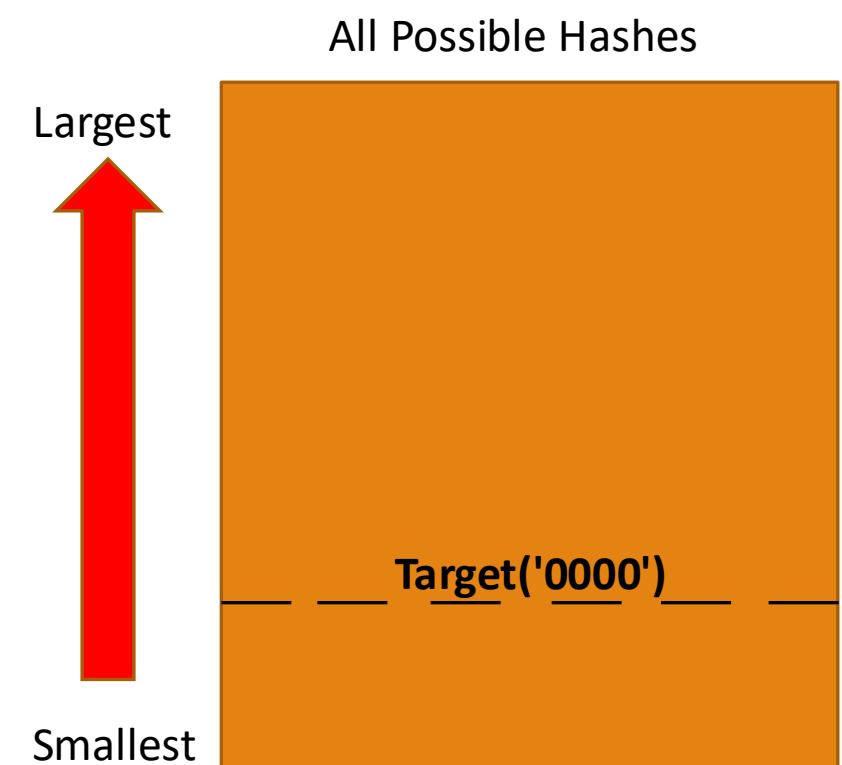
How Mining Works ?

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

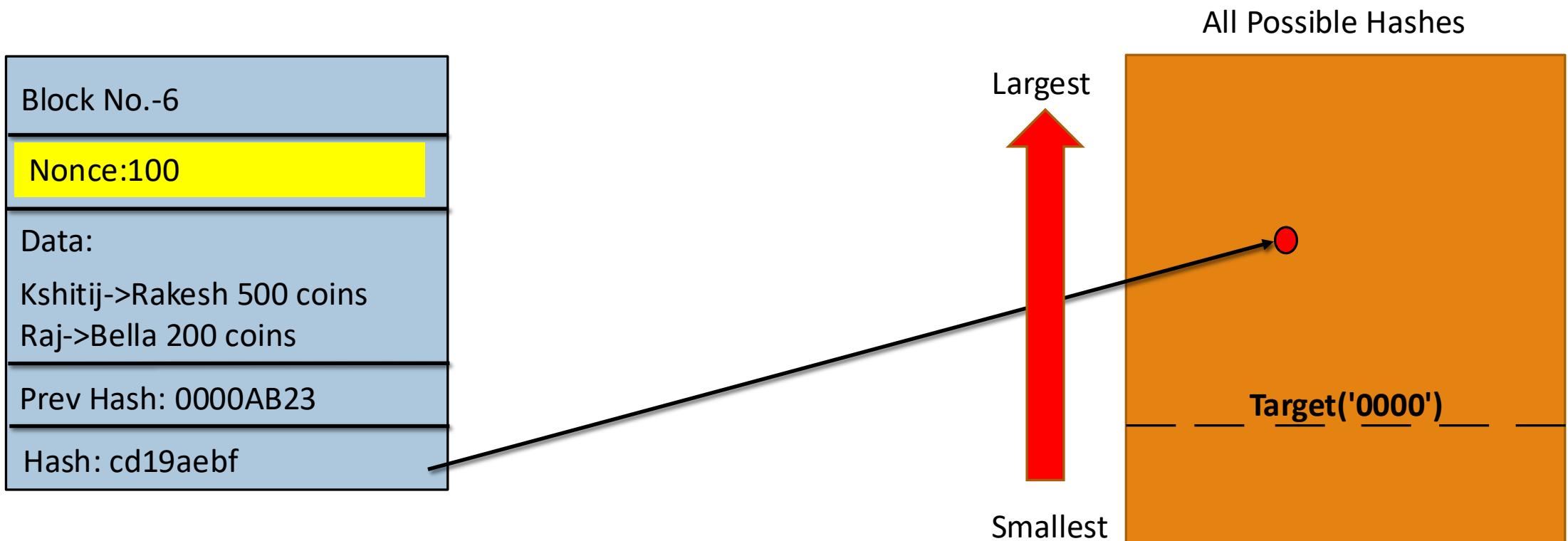


How Mining Works ?

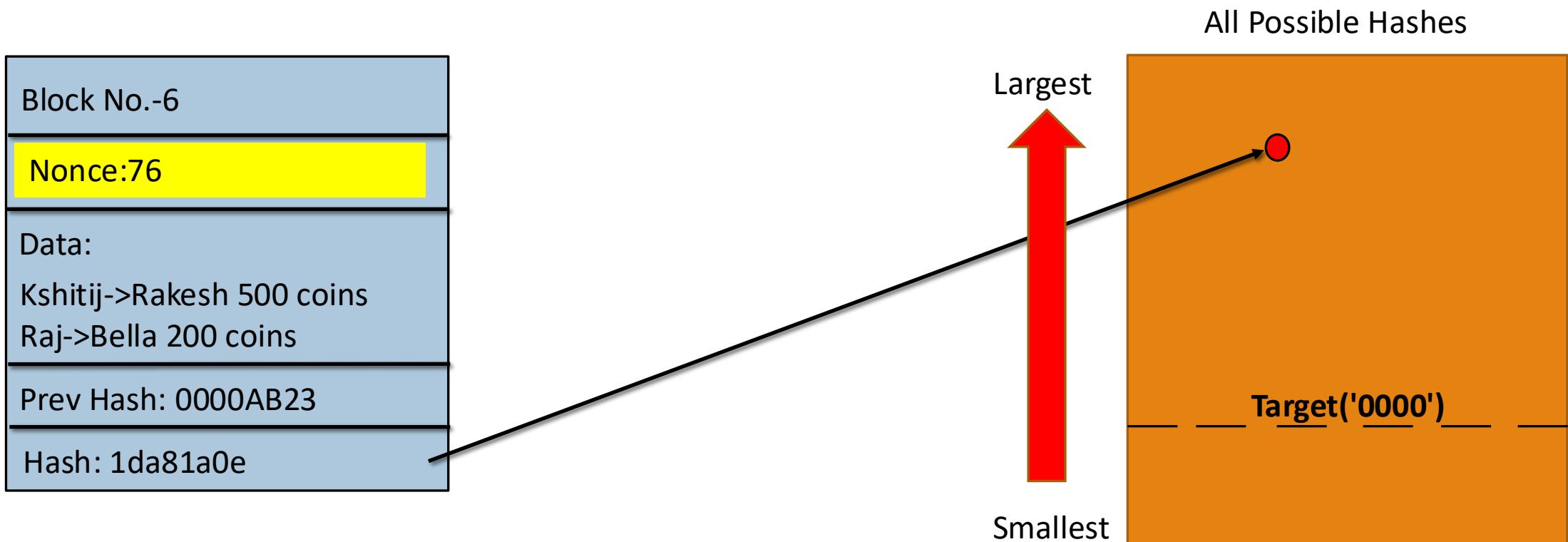
Block No.-6
Nonce:
Data: Kshitij->Rakesh 500 coins Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash:



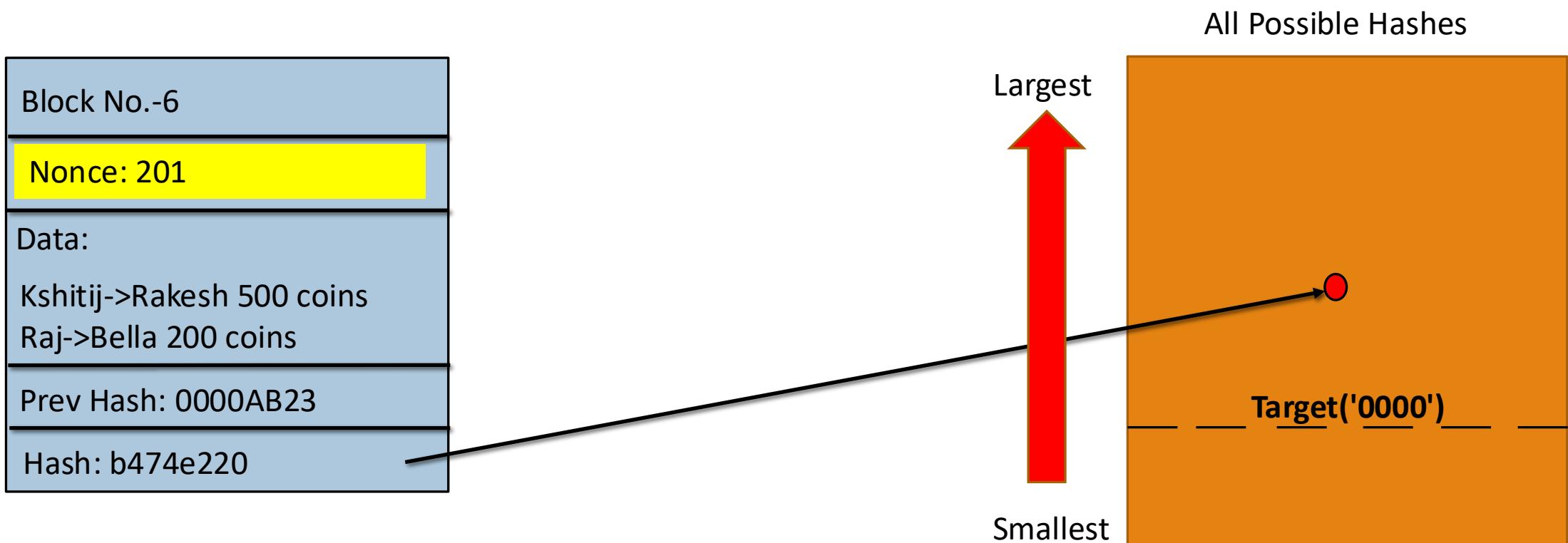
How Mining Works ?



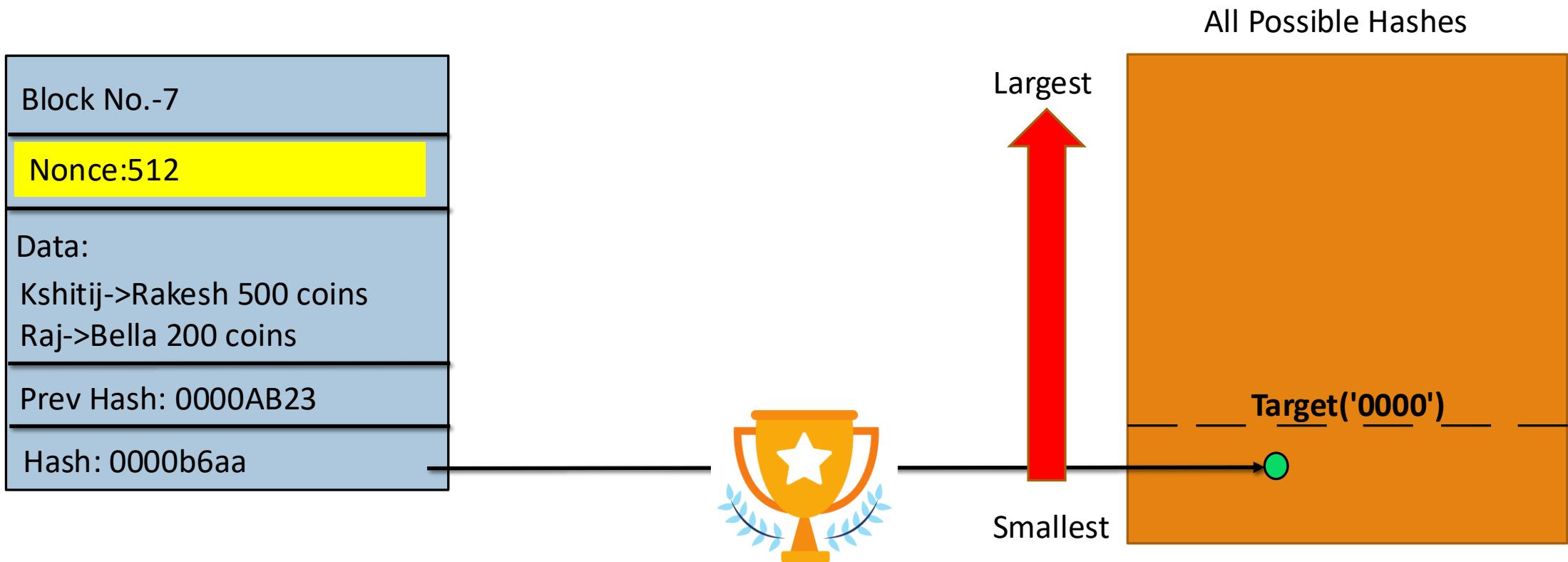
How Mining Works ?



How Mining Works ?

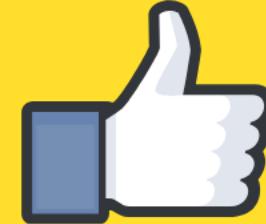


How Mining Works ?



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

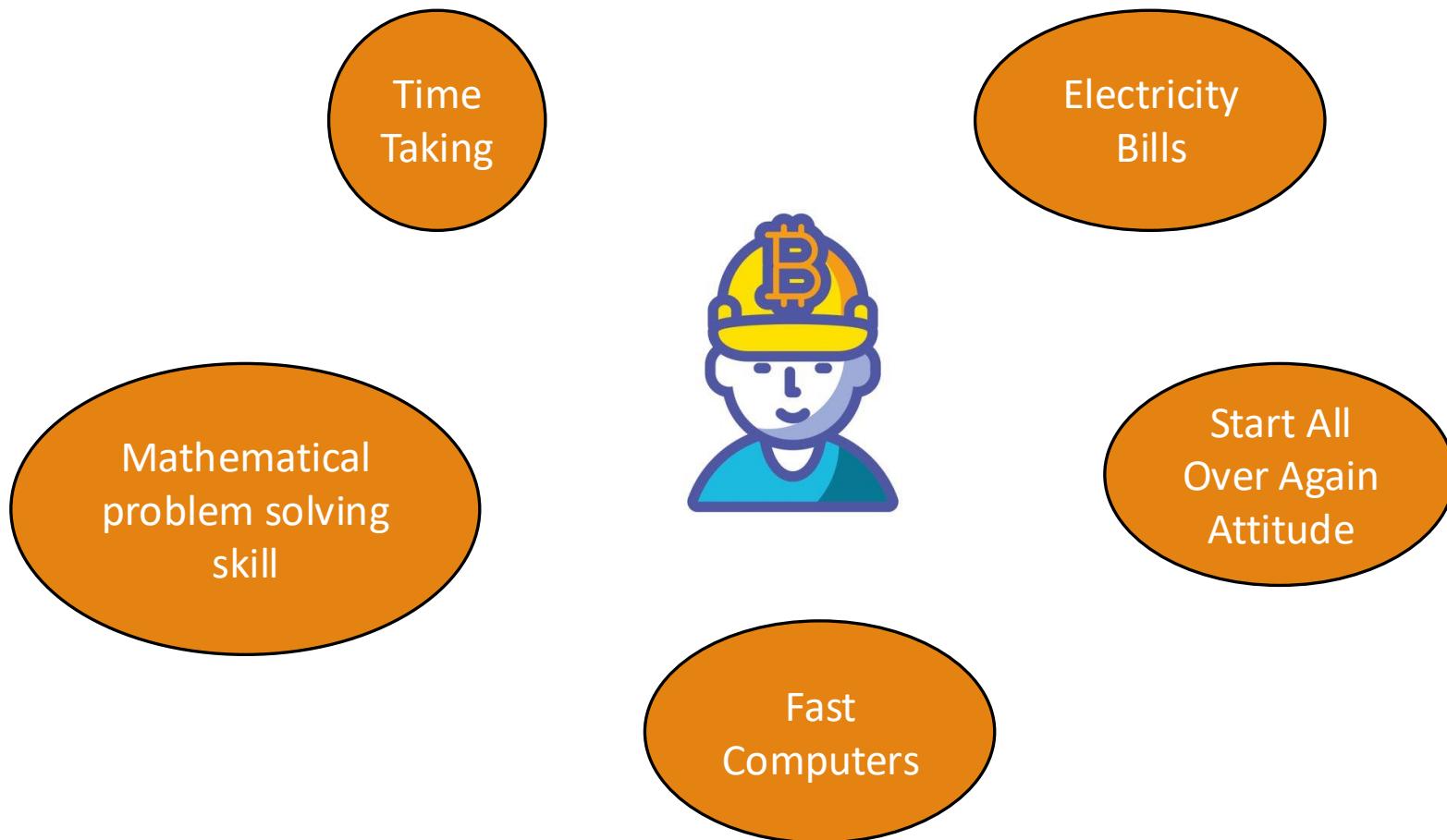


Blockchain Demo



Is Mining that easy?

Challenges faced by Miners



What is Mining?

What is mining? Why mining is required? Nonce basics ? None advanced

Why Mining is required?

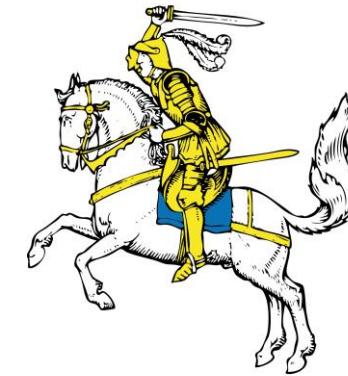
A complex, abstract digital background composed of a grid of blue and white squares. Overlaid on this grid are several concentric, semi-transparent circles. The circles are primarily black with white dashed lines indicating segments. Interspersed throughout the image are numerous binary digits (0s and 1s) in a light blue color, appearing both within the grid cells and along the circumference of the circles.

Byzantine Generals Problem

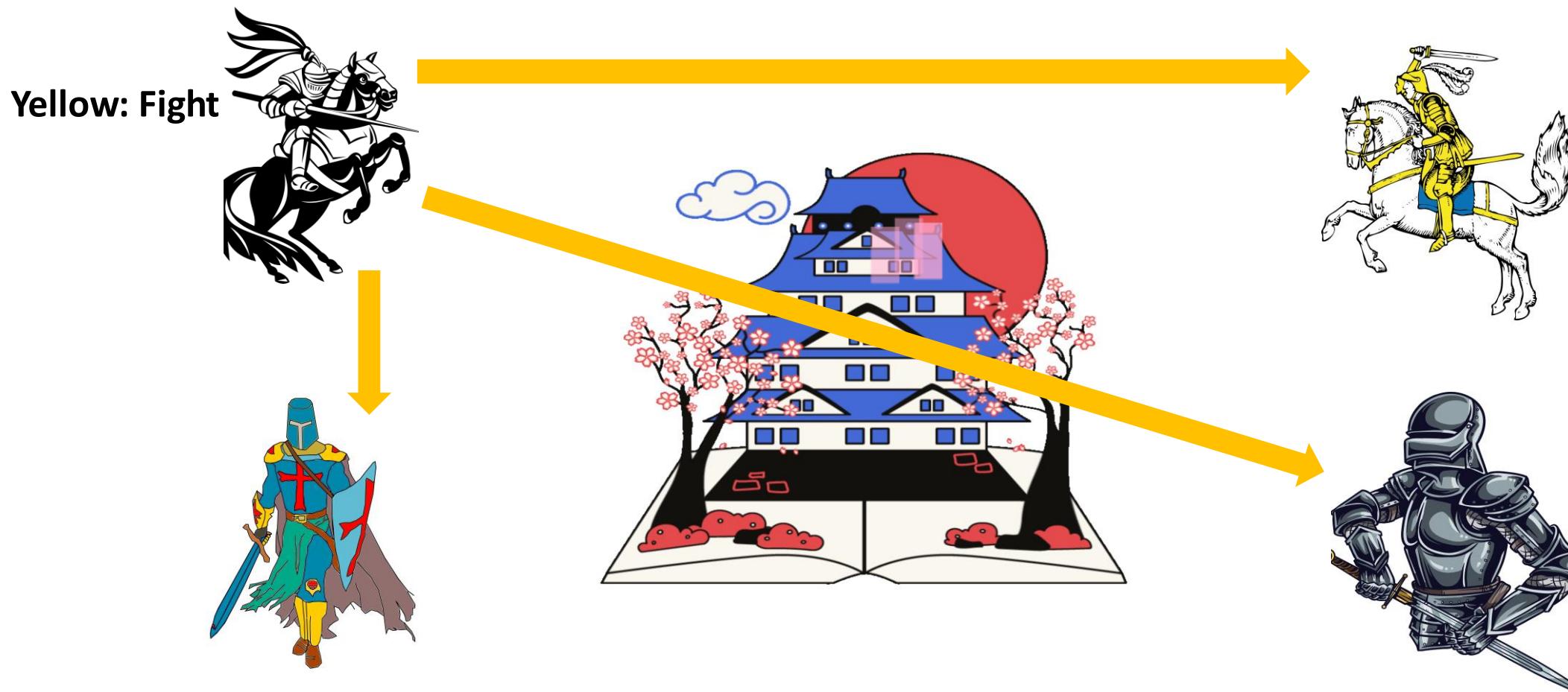
Byzantine Generals Problem



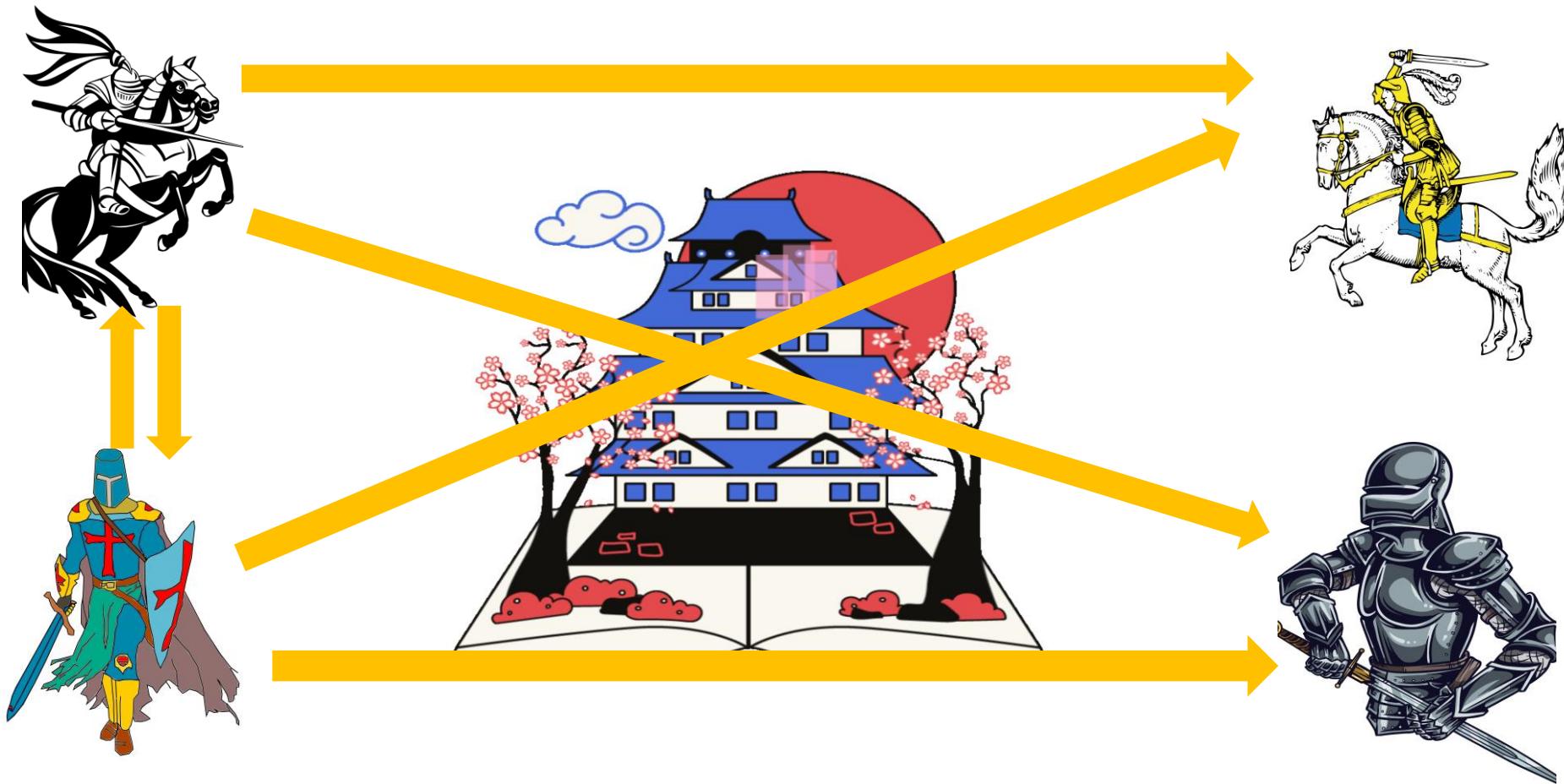
Byzantine Generals Problem



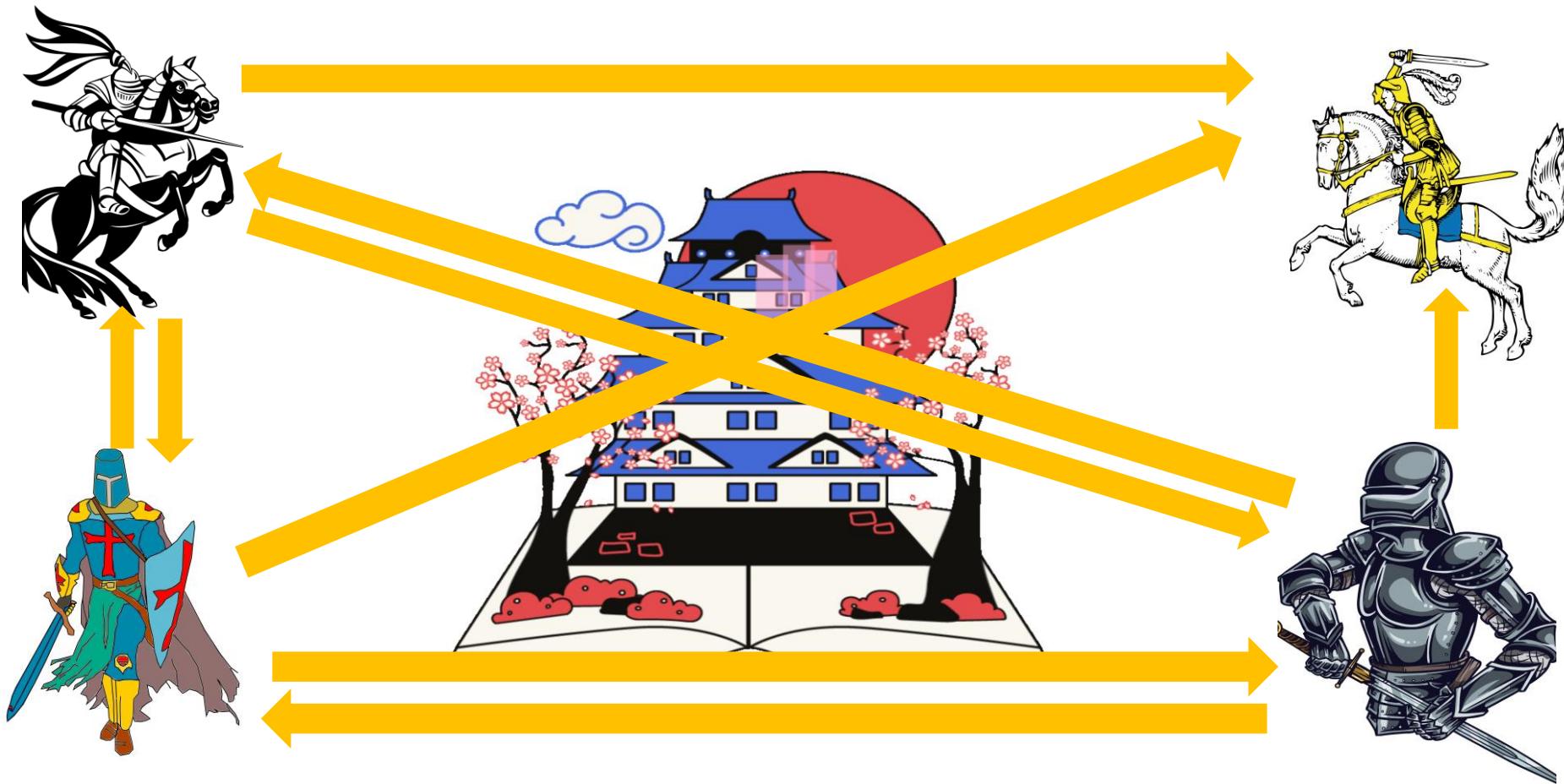
Byzantine Generals Problem



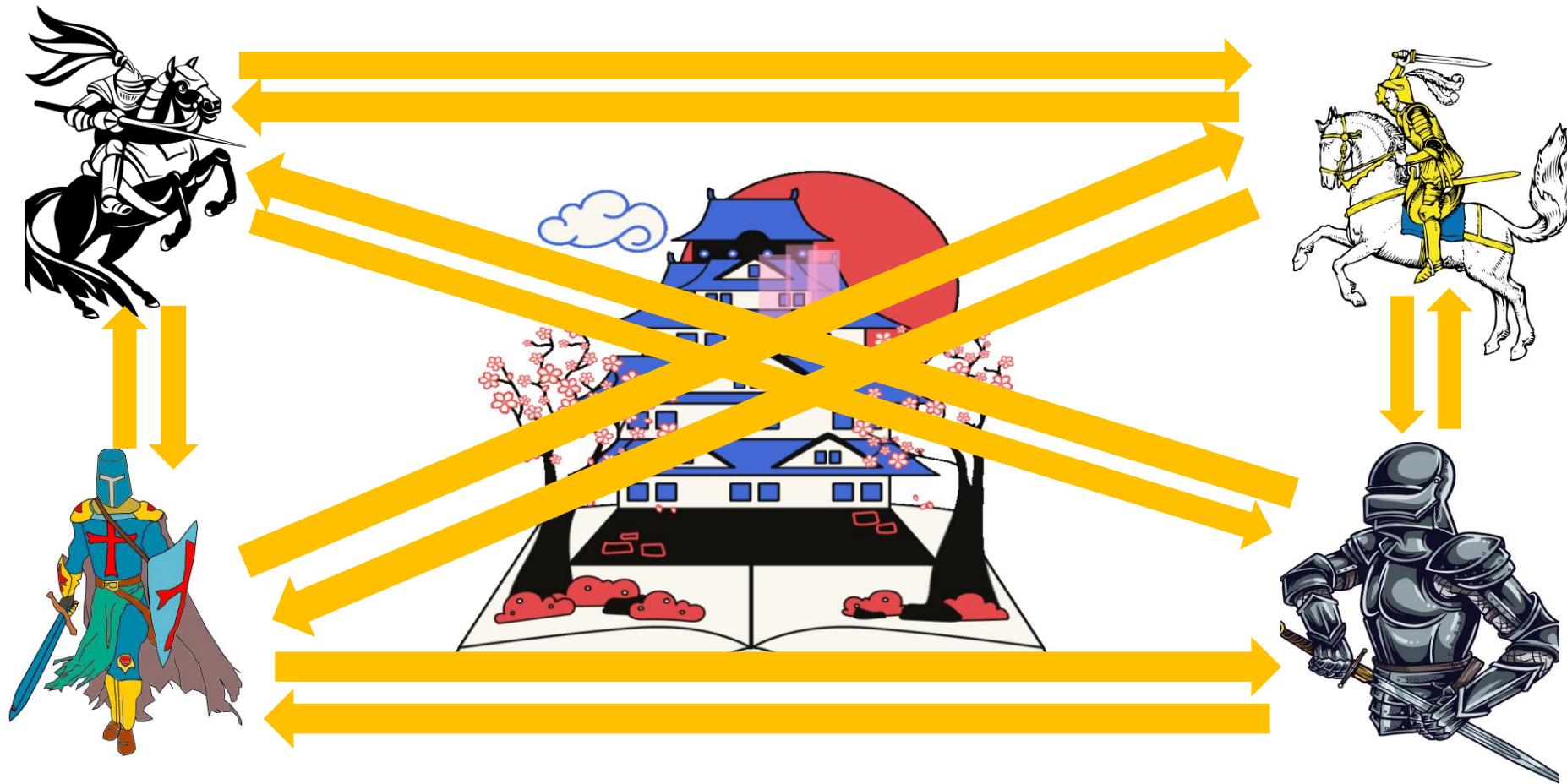
Byzantine Generals Problem



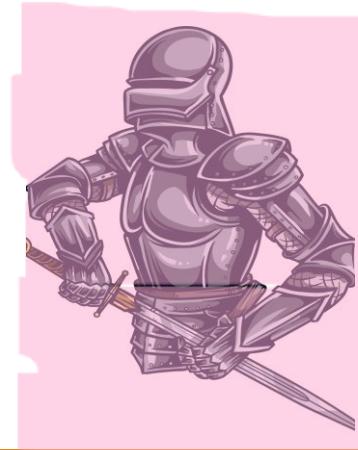
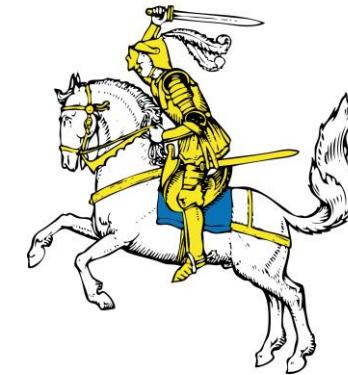
Byzantine Generals Problem



Byzantine Generals Problem

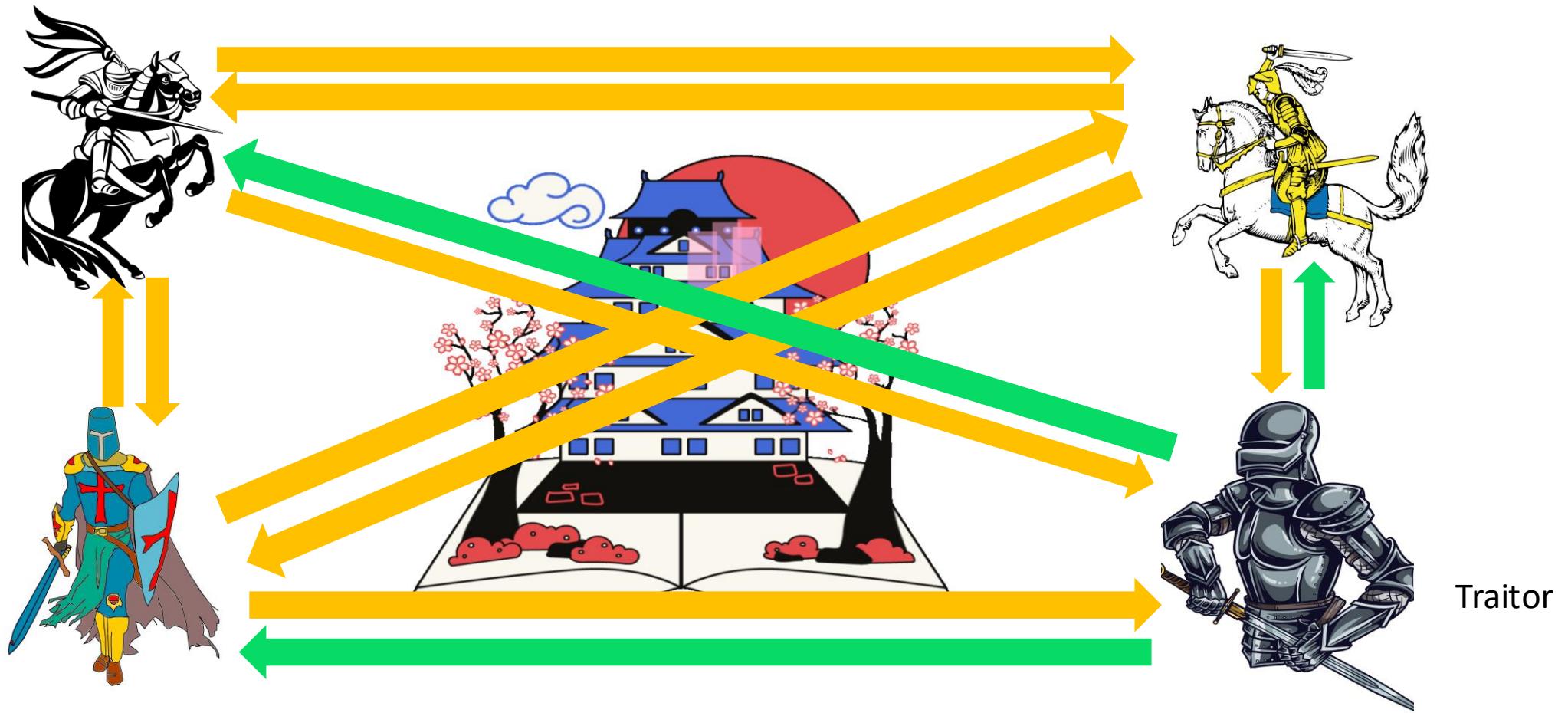


Byzantine Generals Problem



Traitor

Byzantine Generals Problem



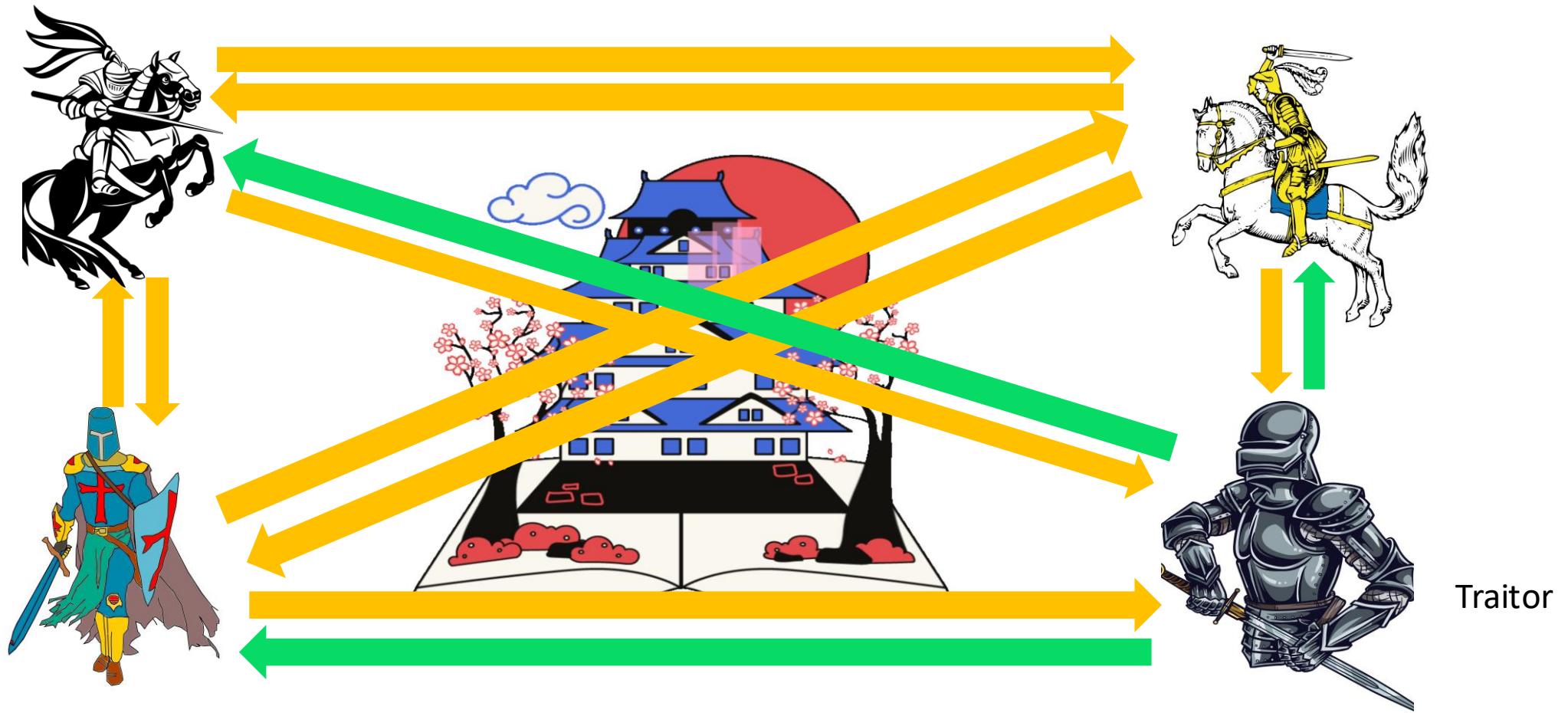
Practical Byzantine Fault Tolerance

by
Miguel Castro

Abstract

Our growing reliance on online services accessible on the Internet demands highly-available systems that provide correct service without interruptions. Byzantine faults such as software bugs, operator mistakes, and malicious attacks are the major cause of service interruptions. This thesis describes a new replication algorithm, BFT, that can be used to build highly-available systems that tolerate Byzantine faults. It shows, for the first time, how to build Byzantine-fault-tolerant systems that can be used in practice to implement real services because they do not rely on unrealistic assumptions and they perform well. BFT works in asynchronous environments like the Internet, it incorporates mechanisms to defend against Byzantine-faulty clients, and it recovers replicas proactively. The recovery mechanism allows the algorithm to tolerate any number of faults over the lifetime of the system provided fewer than $1/3$ of the replicas become faulty within a small window of vulnerability.

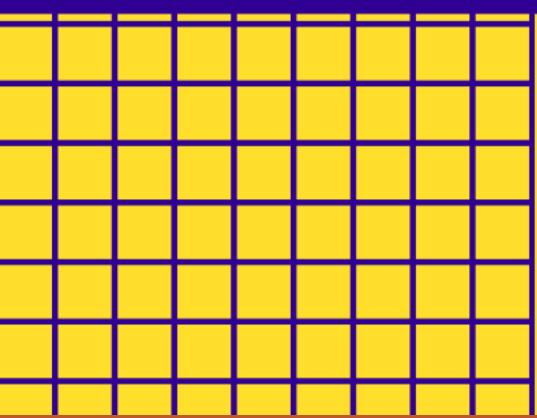
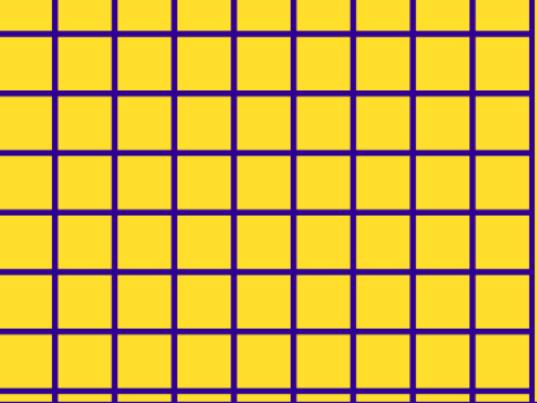
Byzantine Generals Problem





Byzantine Generals Problem

Q) How this Byzantine Fault Tolerance works in Blockchain?



Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

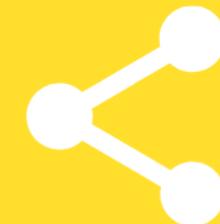
CODE EATER



Discord – Link in description

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



A complex, abstract digital graphic on the left side of the slide. It features a grid of blue and white squares, similar to a binary matrix. Overlaid on this grid are several concentric, semi-transparent circles in shades of blue and grey. One prominent circle is light blue with white tick marks around its perimeter. Another circle is darker blue with a more intricate, segmented pattern. Small, white binary digits (0s and 1s) are scattered across the entire graphic, appearing both within the grid and along the edges of the circles.

Consensus Protocol

Consensus Protocol

- Hashing Algorithm 
- Immutable Ledger 
- Mining 
- Distribute P2P network 

Consensus Protocol

Prevent Attacks

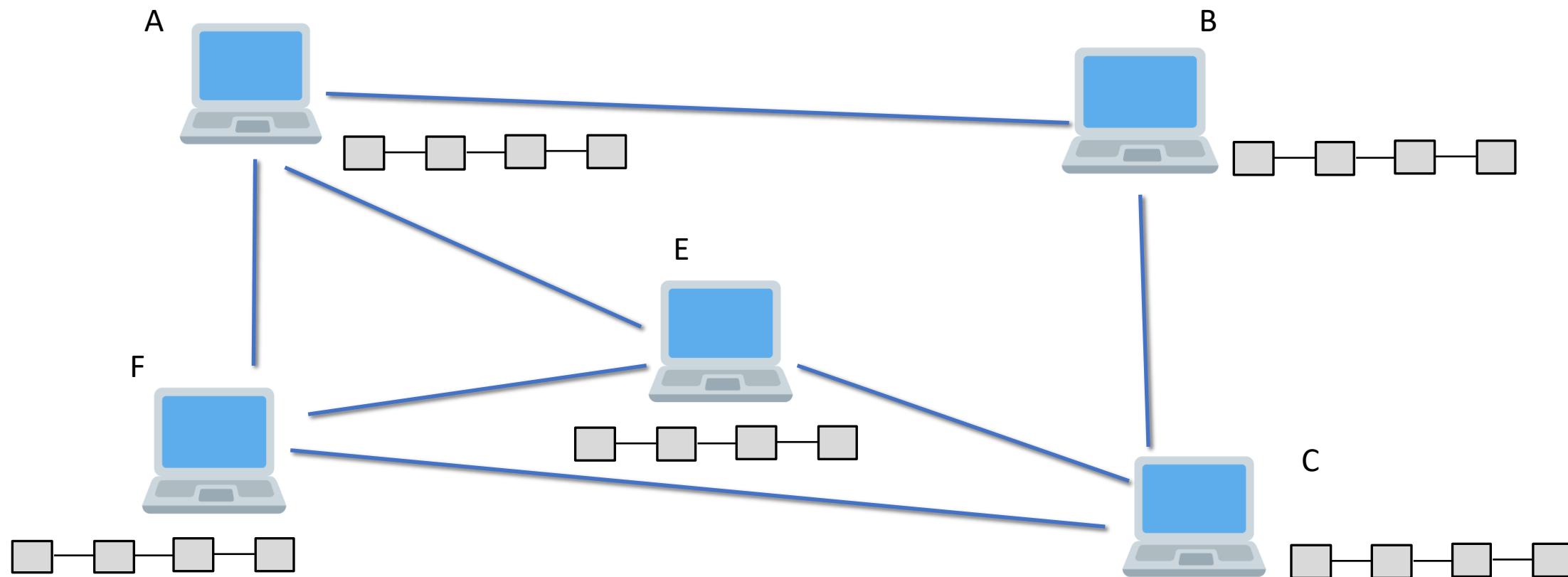
Competing Chain Problem

Consensus Protocol

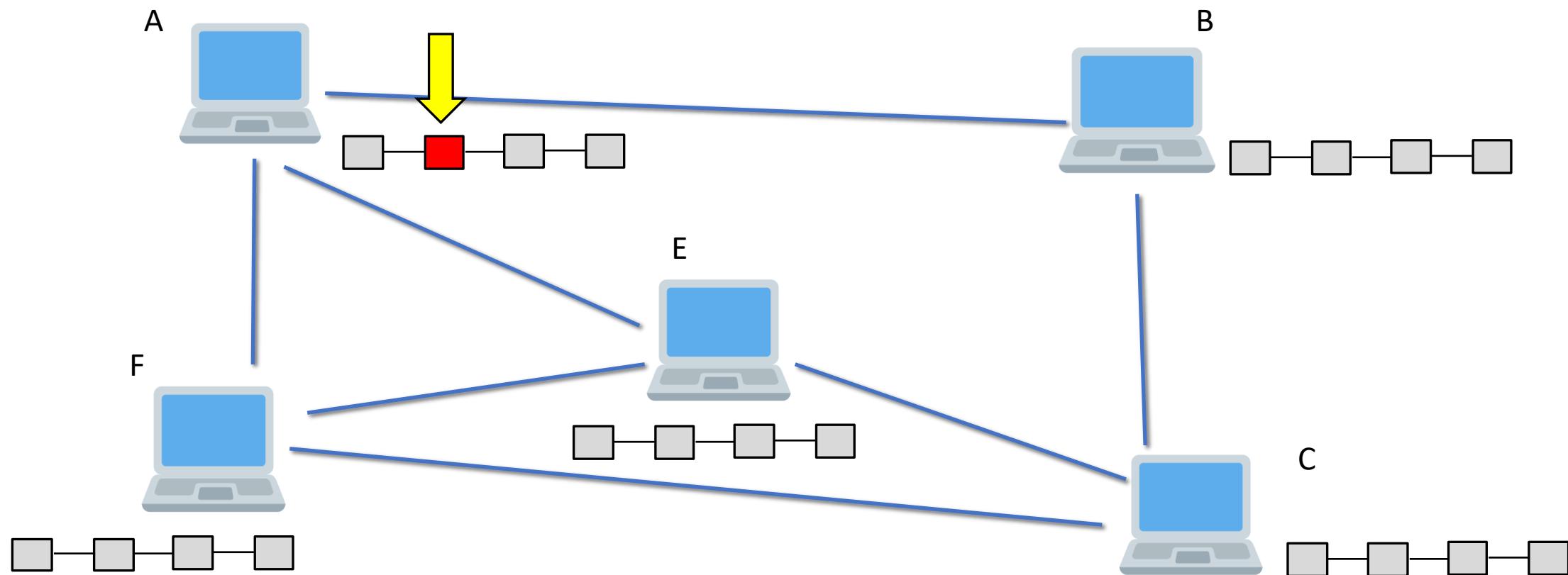
Types of Consensus Protocol-

- **Proof of Work (POW)**
- **Proof of Stake (POS)**
- **Others**

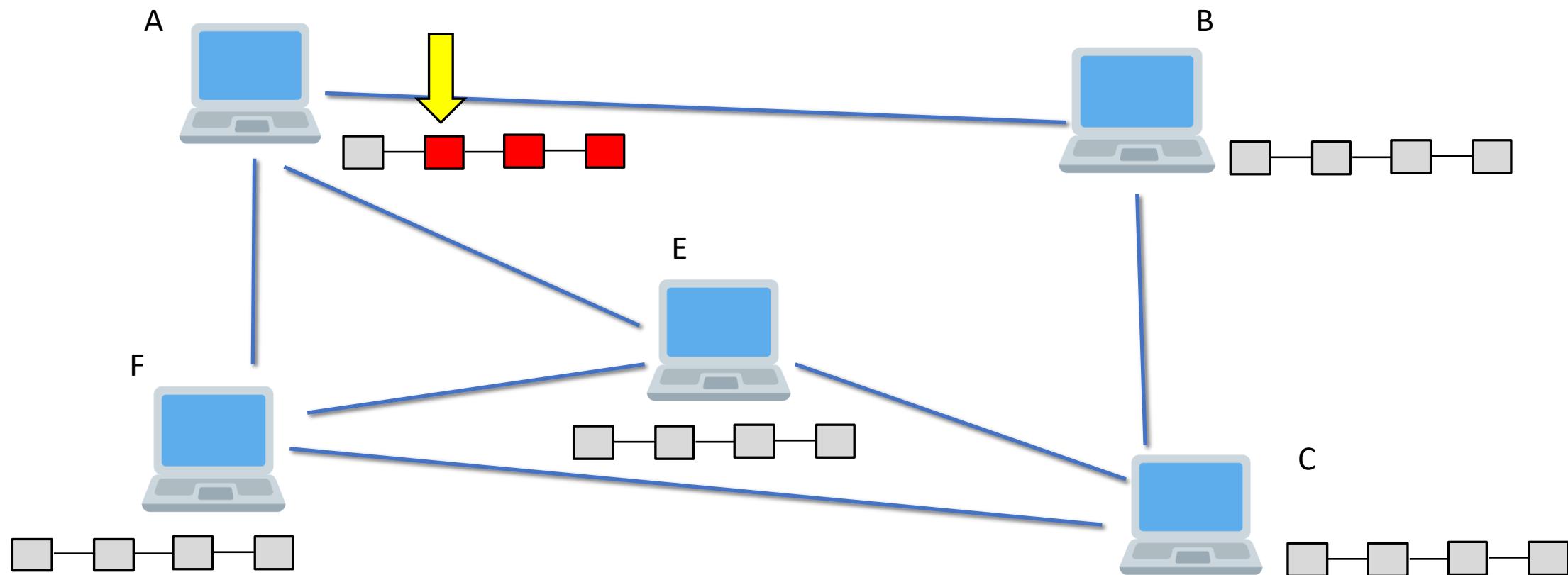
Consensus Protocol



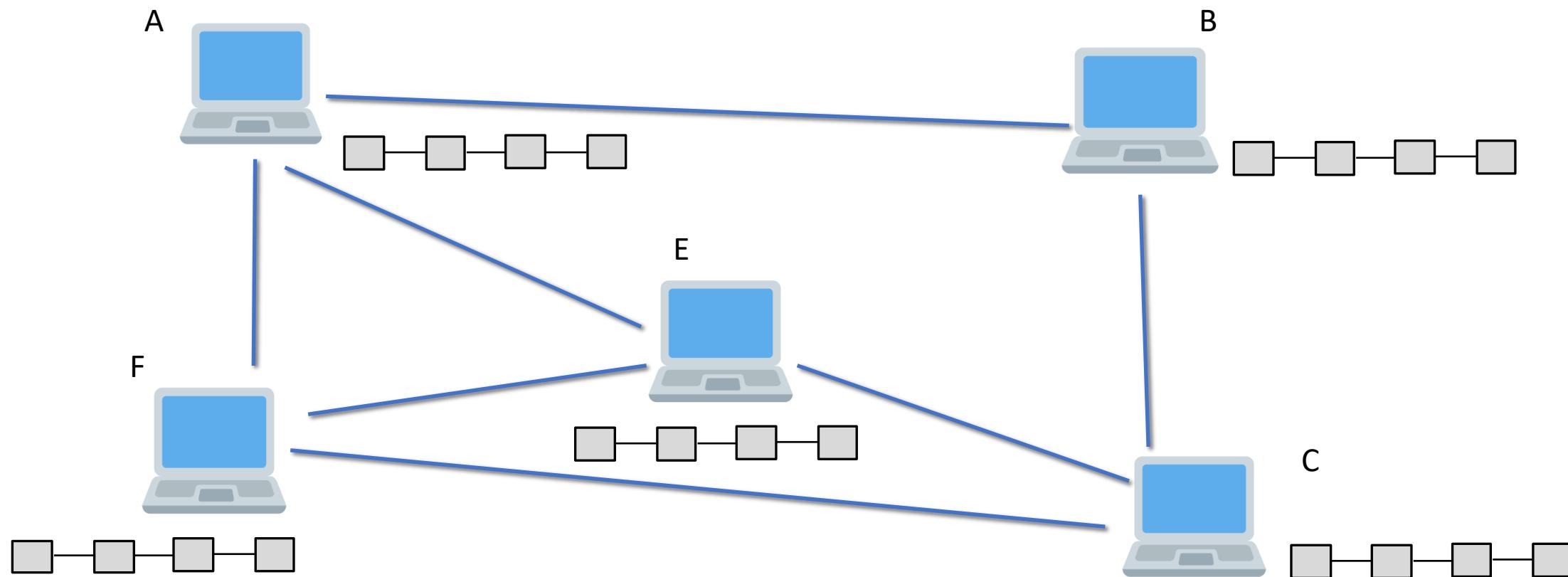
Consensus Protocol



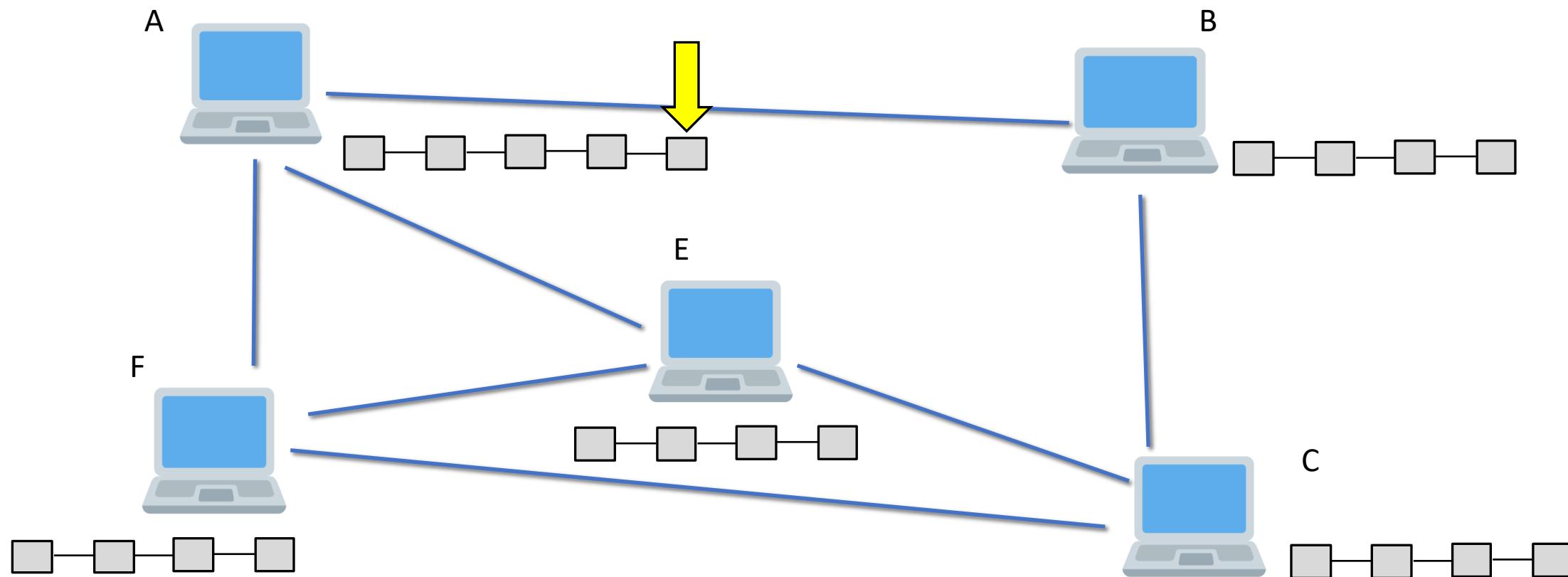
Consensus Protocol



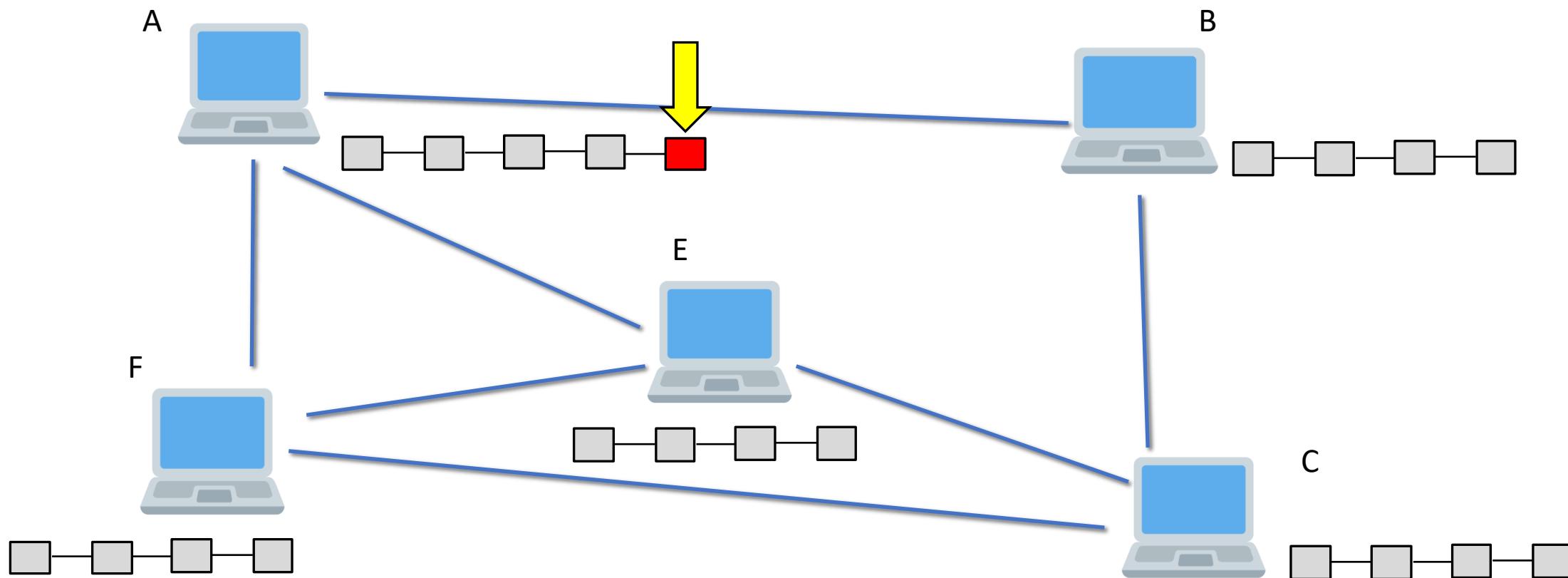
Consensus Protocol



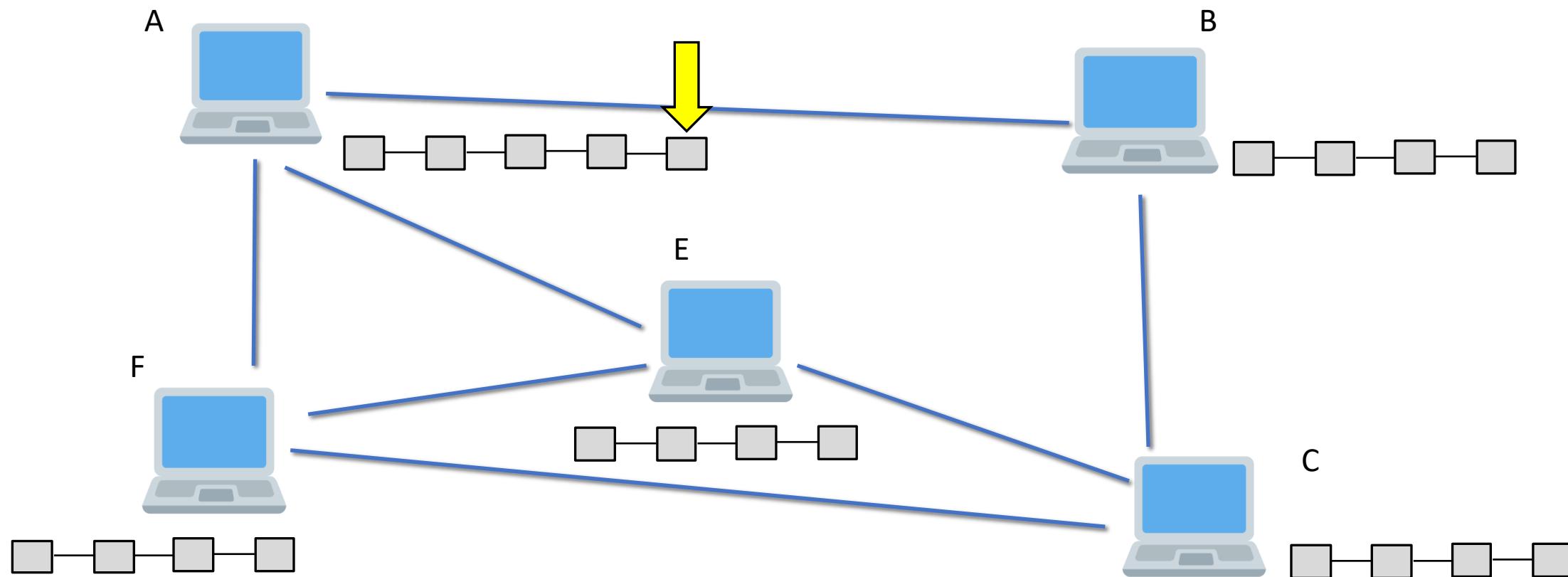
Consensus Protocol



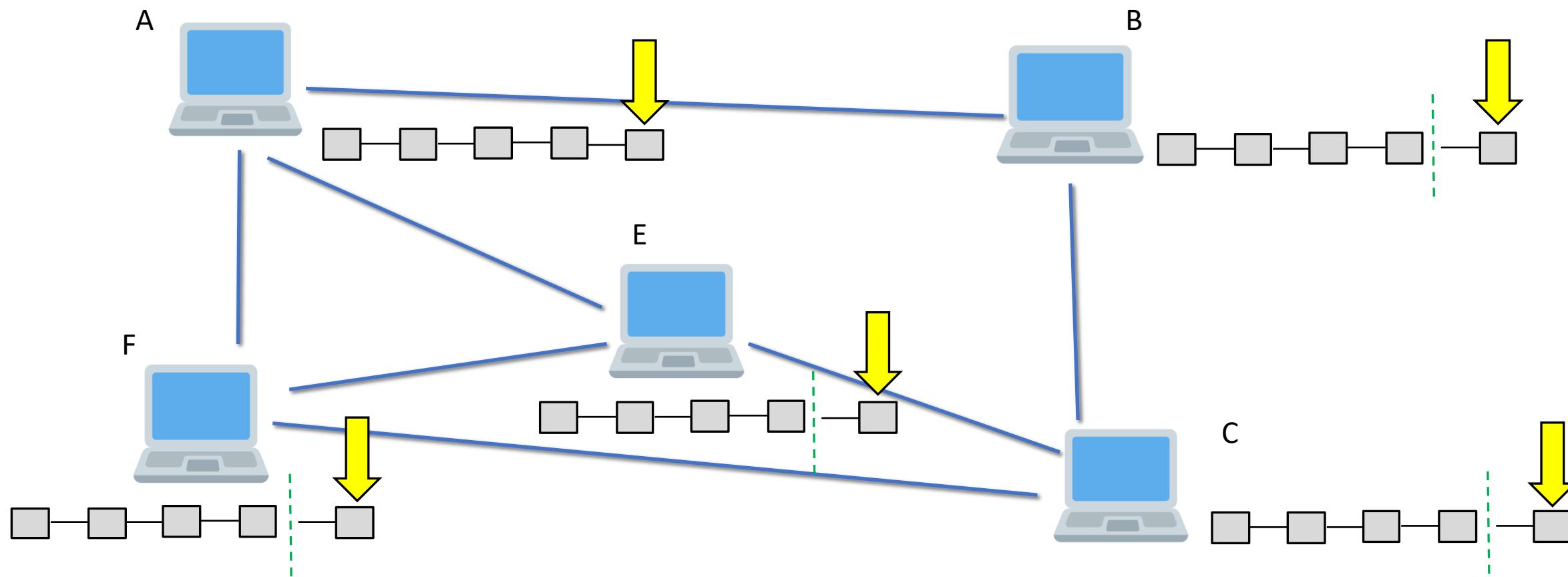
Consensus Protocol



Consensus Protocol

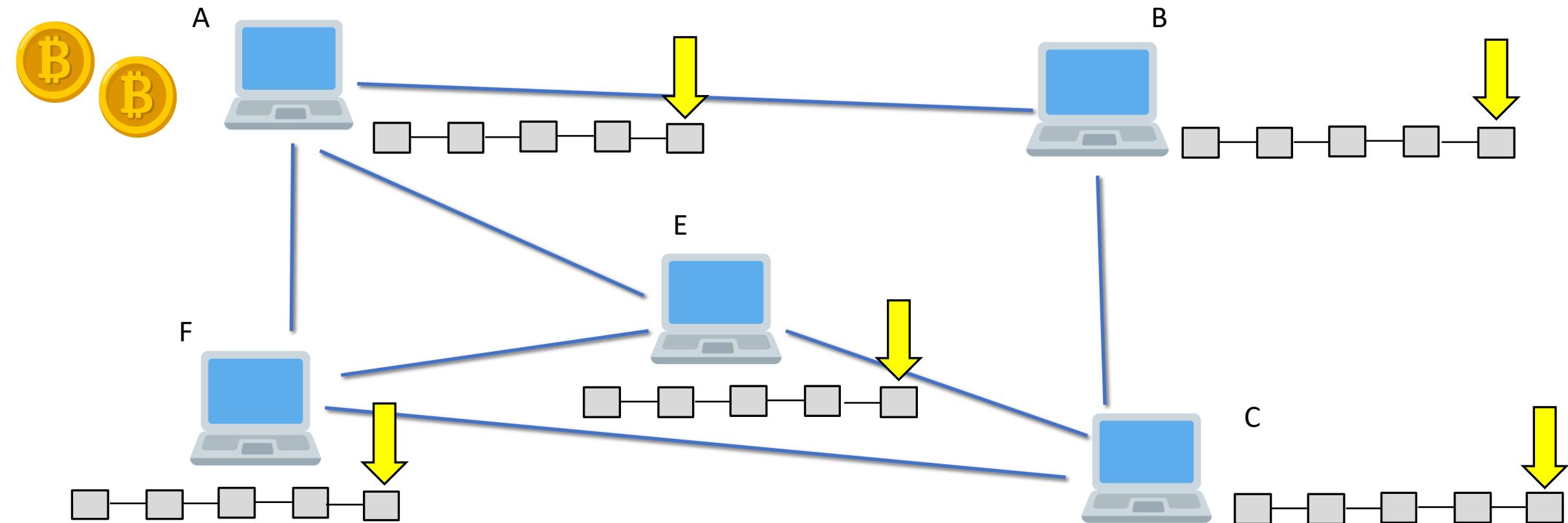


Consensus Protocol



1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed nBits proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be
7. For each transaction, apply "tx" checks 2-4
8. For the coinbase (first) transaction, scriptSig length must be 2-100
9. Reject if sum of transaction sig opcounts > MAX_BLOCK_SIGOPS
10. Verify Merkle hash
11. Check if prev block (matching prev hash) is in main branch or side branches. If not, add this to orphan block in prev chain; done with block
12. Check that nBits value matches the difficulty rules
13. Reject if timestamp is the median time of the last 11 blocks or before
14. For certain old blocks (i.e. on initial block download) check that hash matches known values
15. Add block into the tree. There are three cases: 1. block further extends the main branch; 2. blo make it become the new main branch; 3. block extends a side branch and makes it the new m
16. For case 1, adding to main branch:
 1. For all but the coinbase transaction, apply the following:

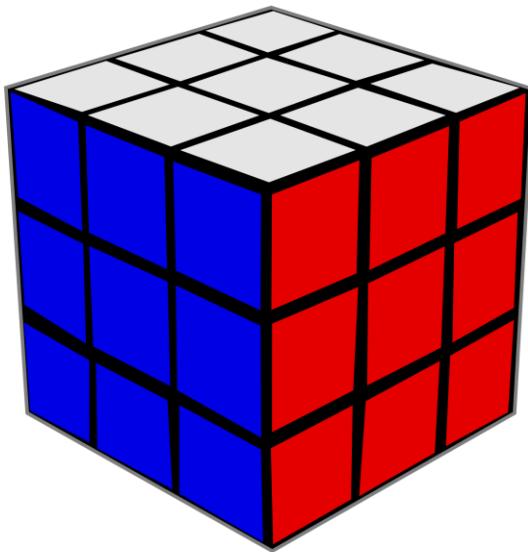
Consensus Protocol

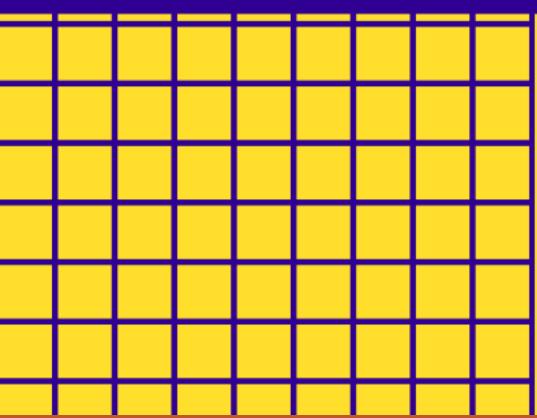
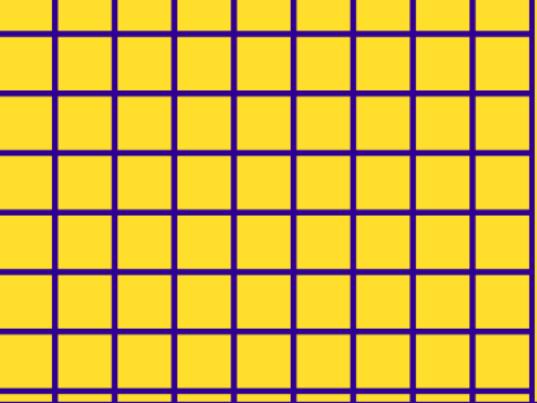


Consensus Protocol

Q)Is this verification and validation a time taking process ?

Consensus Protocol





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

A complex, abstract digital graphic on the left side of the slide. It features a grid of blue and white squares, similar to a binary matrix. Overlaid on this grid are several concentric, semi-transparent circles in shades of blue and grey. One prominent circle is light blue with white tick marks around its perimeter. Another circle is darker blue with a more intricate, segmented pattern. Small, white binary digits (0s and 1s) are scattered across the entire graphic, appearing both within the grid and along the edges of the circles.

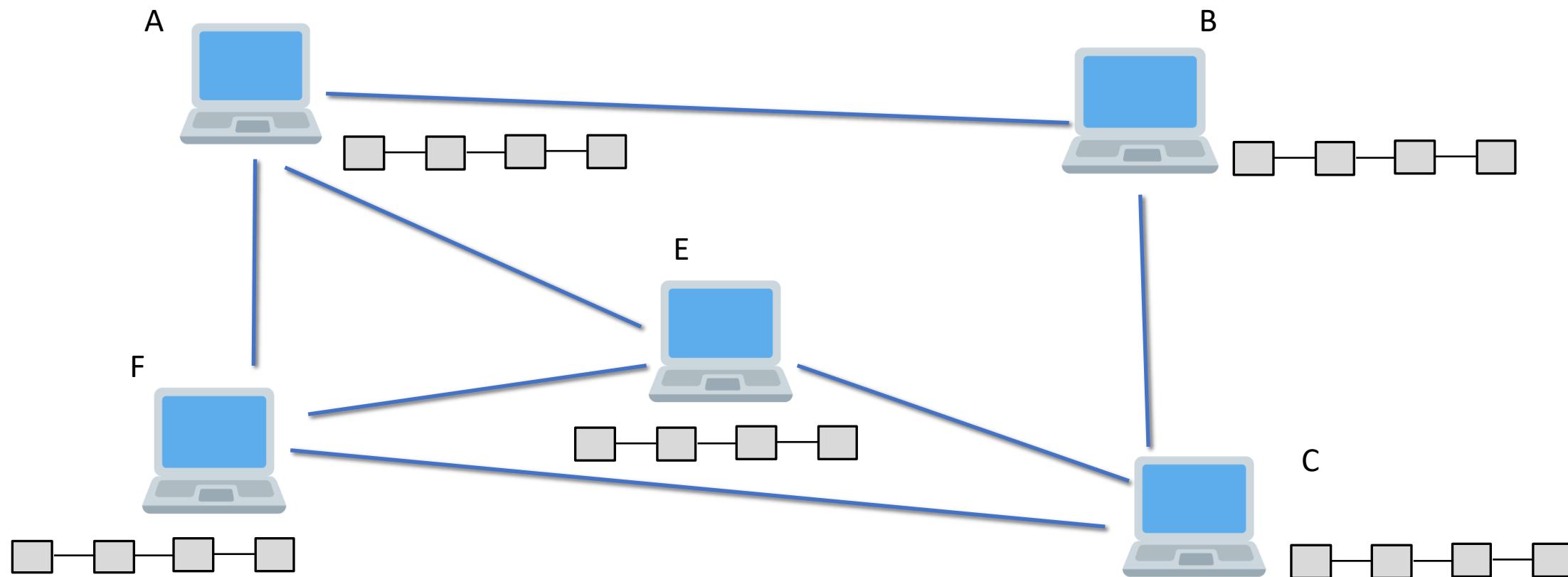
Consensus Protocol

Consensus Protocol

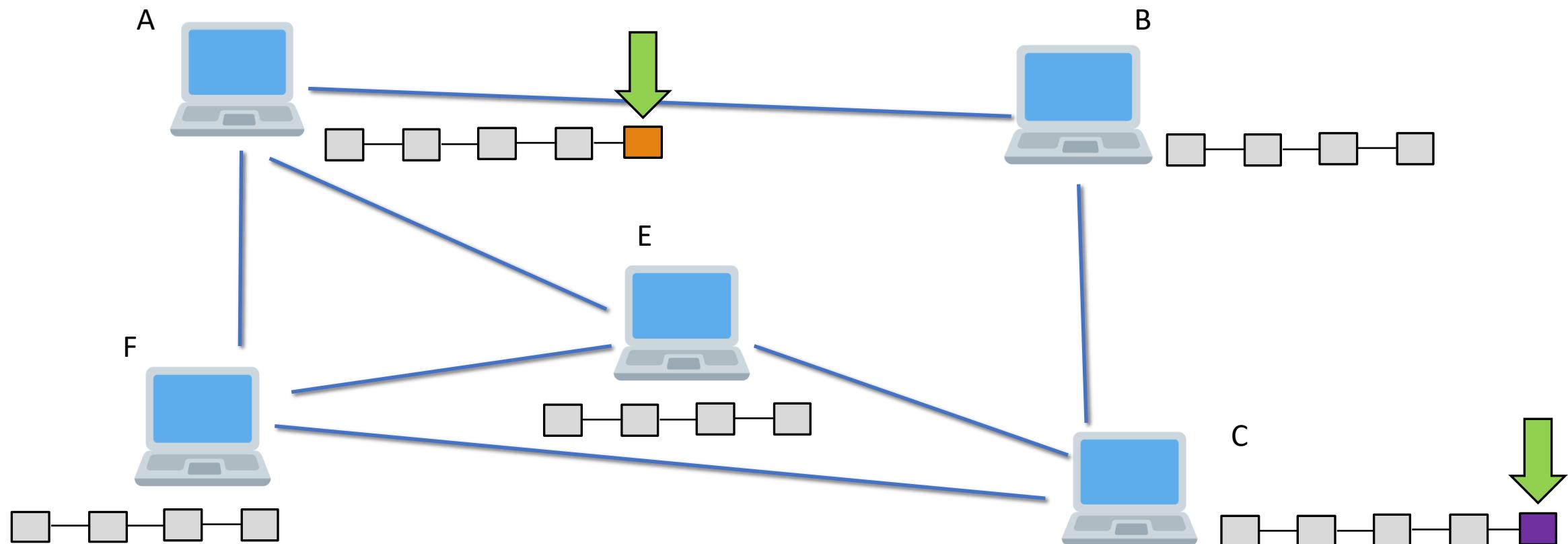
Prevent Attacks

Competing Chain Problem

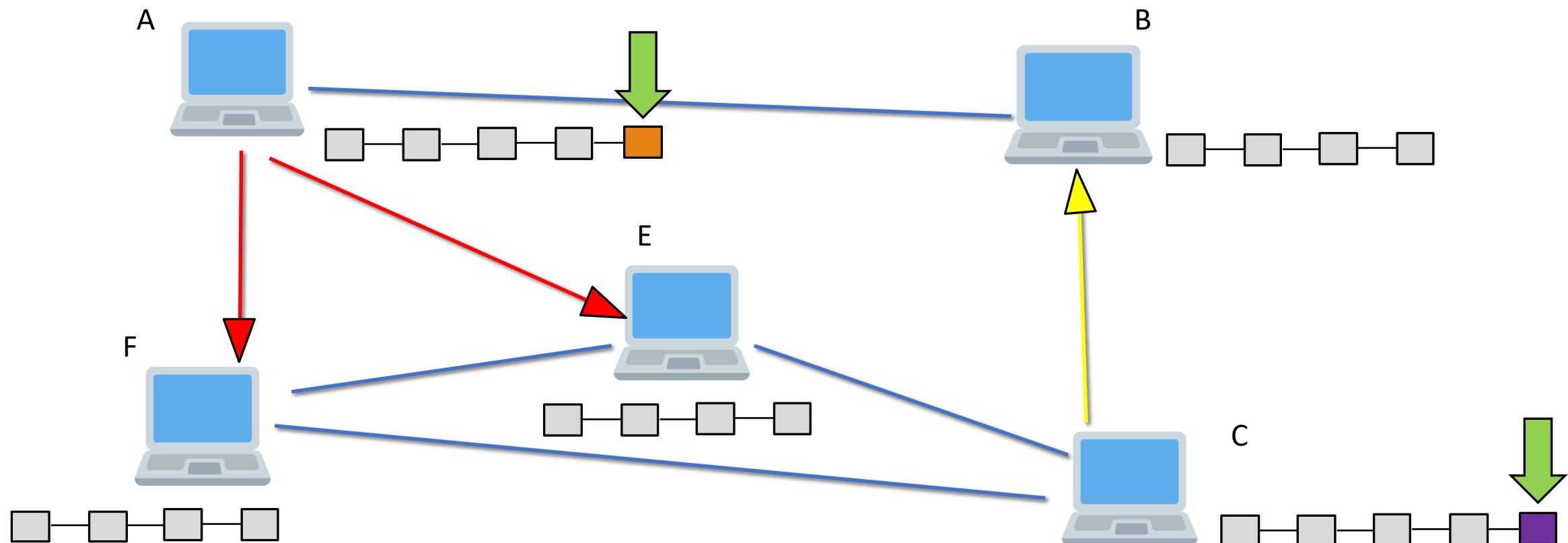
Consensus Protocol



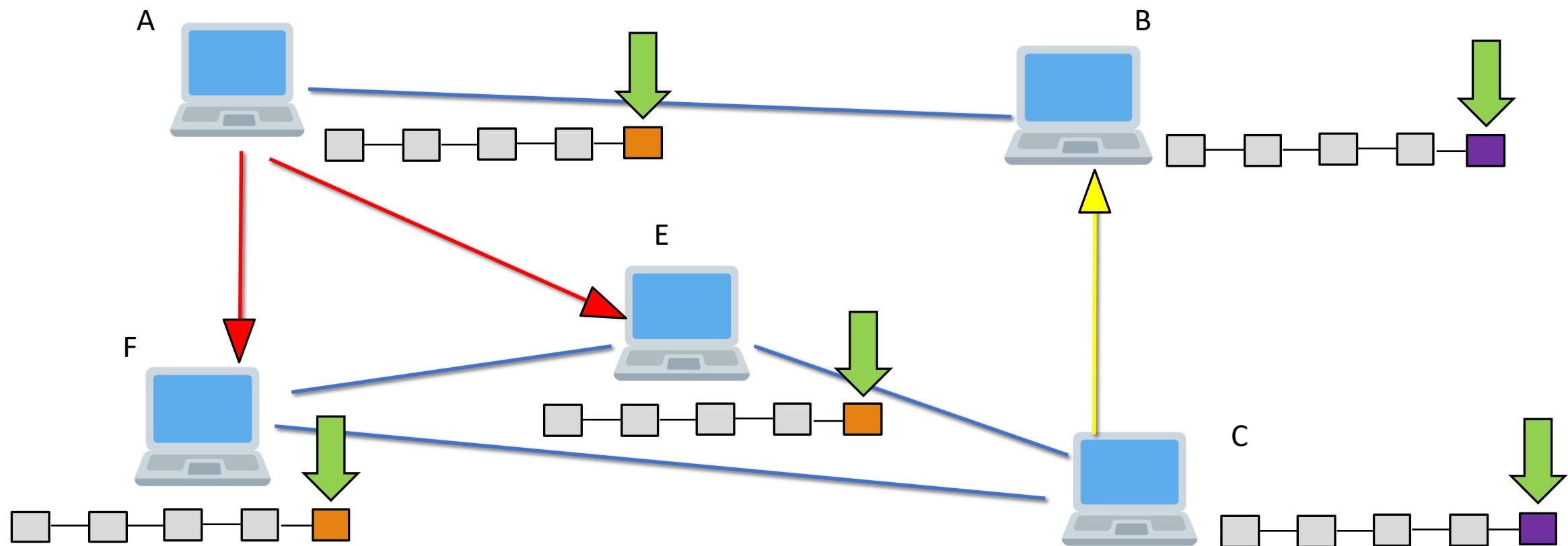
Consensus Protocol



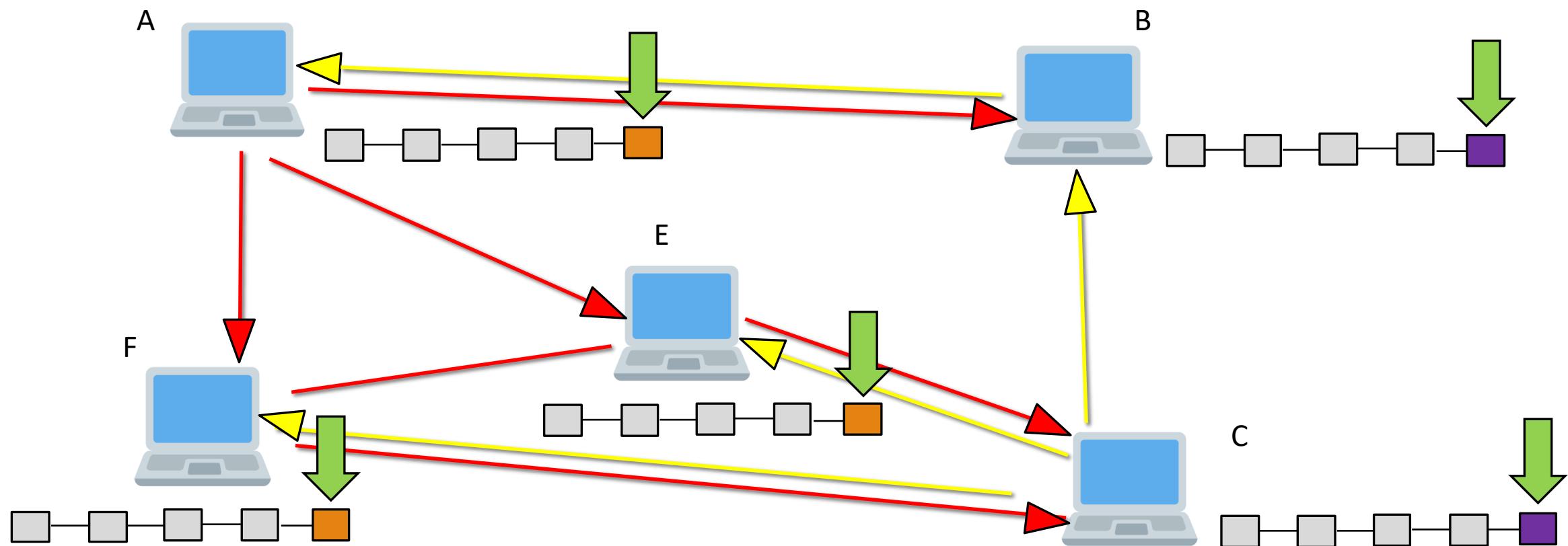
Consensus Protocol



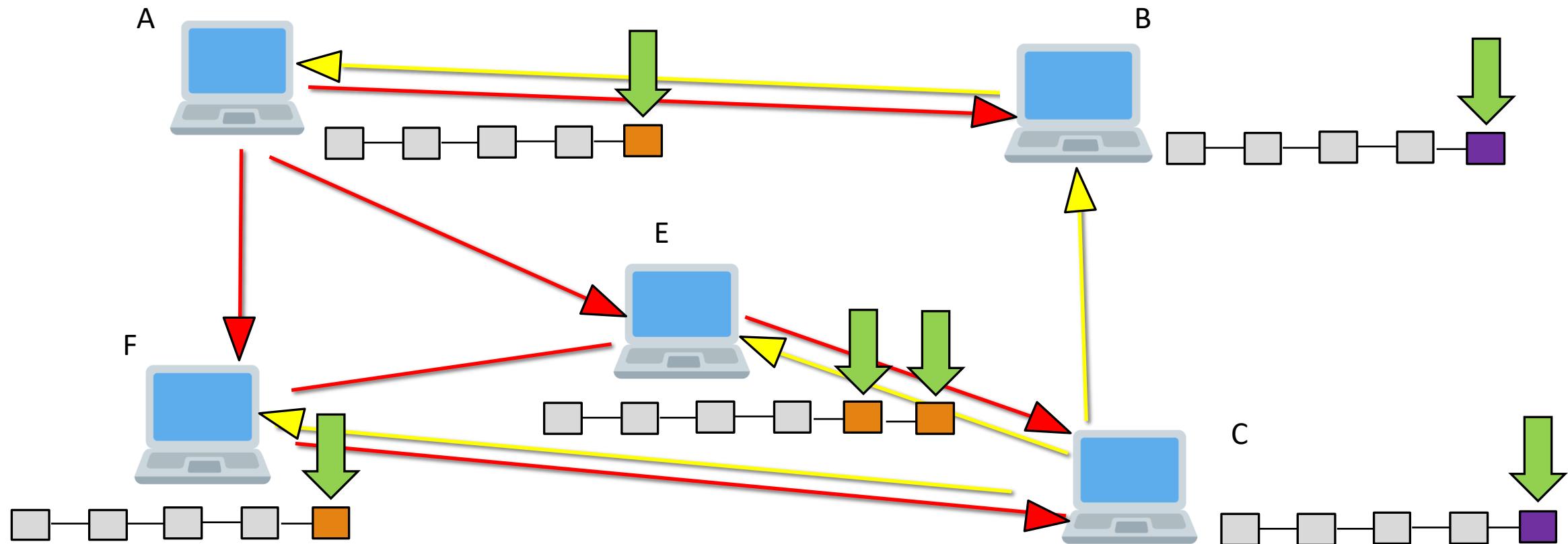
Consensus Protocol



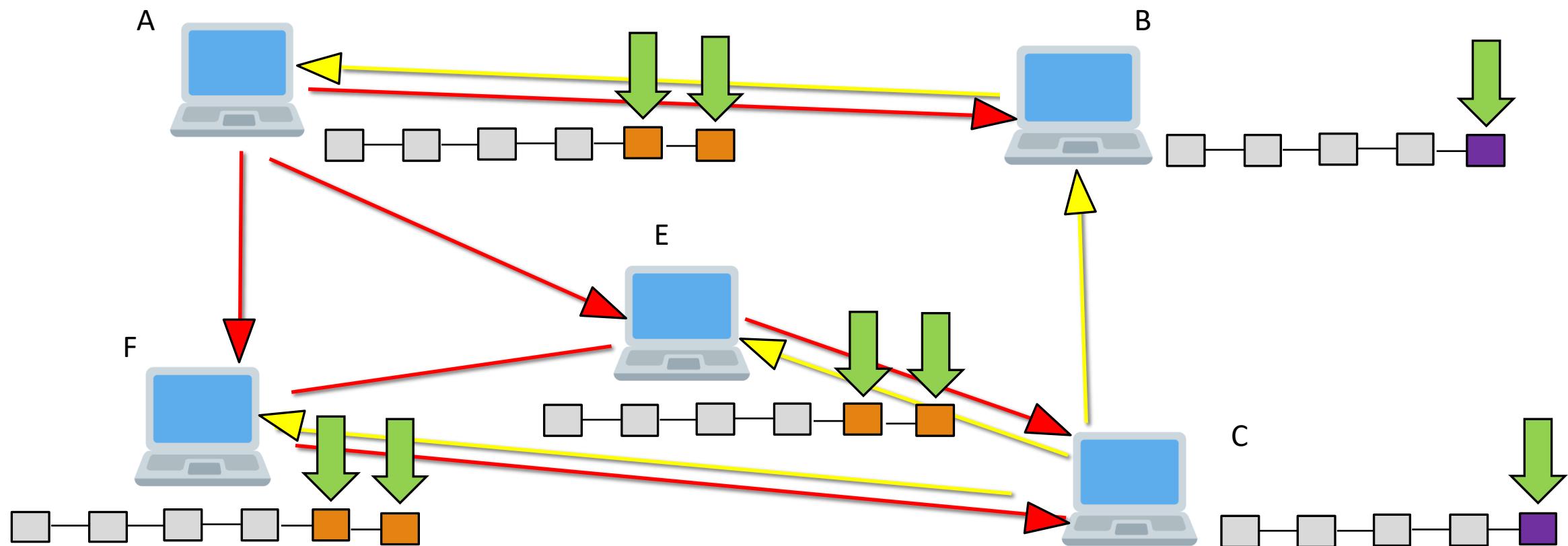
Consensus Protocol



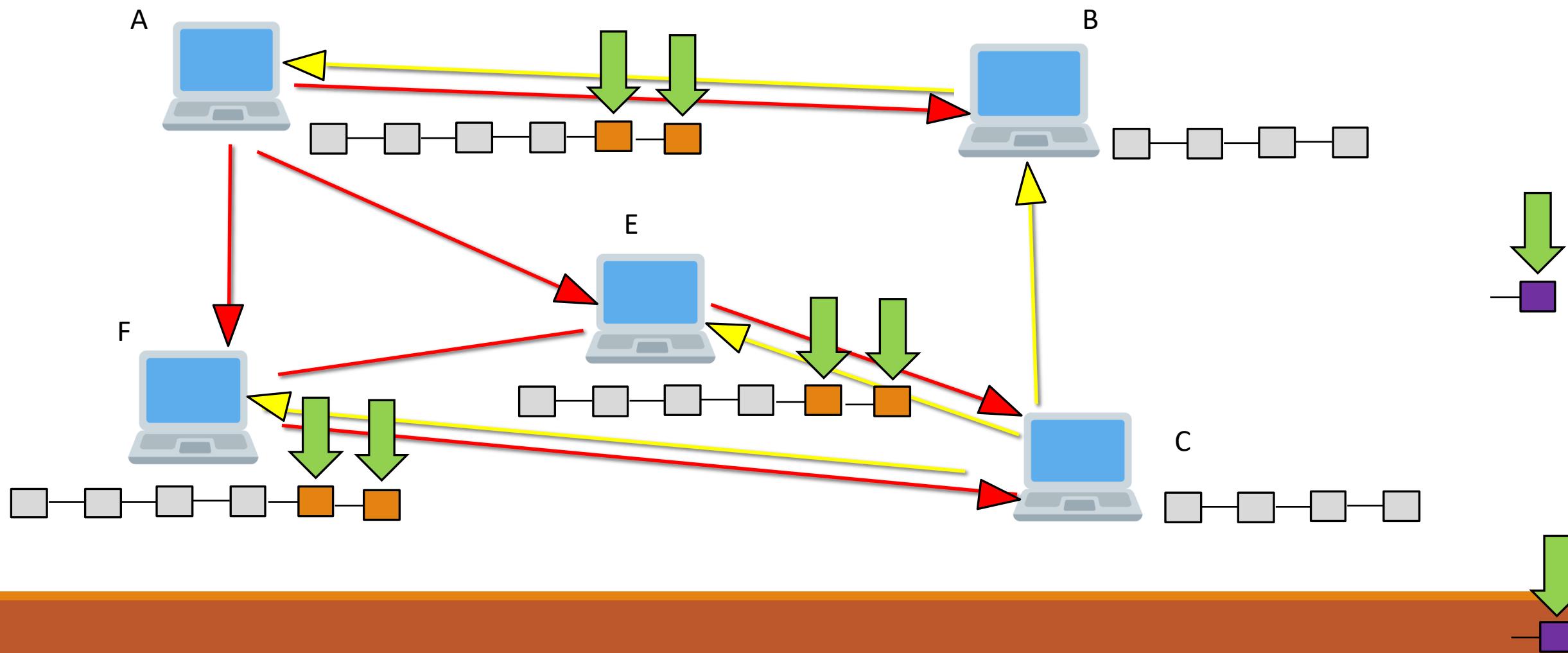
Consensus Protocol



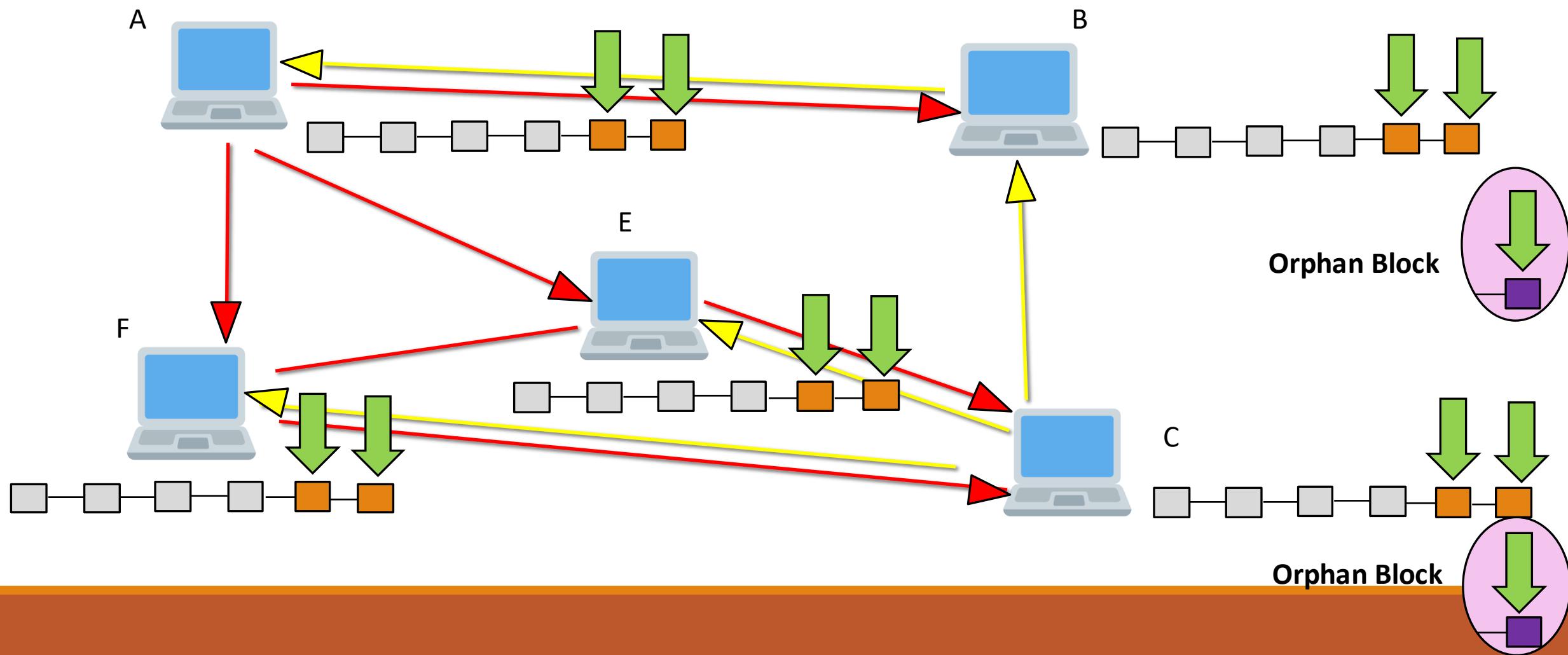
Consensus Protocol



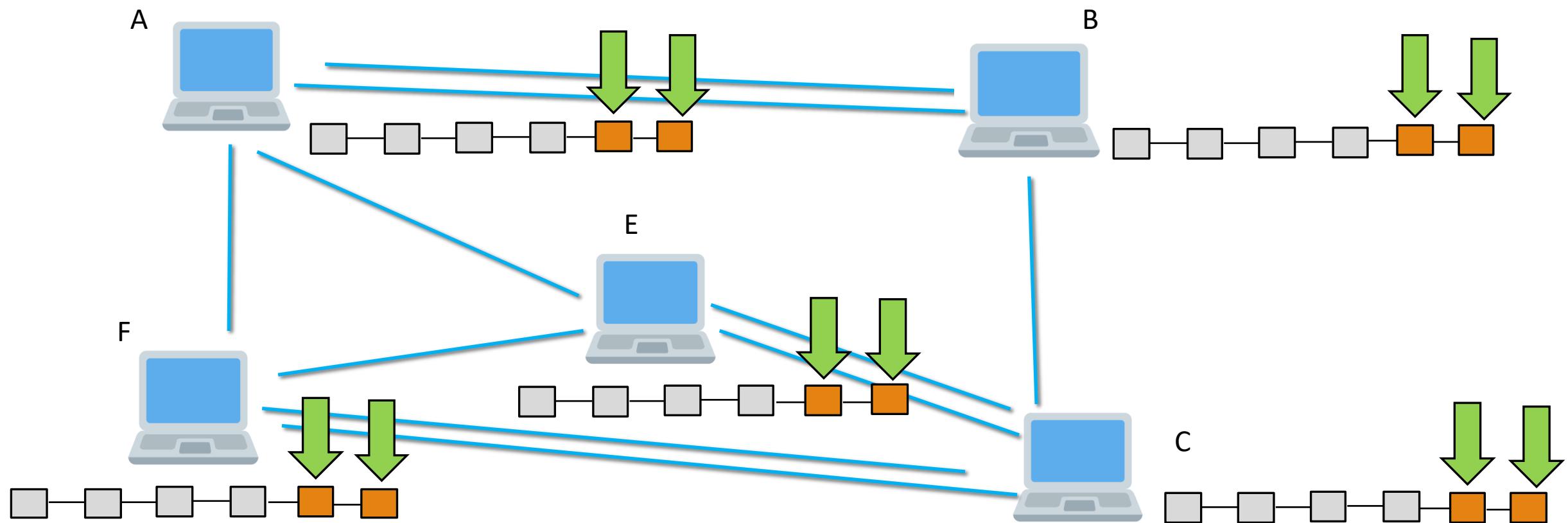
Consensus Protocol



Consensus Protocol



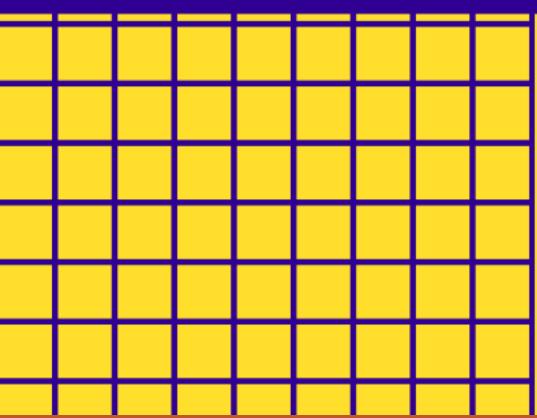
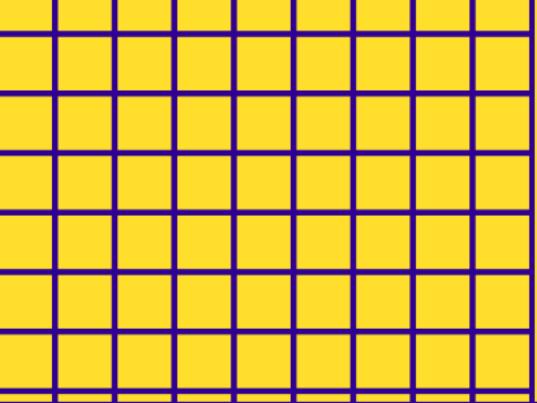
Consensus Protocol



Consensus Protocol

Note-

- The Consensus Protocol of Blockchain is much better than the Byzantine Fault Tolerance as Consensus Protocol only needs a **51%** majority while Byzantine Fault Tolerance needs **approximately 66%**.
- All the transaction in the **Orphan Block** will be dropped and the miner that had mined the block will not get any reward.
- So that's why wait for the **6 confirmations** before assuming payment to be successful.



Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Contents – Module B

What is Bitcoin?

Nonce

Transactions

Bitcoin's Monetary Policy

CPU's vs GPU's vs ASICS

Wallets

Mining

Mempool

Public Key and Private Key



Cryptocurrency

History Of Bitcoin

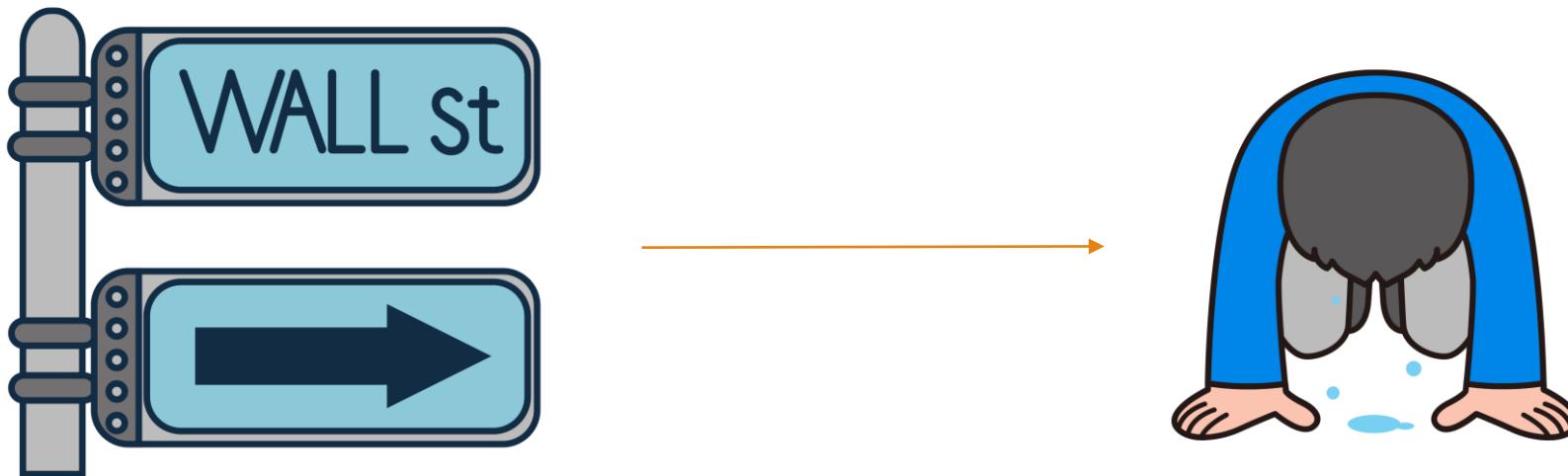


US Economy

Nearly 9 million – Lost Job

Nearly 1.8 million – Small business closed

History Of Bitcoin



History Of Bitcoin

Lehman Brothers



HISTORY OF BITCOIN



History Of Bitcoin

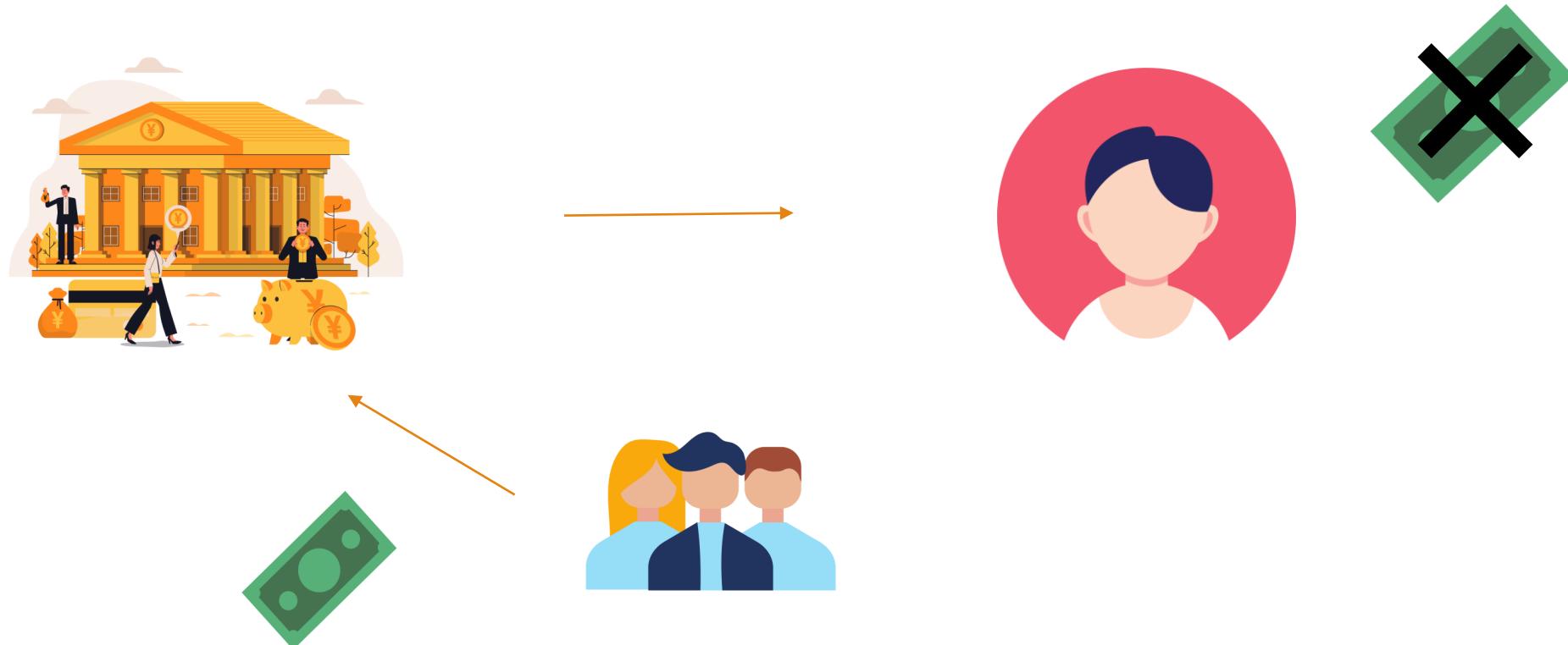


Foolishness of Banks



US Government

History Of Bitcoin



History Of Bitcoin



Foolishness of Banks

US Government

History Of Bitcoin



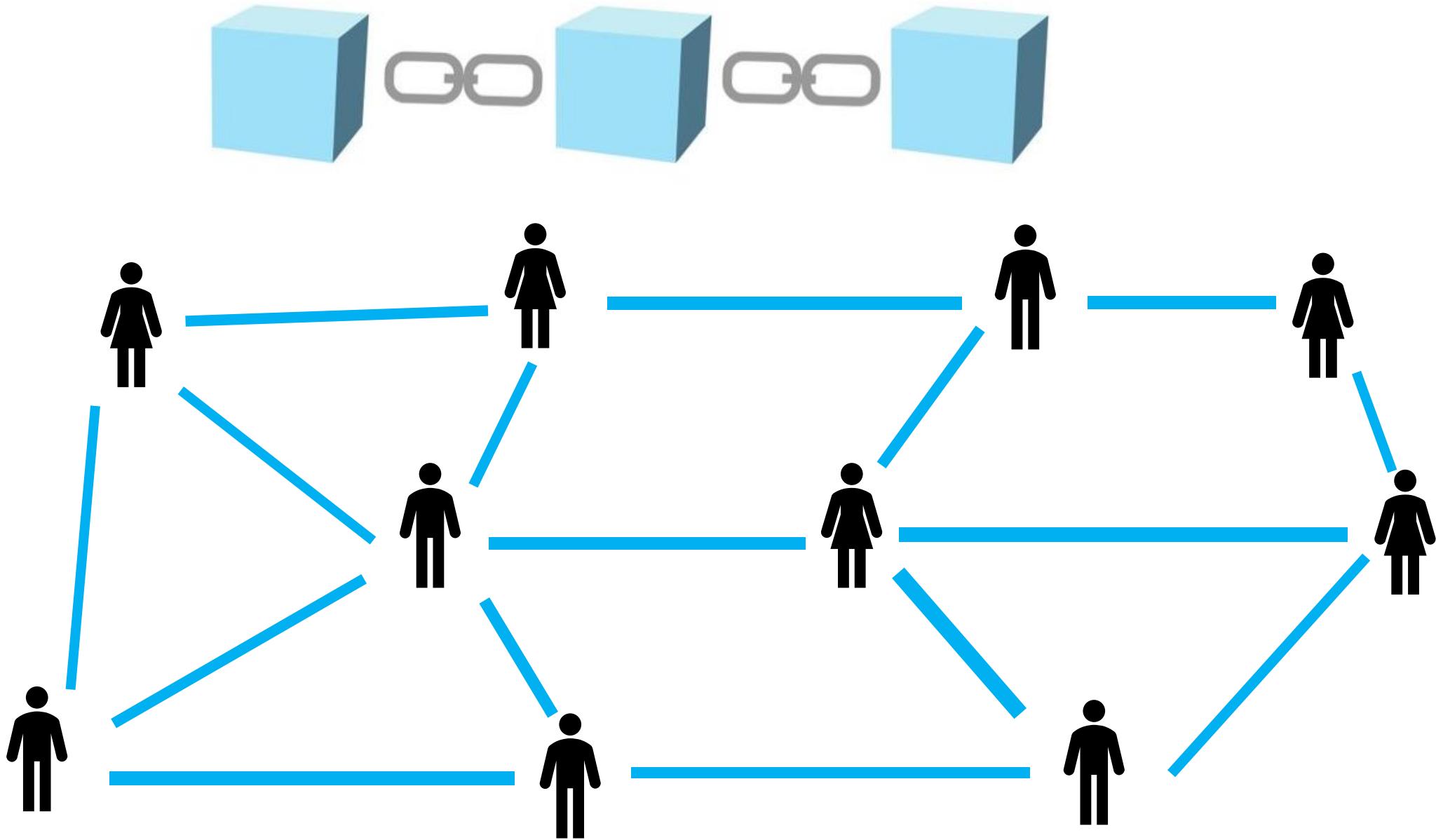
Bitcoin



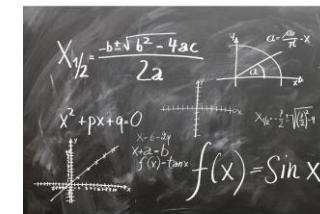
Satoshi Nakamoto

Bitcoin

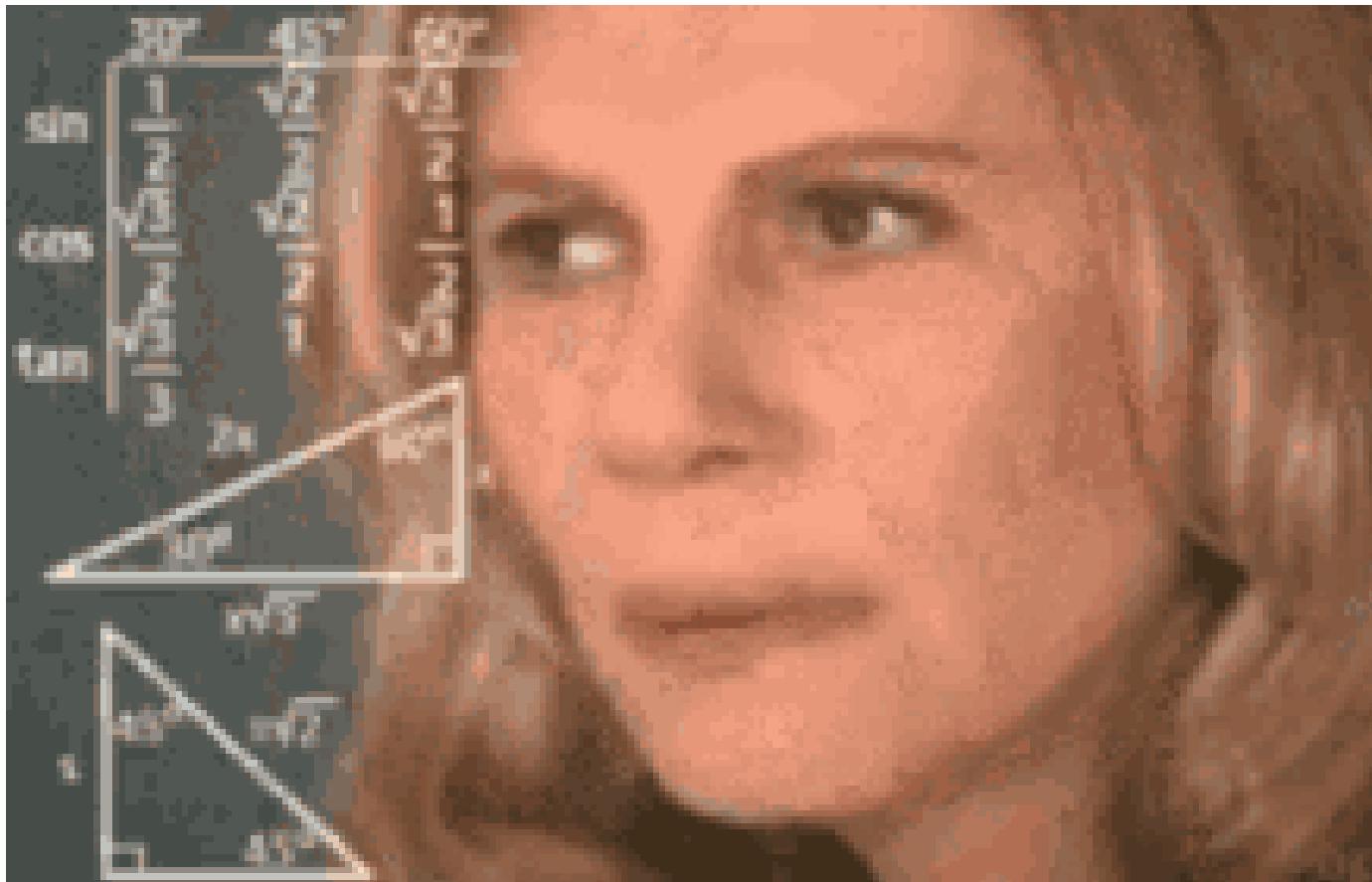
- Bitcoin is a decentralized **digital currency**, without a central bank or **single administrator**, that can be sent from user to user on the peer-to-peer bitcoin network without the need for **intermediaries**.
- It uses Blockchain Technology.



Trust



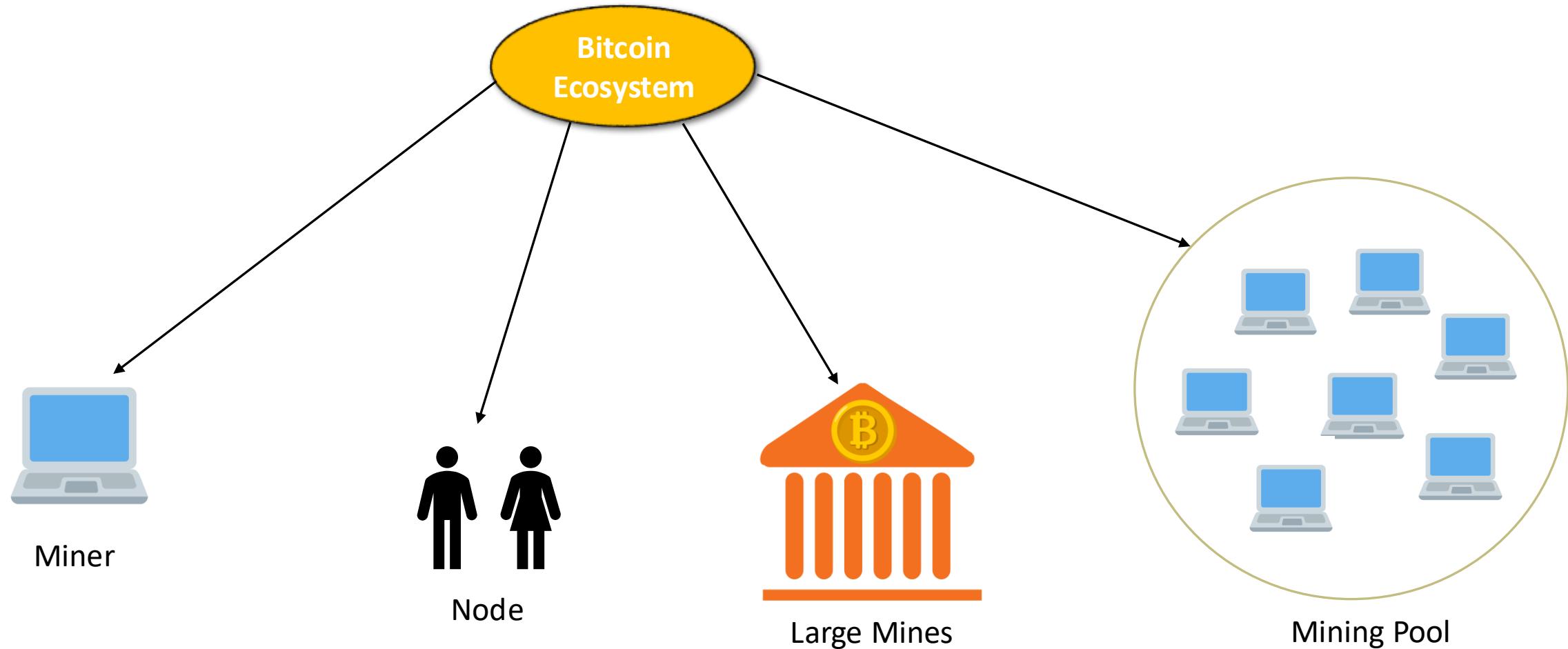
Mathematical Problem

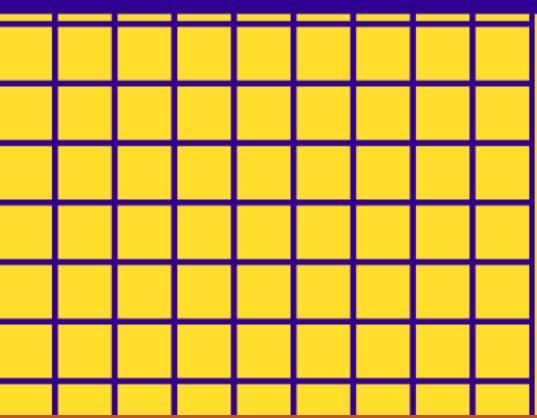
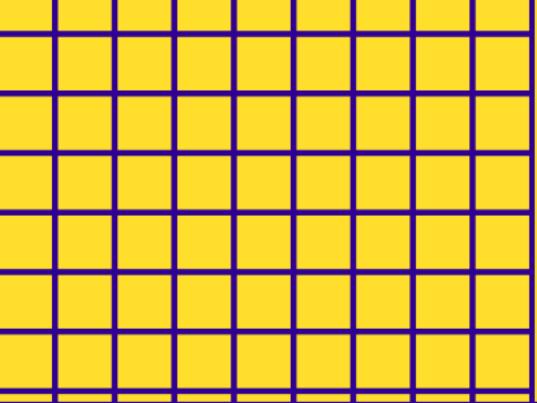




The Big Short

Bitcoin Ecosystem





Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

Blockchain vs Coin

Technology

Blockchain

Protocol/Coin

Waves

Bitcoin

Ethereum

Blockchain vs Coin vs Token

Technology

Blockchain

Protocol/Coin

Waves

Bitcoin

Ethereum

Token

WGB	BI
INTL	WGR



TRX	SNT
REP	AE

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



A complex, abstract digital background composed of a grid of blue and white squares. Overlaid on this grid are several concentric, semi-transparent circles in shades of blue and cyan. The circles appear to be rotating or pulsating. Interspersed throughout the grid and around the circles are numerous binary digits (0s and 1s), some of which are larger and more prominent than others, creating a sense of digital data flow and computation.

Bitcoin's Monetary Policy

Bitcoin's Monetary Policy

The Halving

Block Frequency

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	11 May 2020	650'000	6.25 new XBT
3rd halving	Expected 2024	740'000	3.125 new XBT
4th halving	Expected 2028	850'000	1.5625 new XBT
Maximum supply reached	Expected 2140	6'930'000	0 new XBT

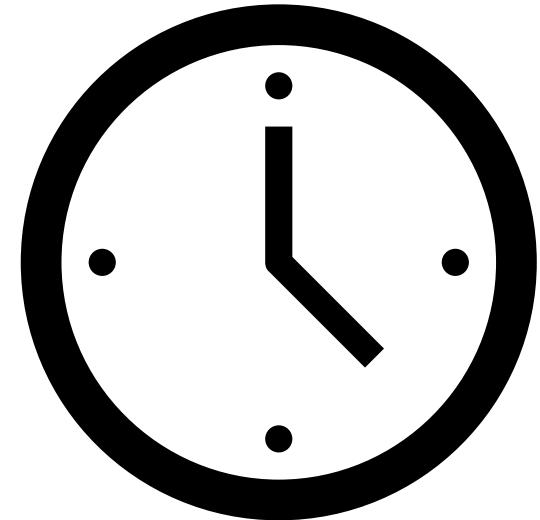
Note- Supply cap of Bitcoin is 21 million.

The Halving



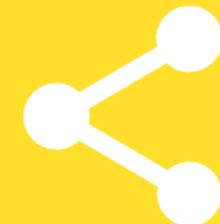
Block Frequency

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



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





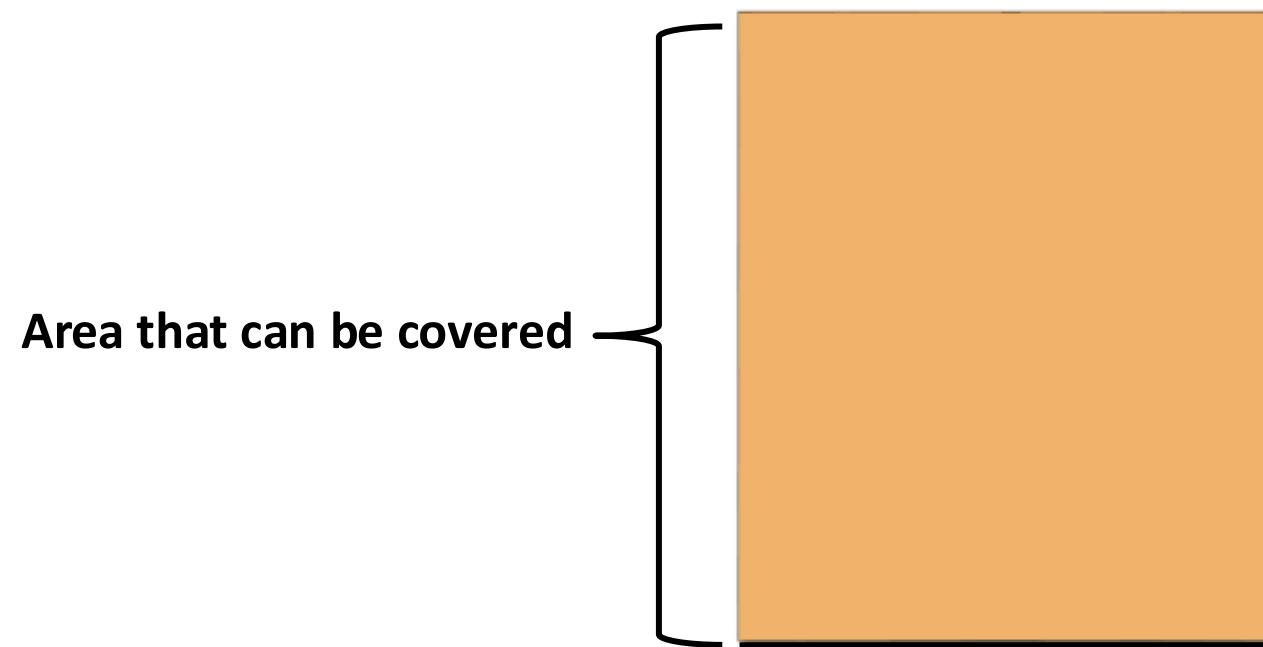
Bitcoin's Target History

A complex, abstract digital background composed of a grid of blue and white squares. Overlaid on this grid are several concentric, semi-transparent circles in shades of blue and cyan. The circles appear to be rotating or pulsating. Interspersed throughout the grid and around the circles are numerous binary digits (0s and 1s), some of which are larger and more prominent than others, creating a sense of digital data flow and computation.

Bitcoin's Monetary Policy

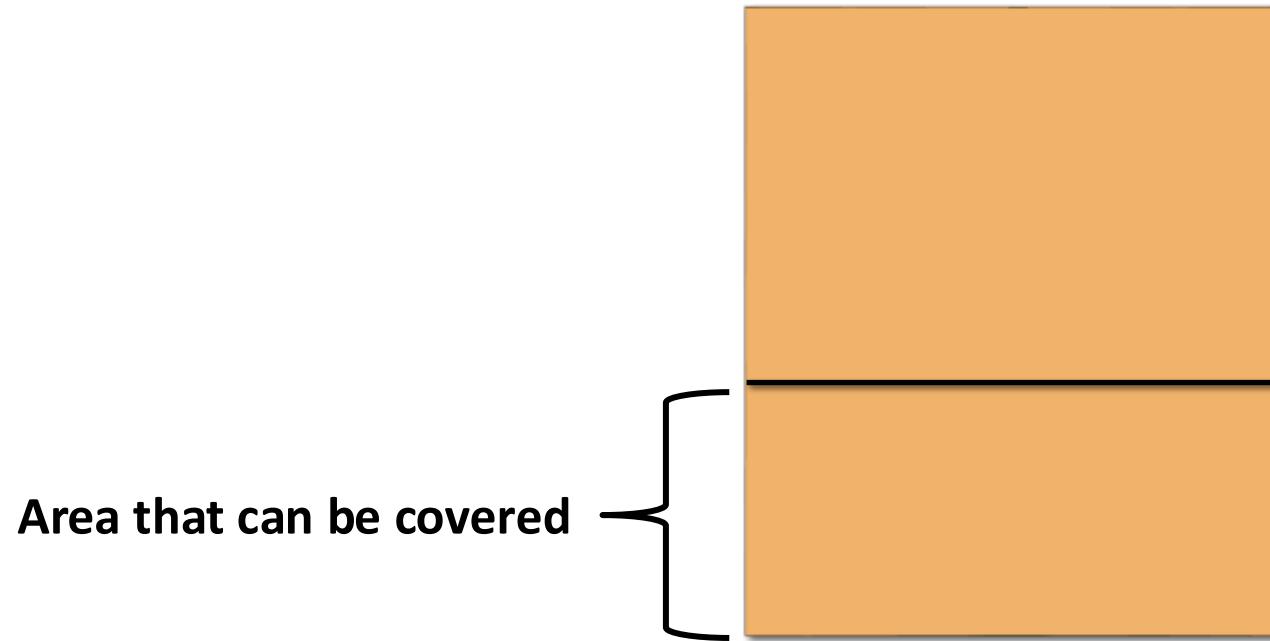
Understanding Mining Difficulty

Let's take a five digit number= XXXXX



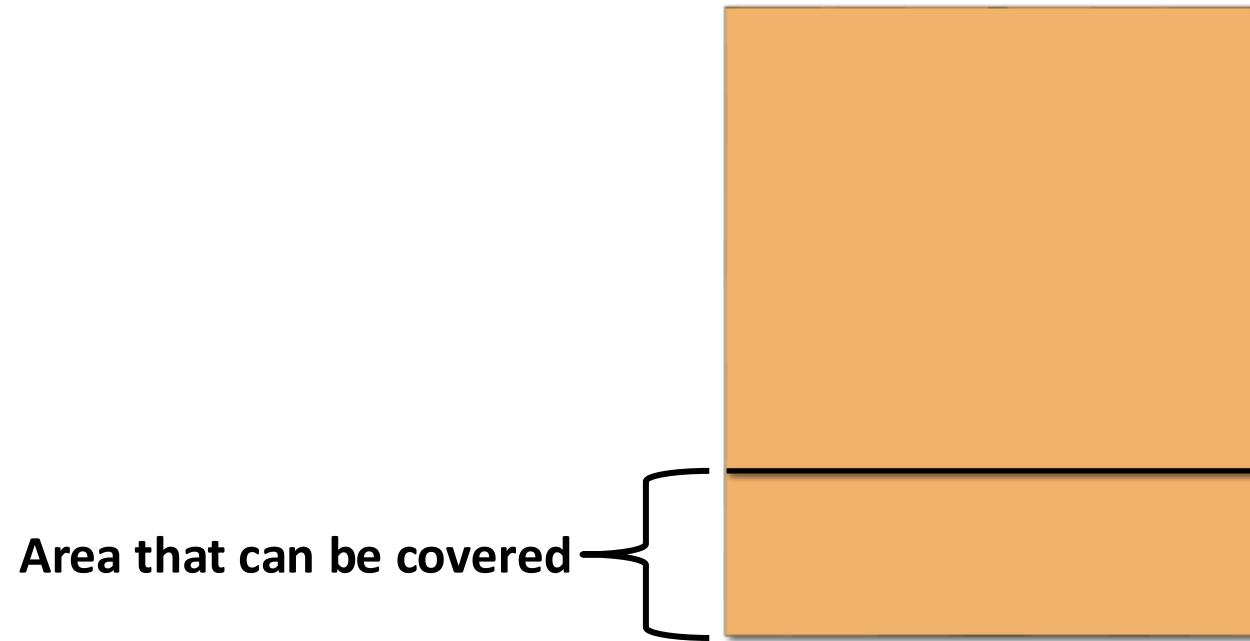
Understanding Mining Difficulty

Let's take a five digit number= **0XXXX**



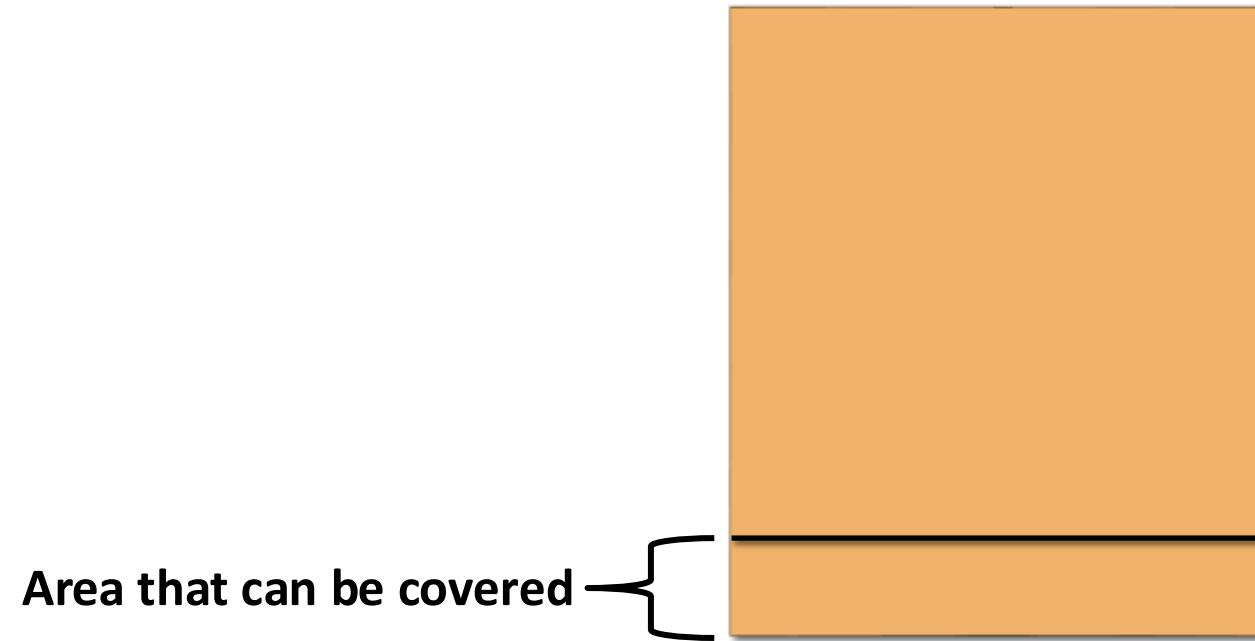
Understanding Mining Difficulty

Let's take a five digit number= **00XXX**



Understanding Mining Difficulty

Let's take a five digit number= **000XX**



Understanding Mining Difficulty

Current Target:

19 leading 0's

Understanding Mining Difficulty

Total Possible 64-digits hexadecimal numbers = $16^{64} \simeq 10^{77}$

Total valid hashed(with 19 leading 0's) = $16^{(64-19)} \simeq 10^{54}$

Probability that a randomly picked hash is valid = $(10^{54}/10^{77}) \simeq 10^{-23}$

Understanding Mining Difficulty

Q) Who adjusts the difficulty ?

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases. – [Satoshi Nakamoto](#)

**GIVE THIS VIDEO
A THUMBS-UP !**

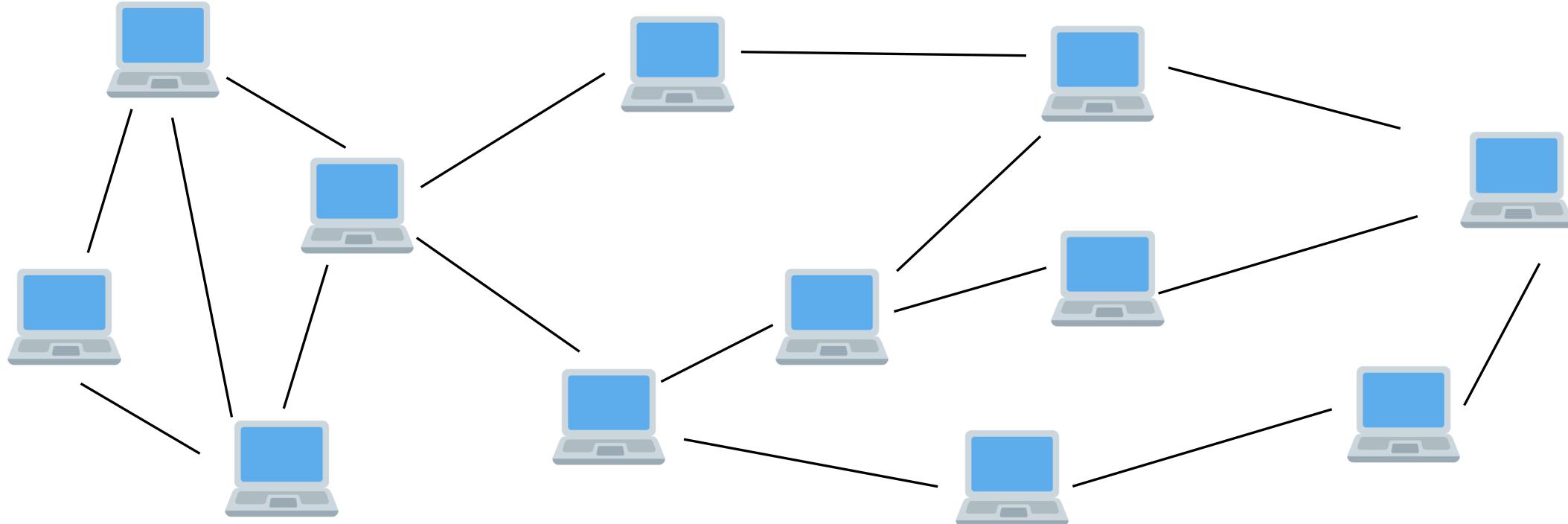
CODE EATER



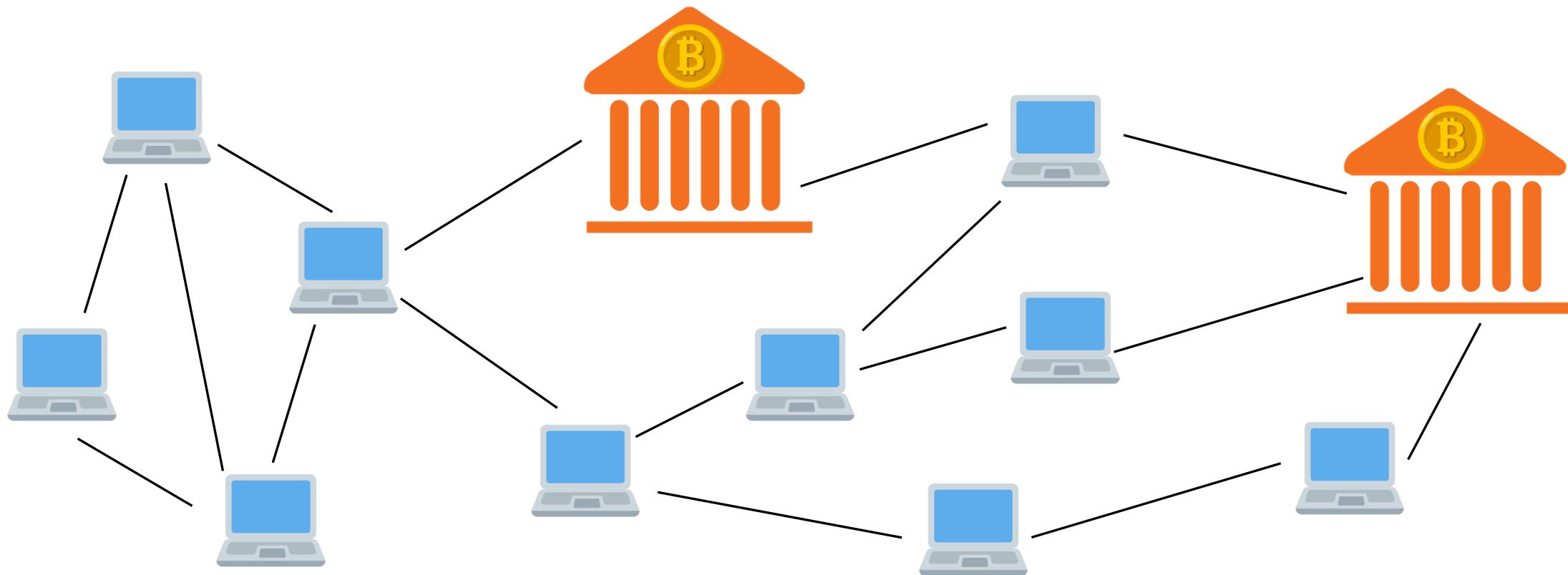


Mining Pool

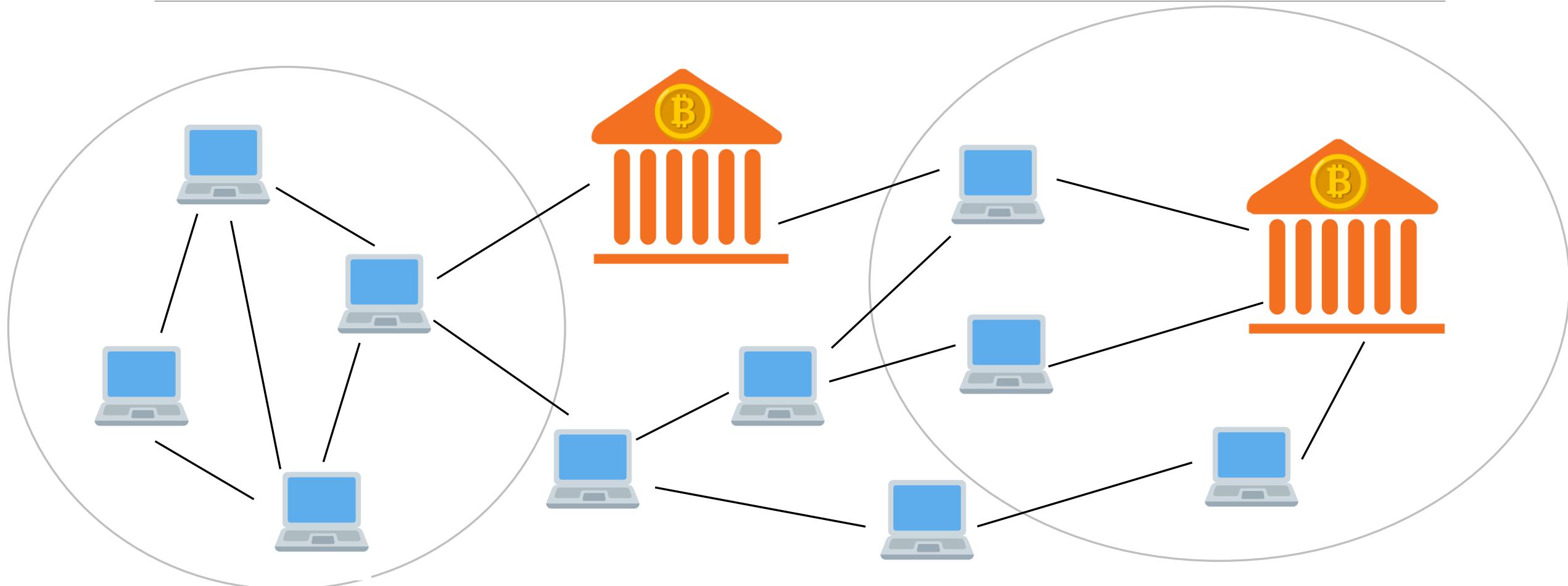
Mining Pools



Mining Pools



Mining Pools

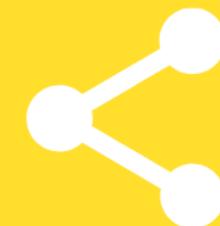


Mining Pools Benefits

- You don't have to buy costly equipment's.
- You don't have to worry about mining setup.
- Distribution of rewards according to the mining power.
- No wastage of power.

**GIVE THIS VIDEO
A THUMBS-UP !**

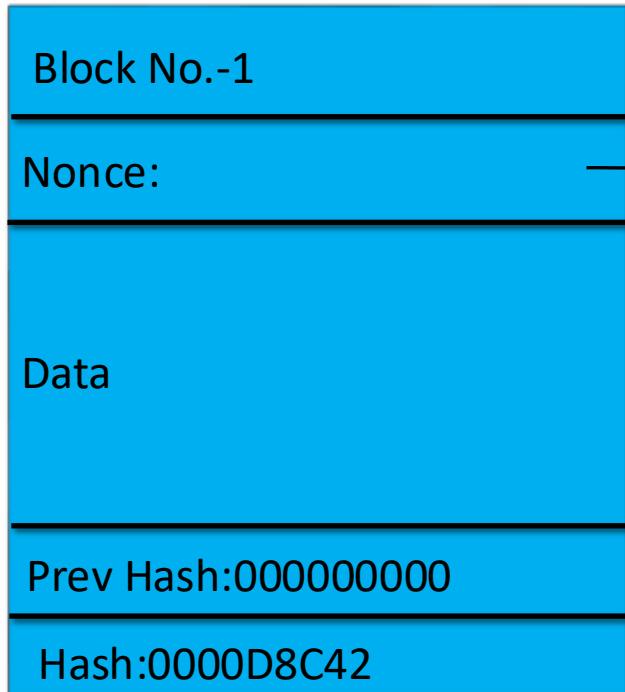
CODE EATER



A complex, abstract digital graphic on the left side of the slide. It features a central circular element with concentric rings and a grid pattern. Overlaid on this are numerous binary digits (0s and 1s) represented as small blue squares, some of which are highlighted in white. The overall color scheme is dark blue and black.

Nonce Range

Nonce Range



Nonce is a 32 bit number.

Range of Nonce = 0 to $2^{32} - 1 \simeq 0$ to 4×10^9

Nonce Range

SHA 256

XX

Total number of possible hashes = $16 \times 16 \times \dots \times 16 = 16^{64} \approx 10^{77}$

Nonce Range

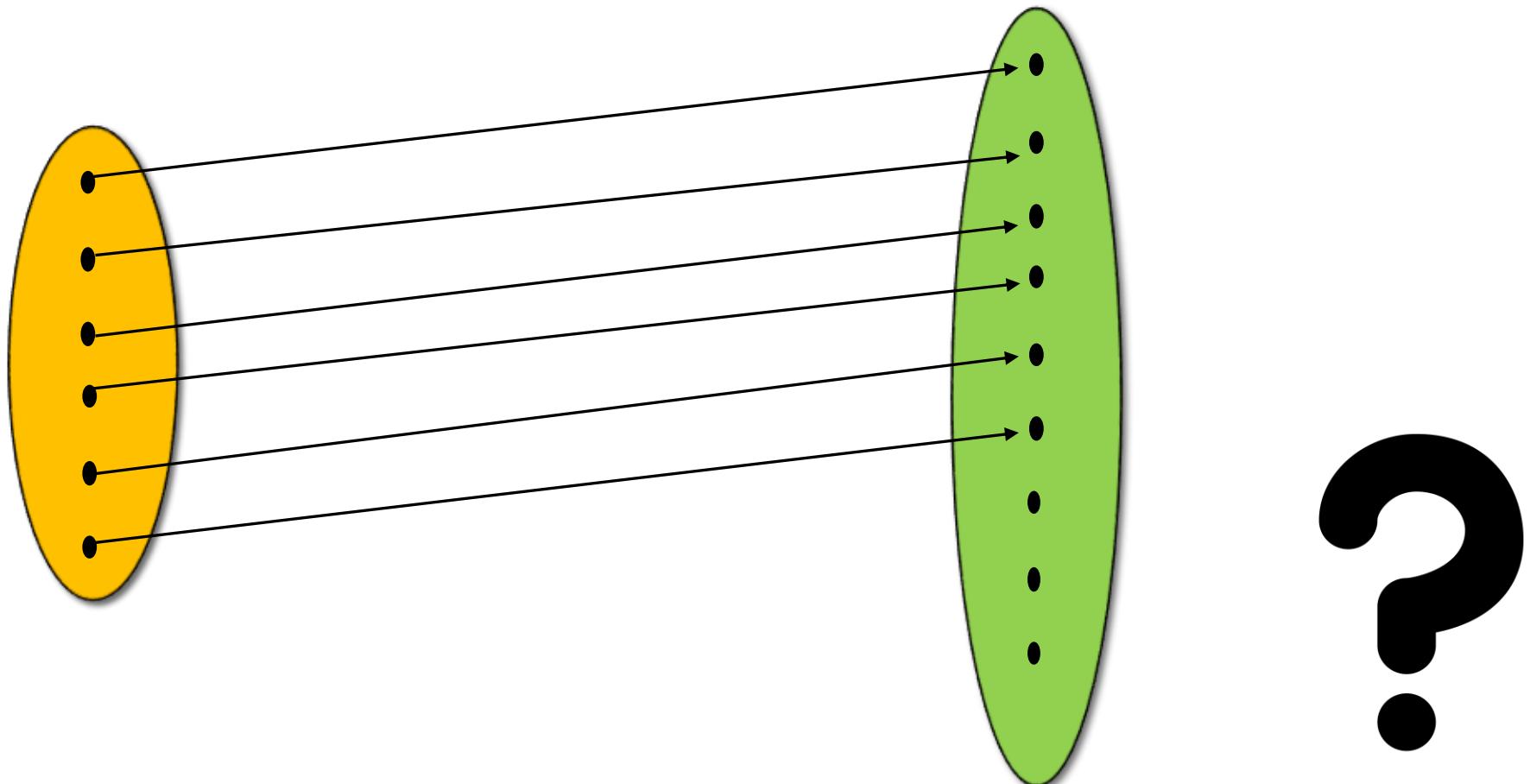
Total valid hashed $\simeq 10^{77}$

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

10⁷⁷ >>> 4 x10⁹

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

Nonce Range



Nonce Range

A modest mines does 10^8 hashes/sec.

4×10^9 nonce will be covered in = $(4 \times 10^9)/(10^8) = 40$ seconds.

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

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



The background of the slide features a complex, abstract design in shades of blue. It consists of several concentric, semi-transparent circles that overlap each other. Between these circles are various horizontal and vertical lines, creating a grid-like pattern. Scattered throughout this grid are numerous binary digits (0s and 1s), which appear to be floating or part of a larger digital matrix. The overall effect is one of a high-tech, digital environment.

Timestamp

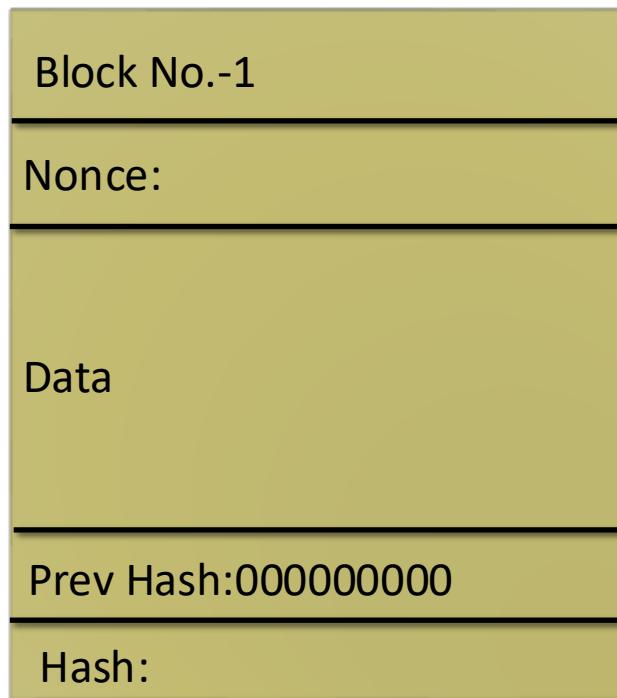
Recap of Nonce Range

A modest mines does 10^8 hashes/sec.

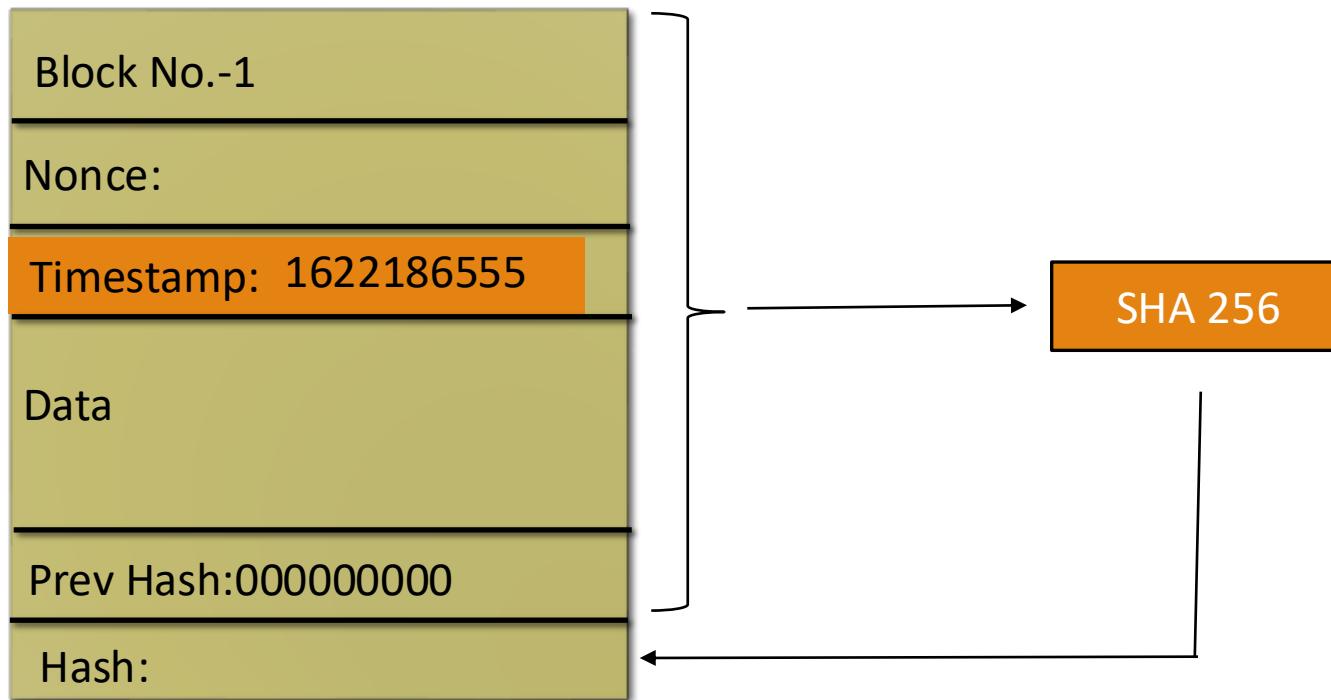
4×10^9 nonce will be covered in = $(4 \times 10^9)/(10^8) = 40$ seconds.

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

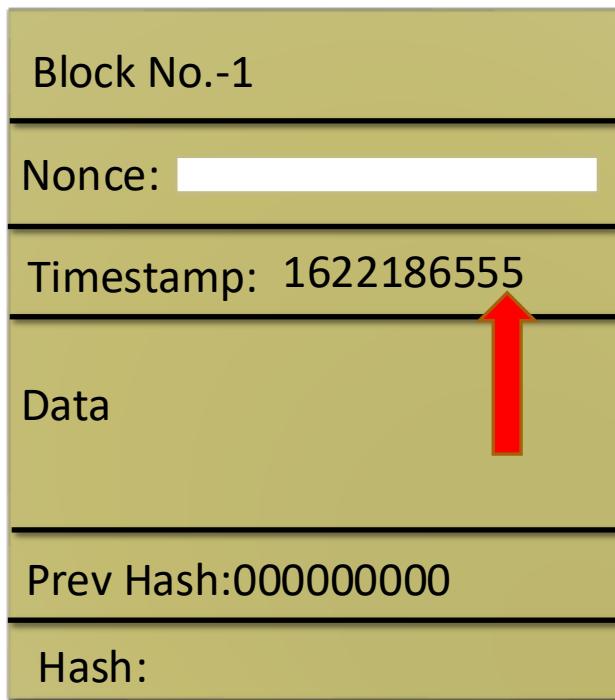
Timestamp



Timestamp



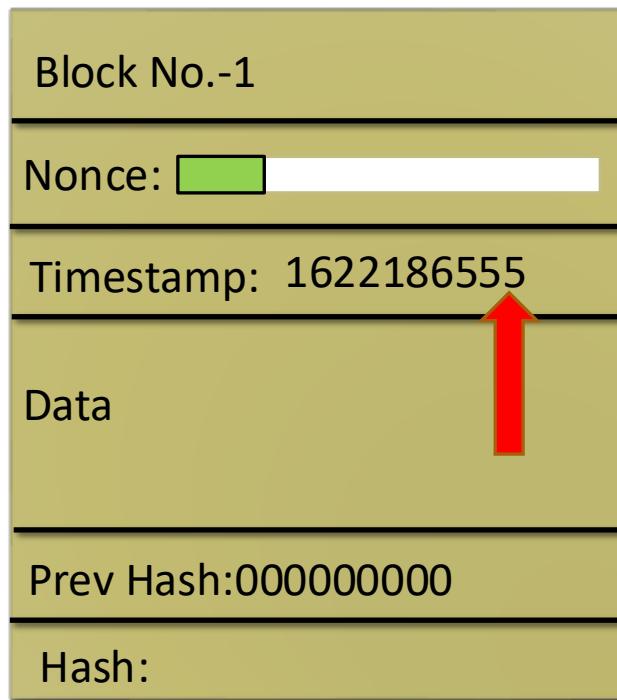
Timestamp



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

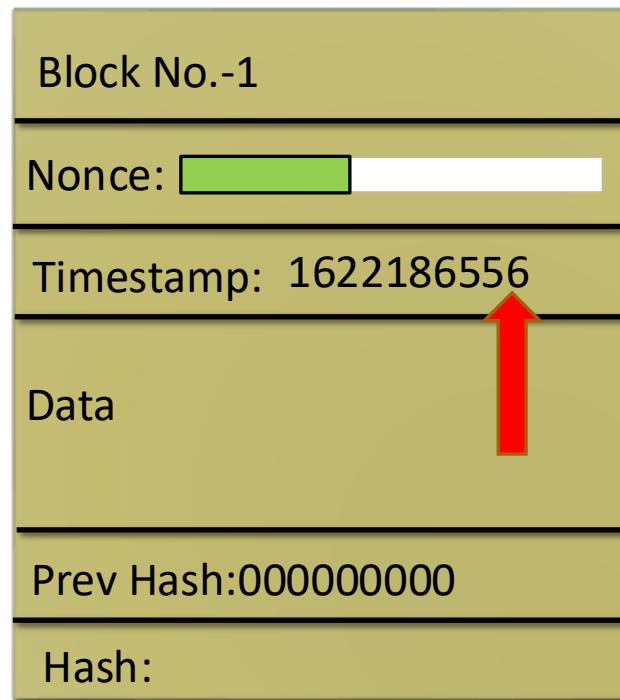
A miner will exhaust **0.1 Billion
nonce** in **1 sec.**

Timestamp

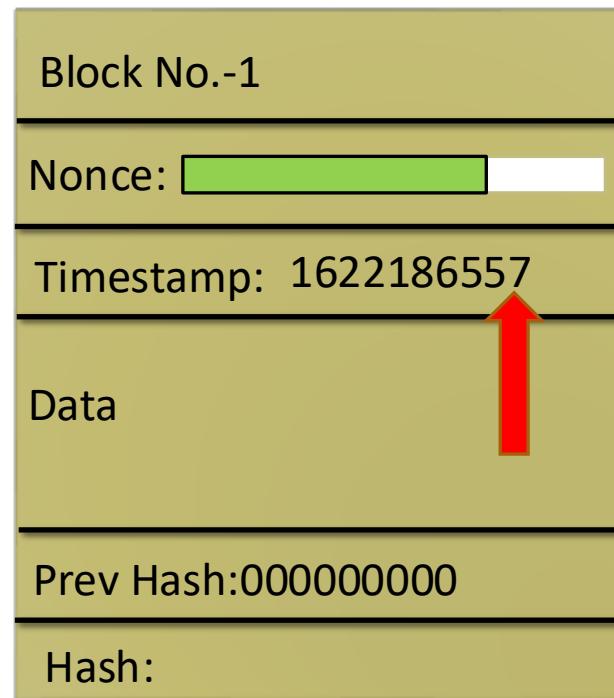


0.5 seconds

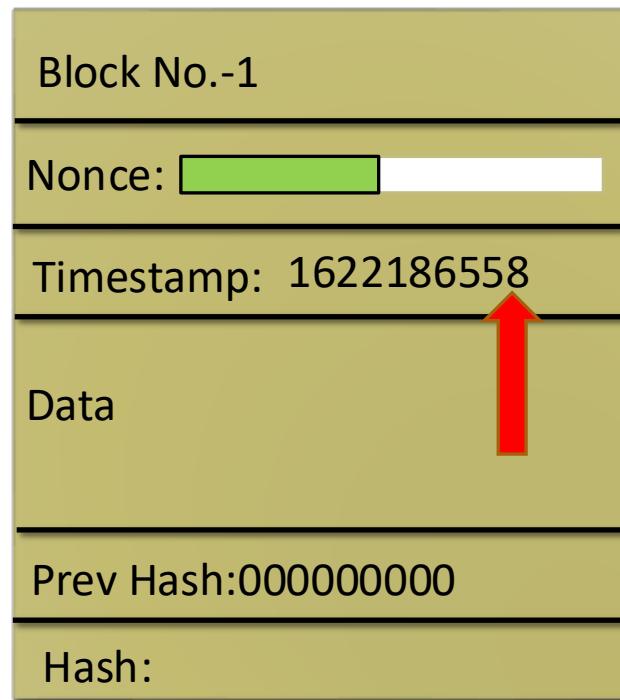
Timestamp



Timestamp



Timestamp



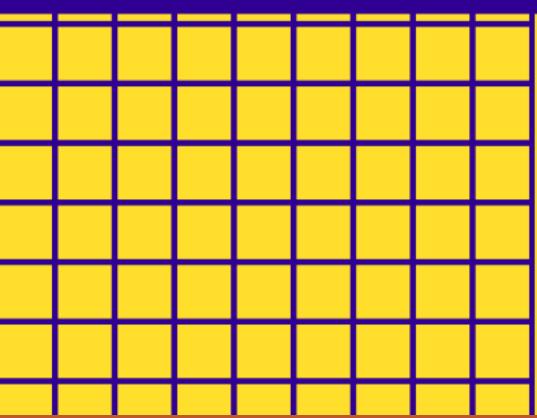
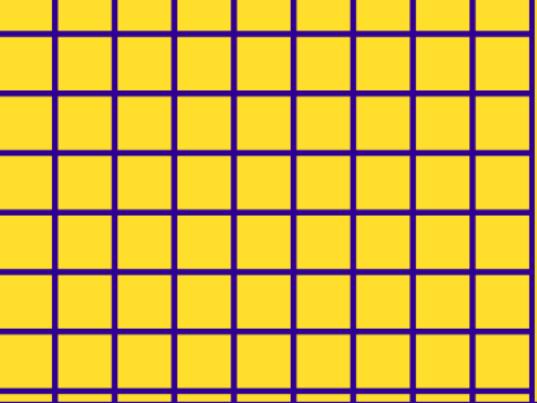
Timestamp

Current hashing rate is equal to **234 million trillion hashes/sec.**

4×10^9 nonce will be covered in = $(4 \times 10^9) / (10^6 \times 10^{12}) = 4 \times 10^{-9}$ seconds.

$4 \times 10^{-9} \text{ sec} <<< 1 \text{ sec}$

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



Instagram - @codeeater21

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Discord – Link in description

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





Mempool

Recap Timestamp...

Current hashing rate is equal to **234 million trillion hashes/sec.**

4×10^9 nonce will be covered in = $(4 \times 10^9) / (10^6 \times 10^{12}) = 4 \times 10^{-9}$ seconds.

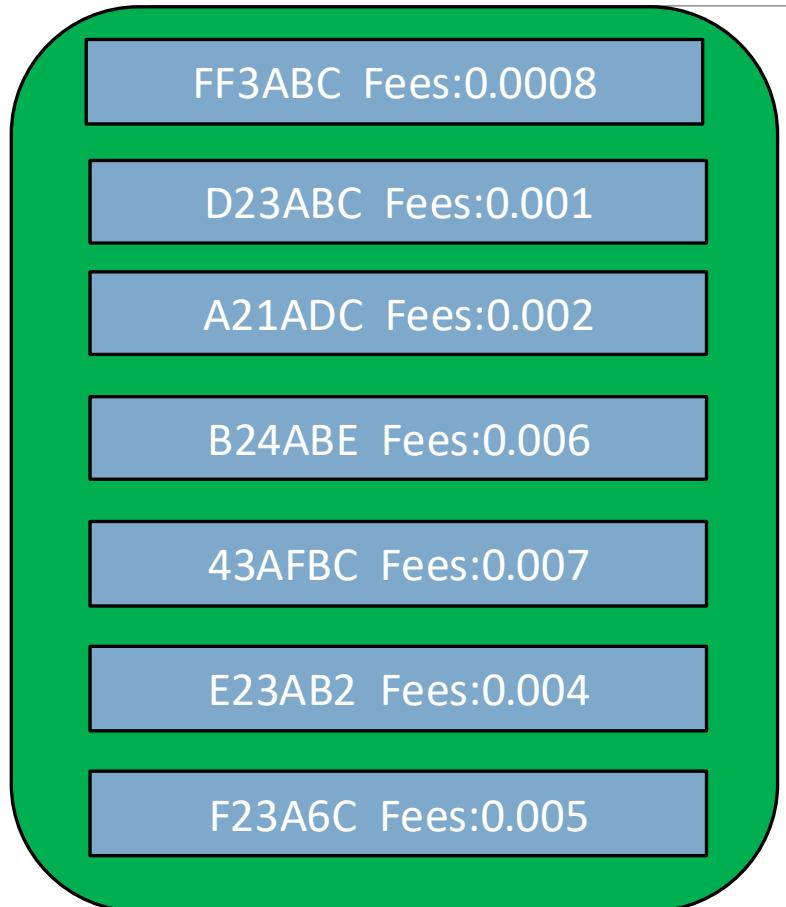
$4 \times 10^{-9} \text{ sec} <<< 1 \text{ sec}$

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

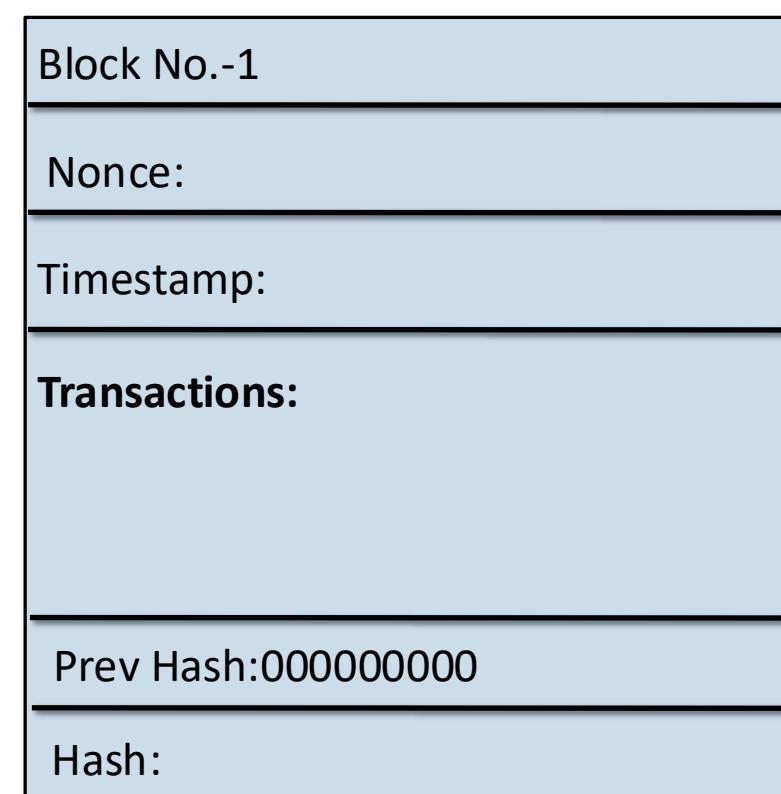
Mempool

Block No.-1
Nonce:
Timestamp:
Transactions:
Prev Hash:00000000
Hash:

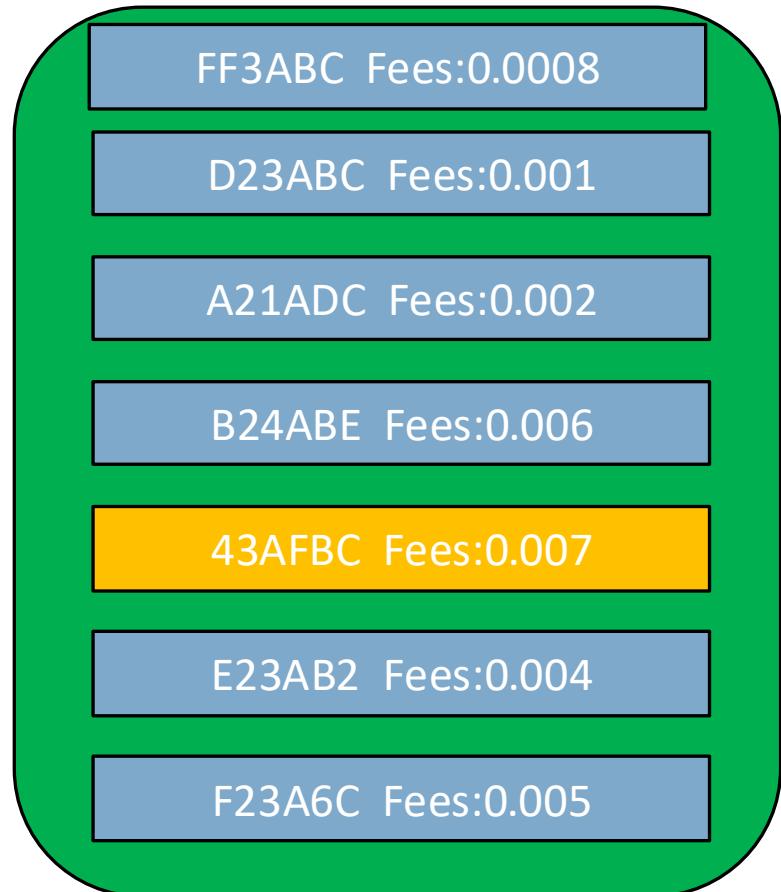
Mempool



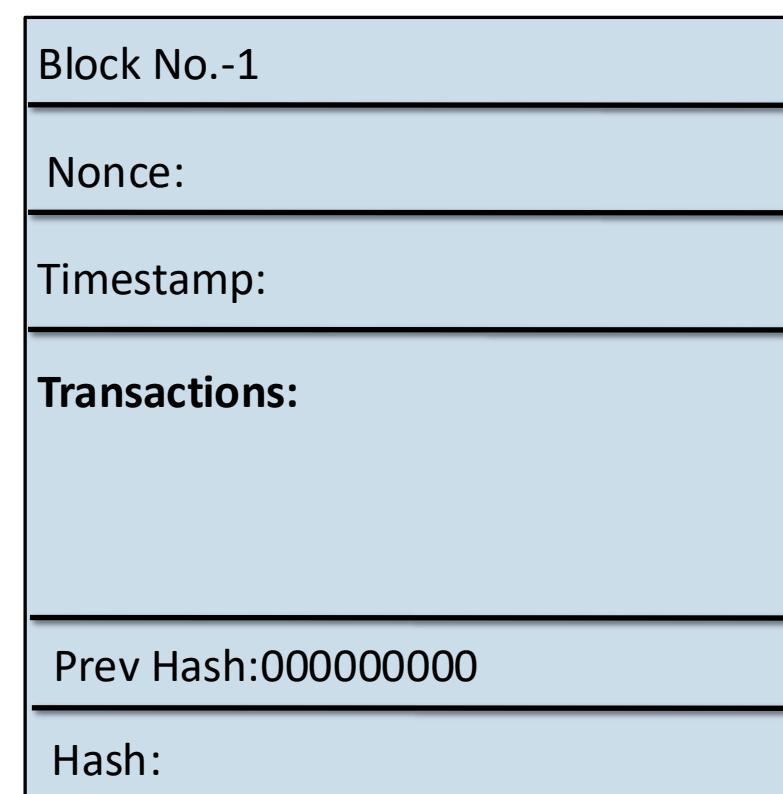
Mempool



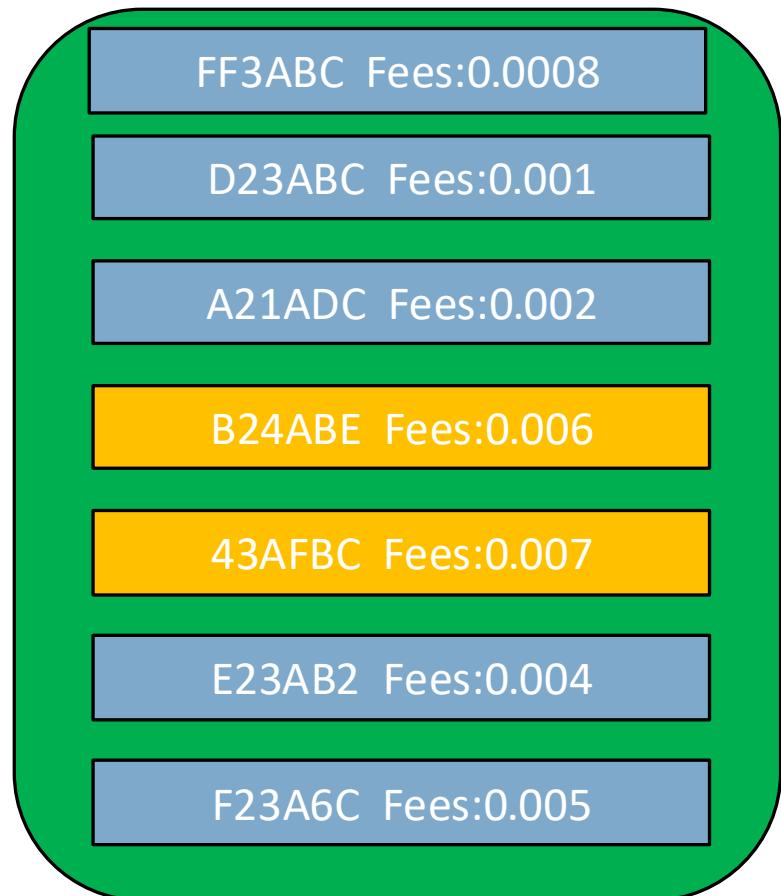
How actually mining of transaction takes place?



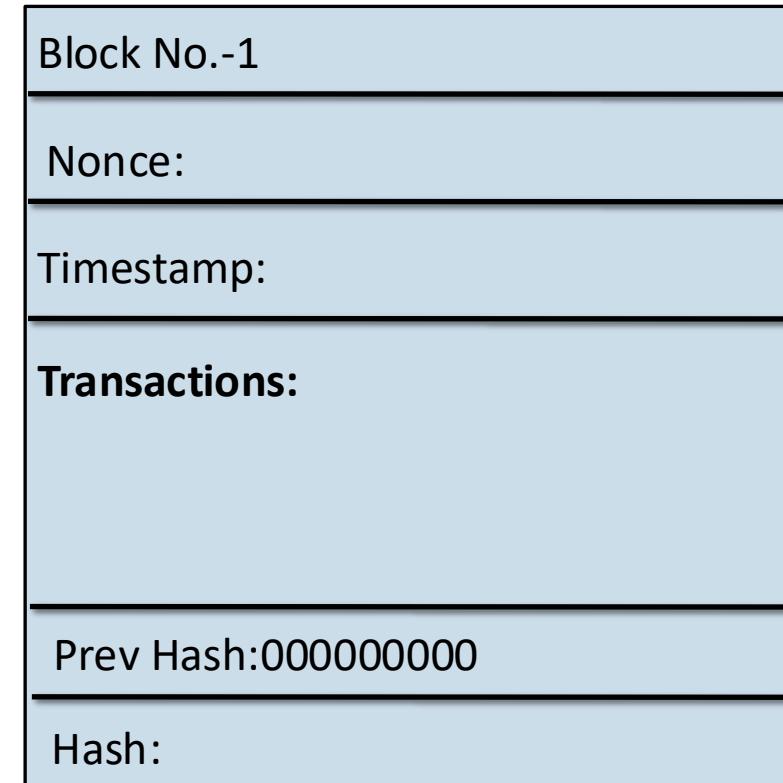
Mempool



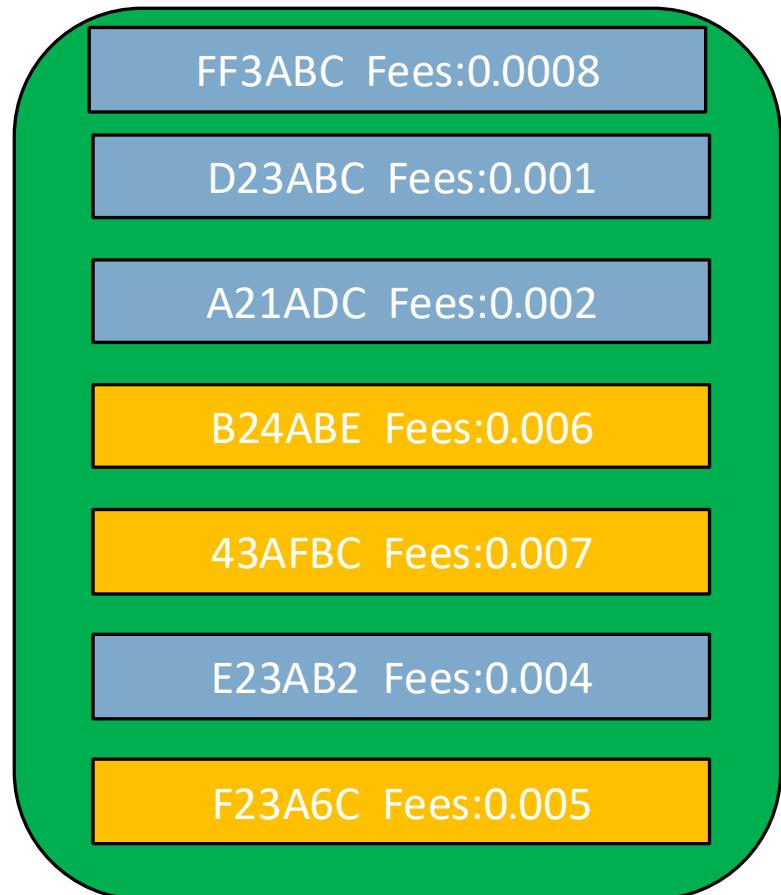
How actually mining of transaction takes place?



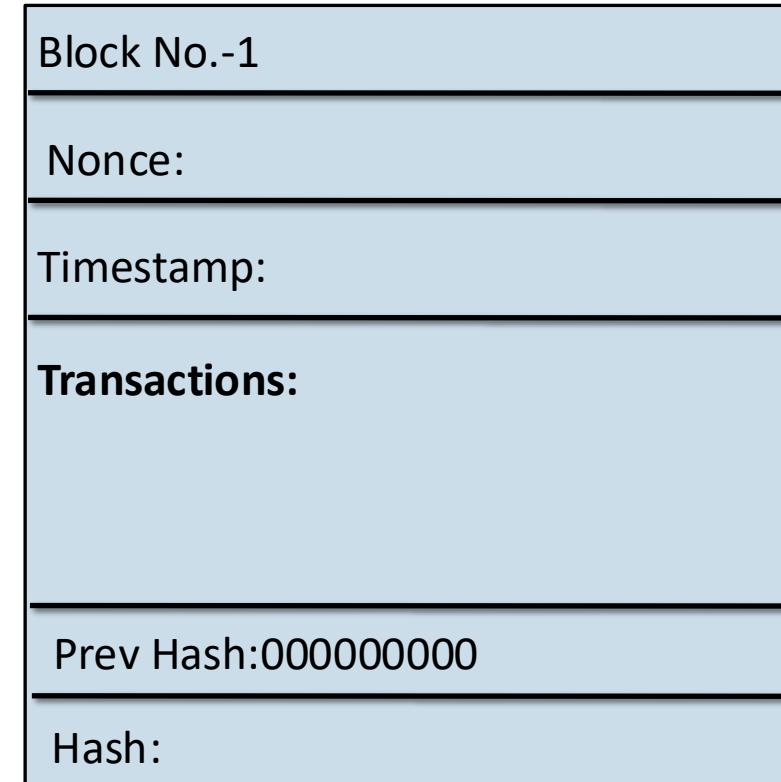
Mempool



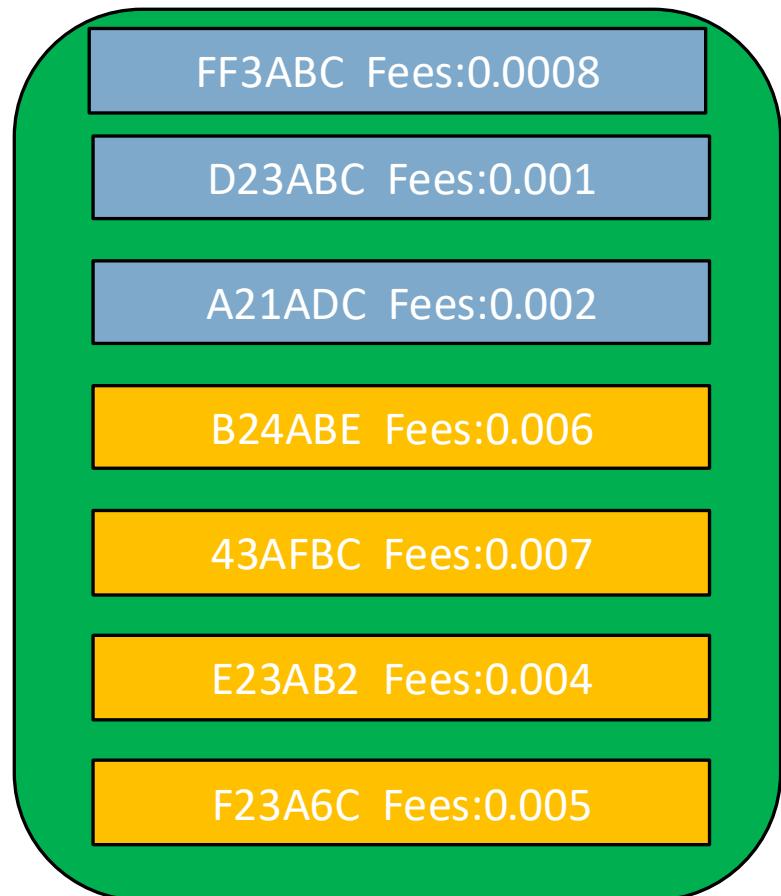
How actually mining of transaction takes place?



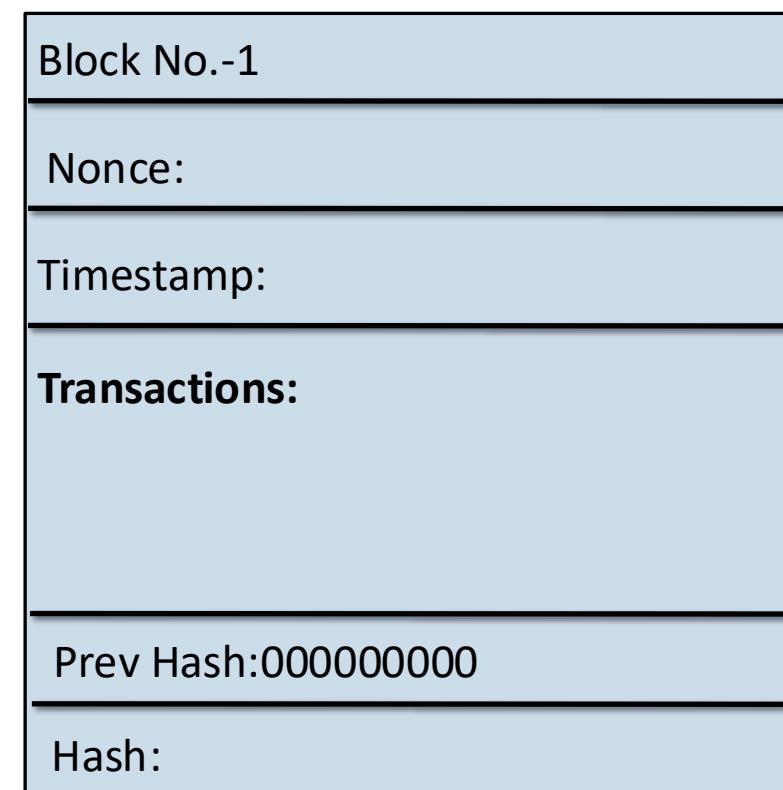
Mempool



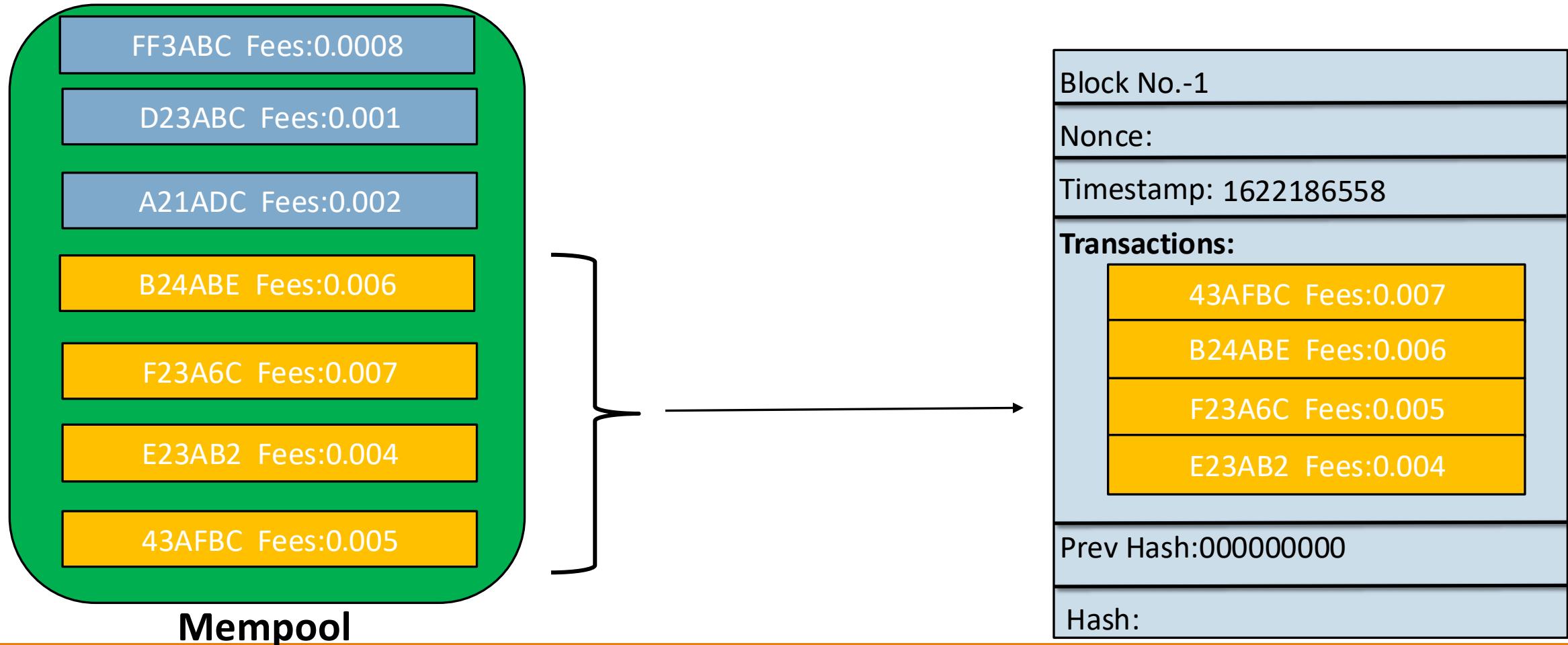
How actually mining of transaction takes place?



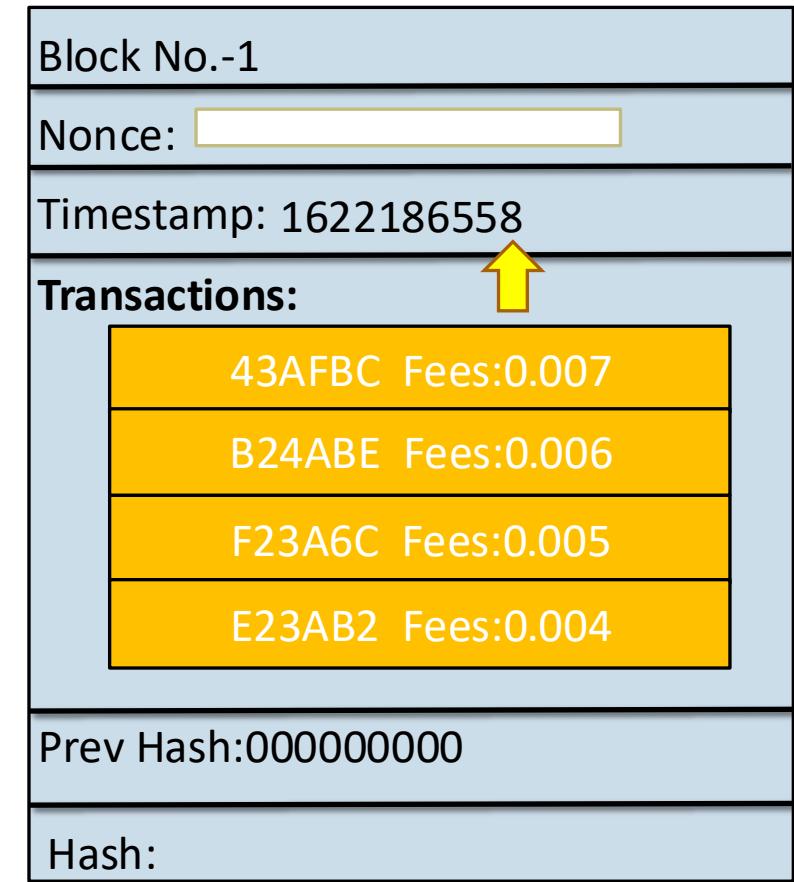
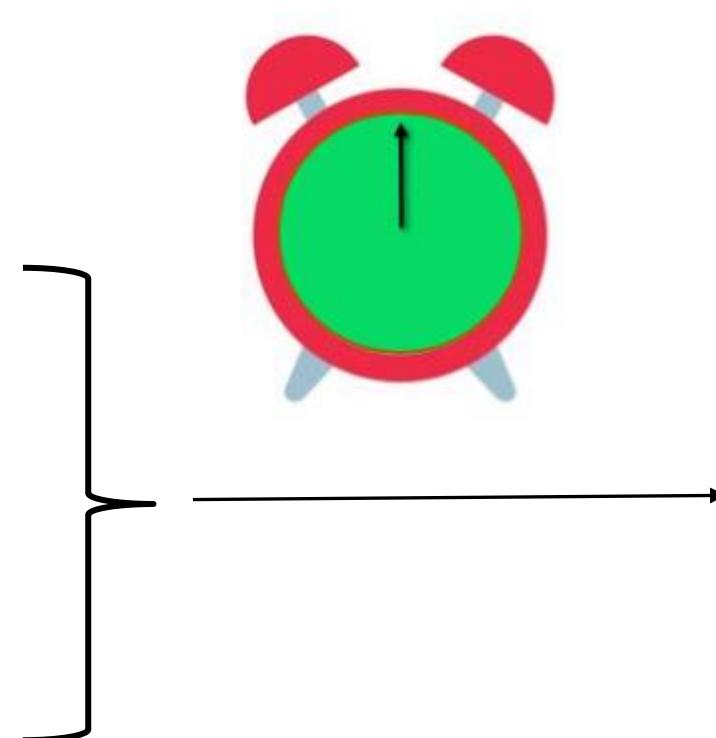
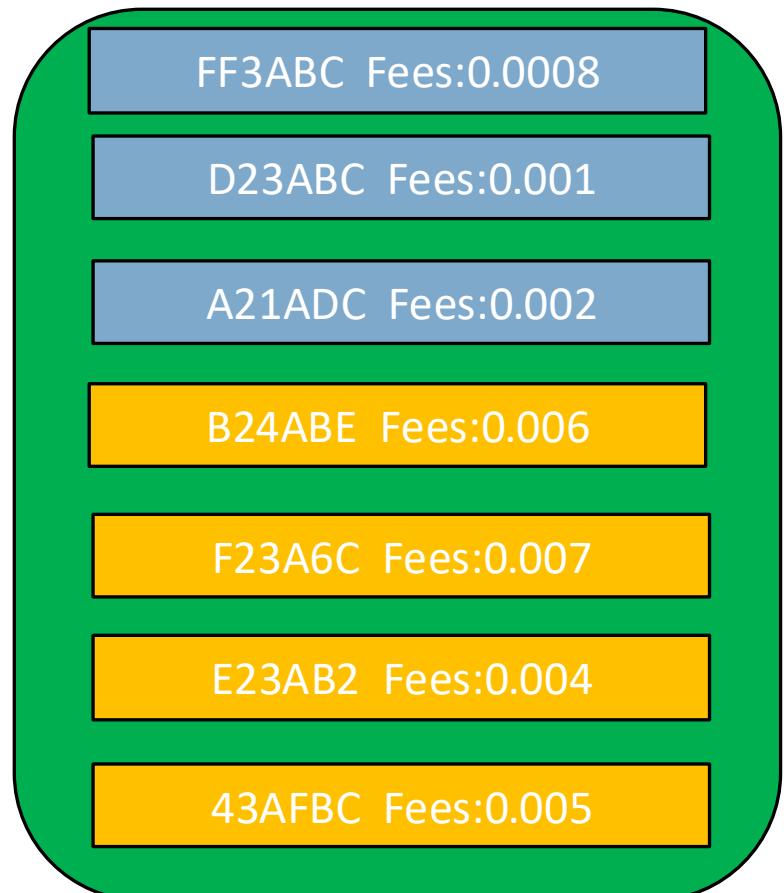
Mempool



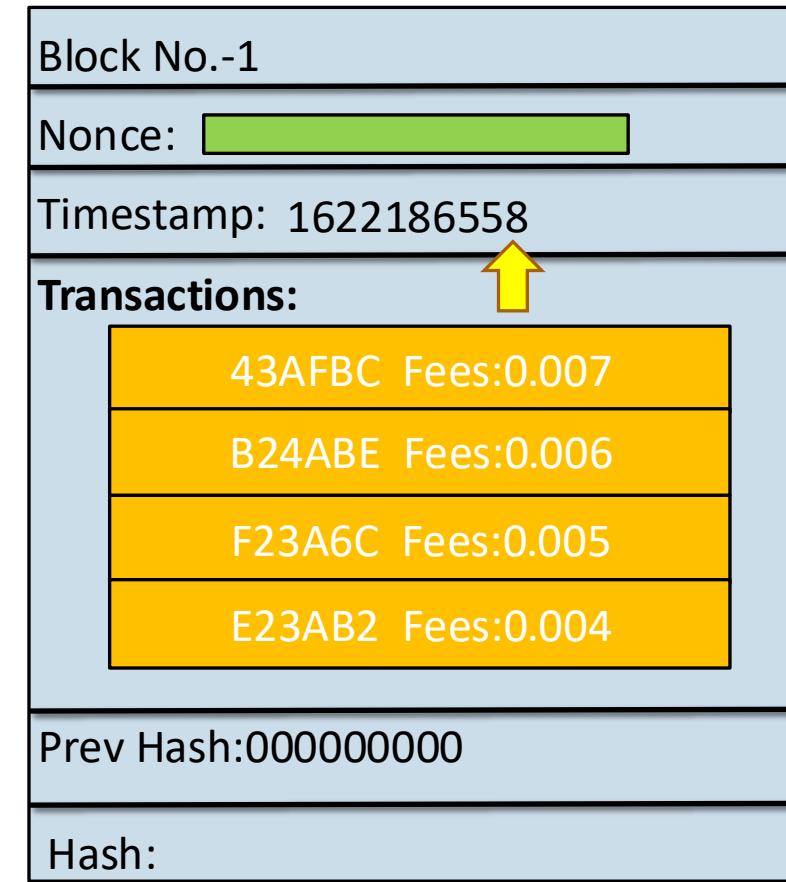
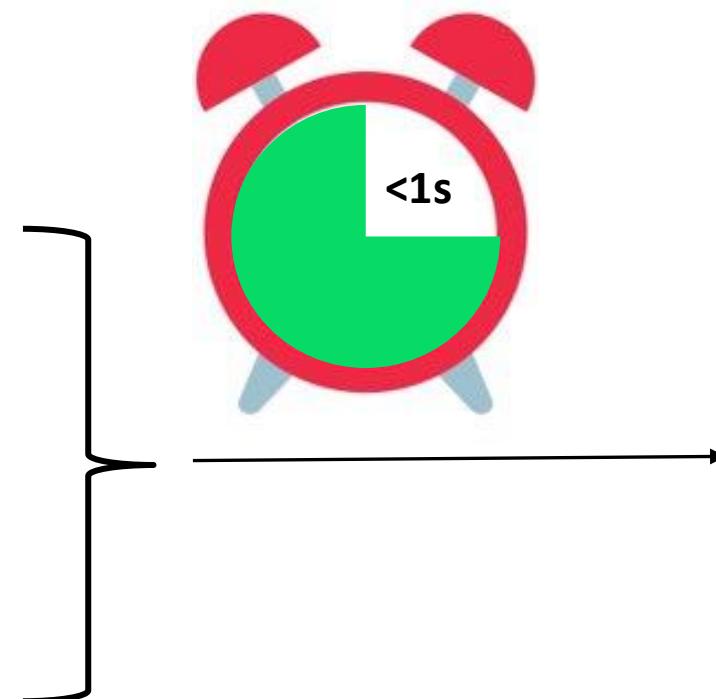
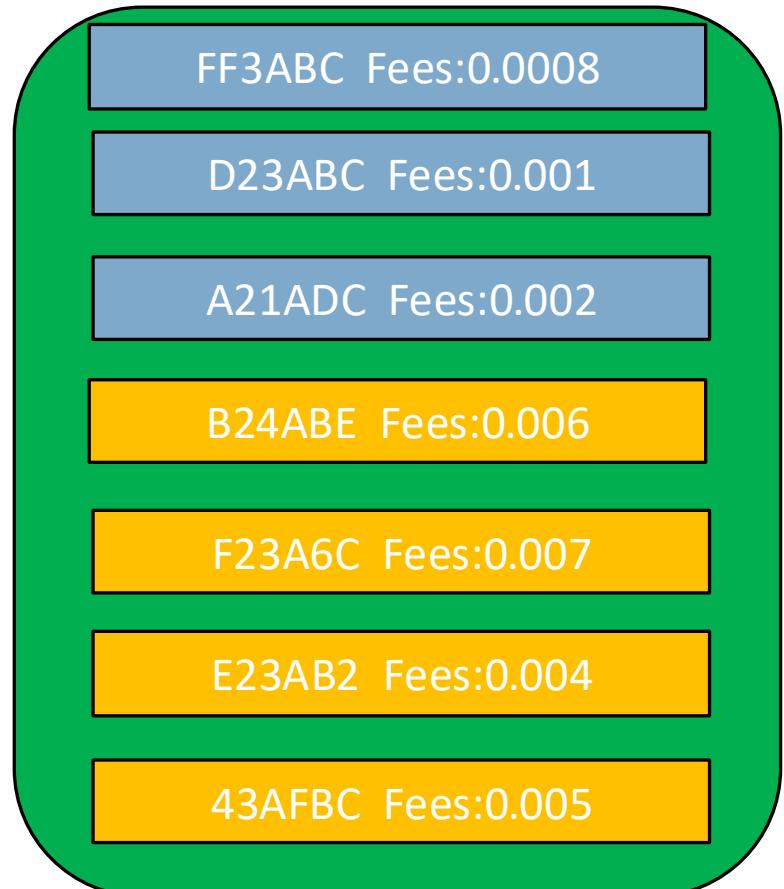
How actually mining of transaction takes place?



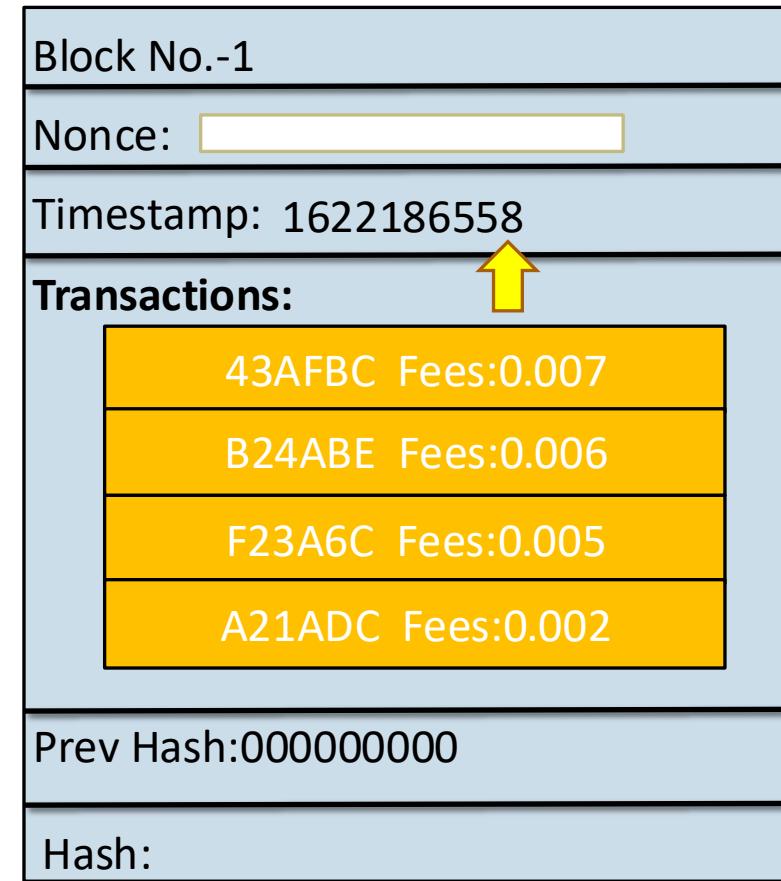
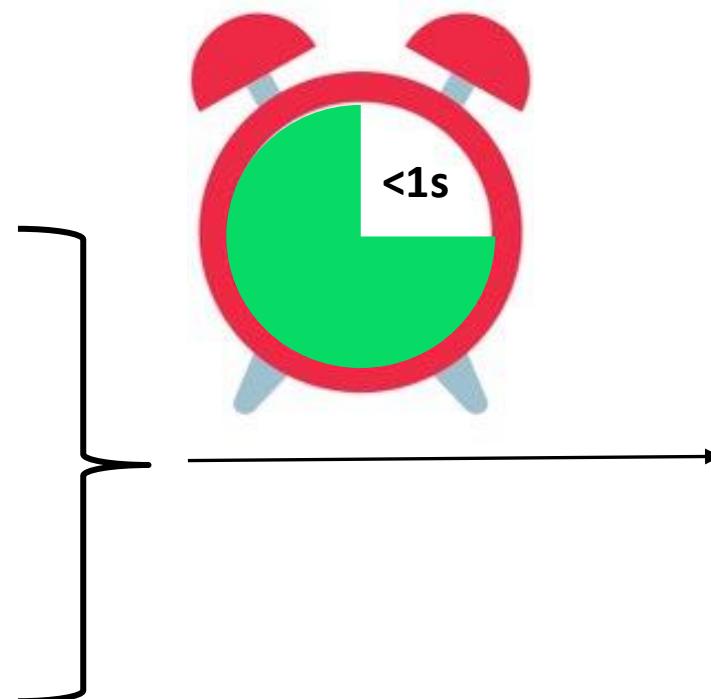
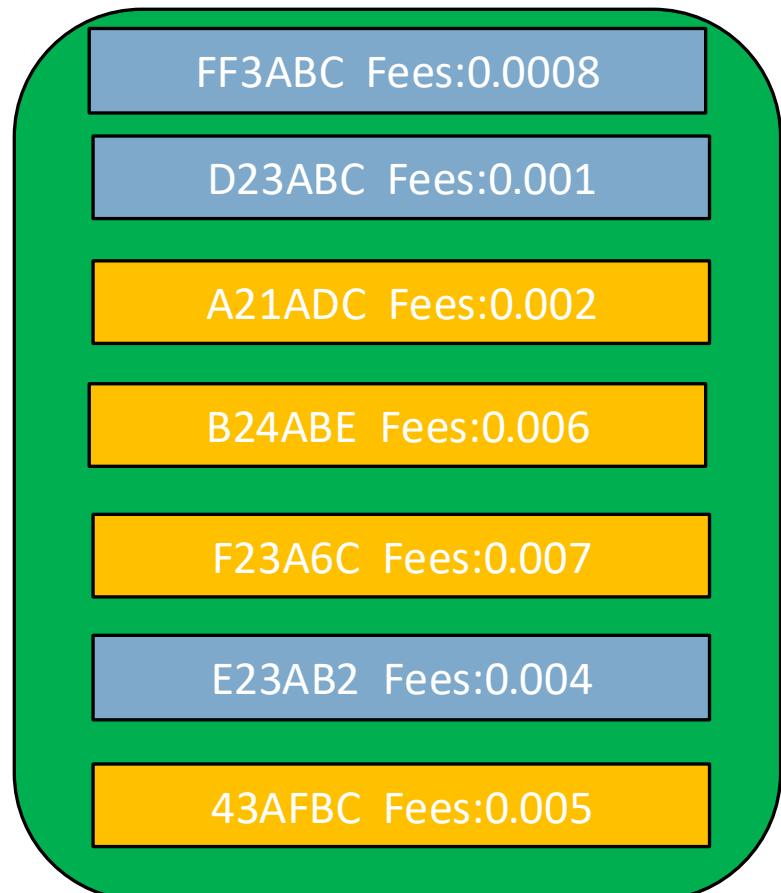
How actually mining of transaction takes place?



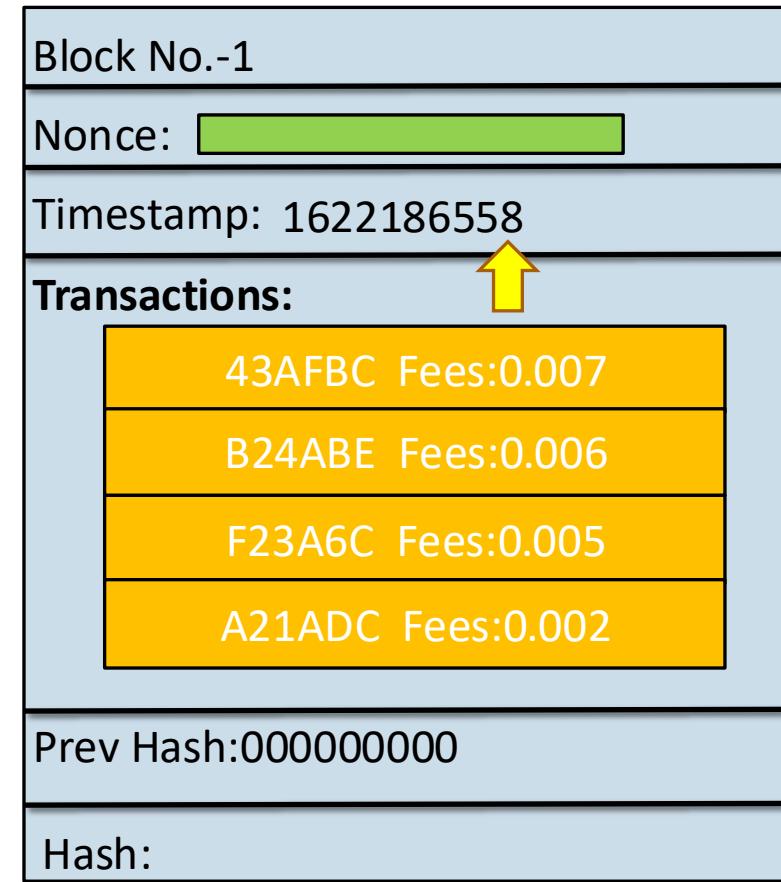
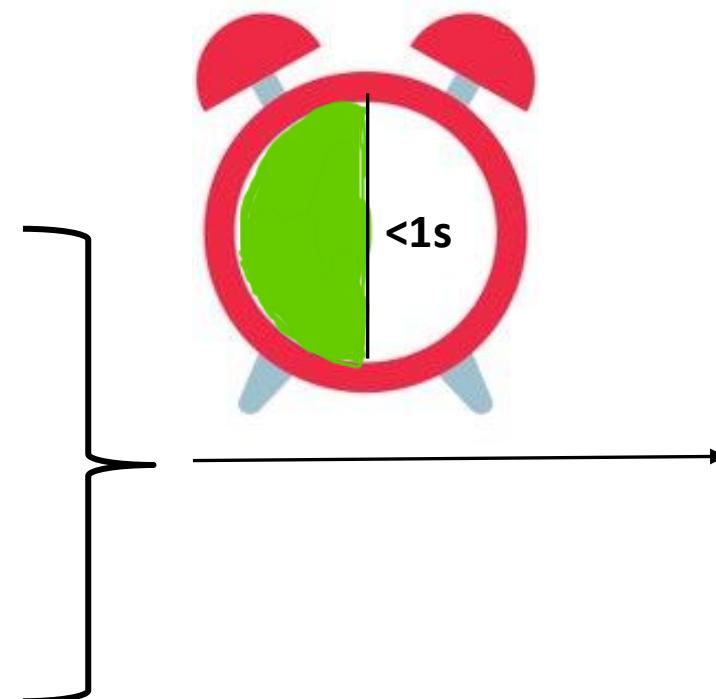
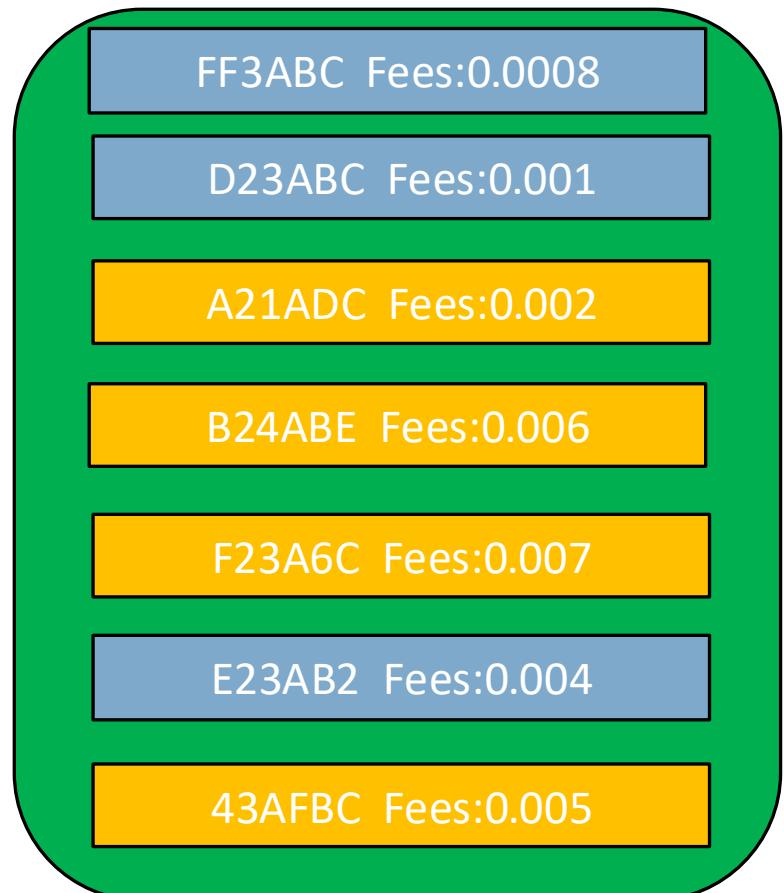
How actually mining of transaction takes place?



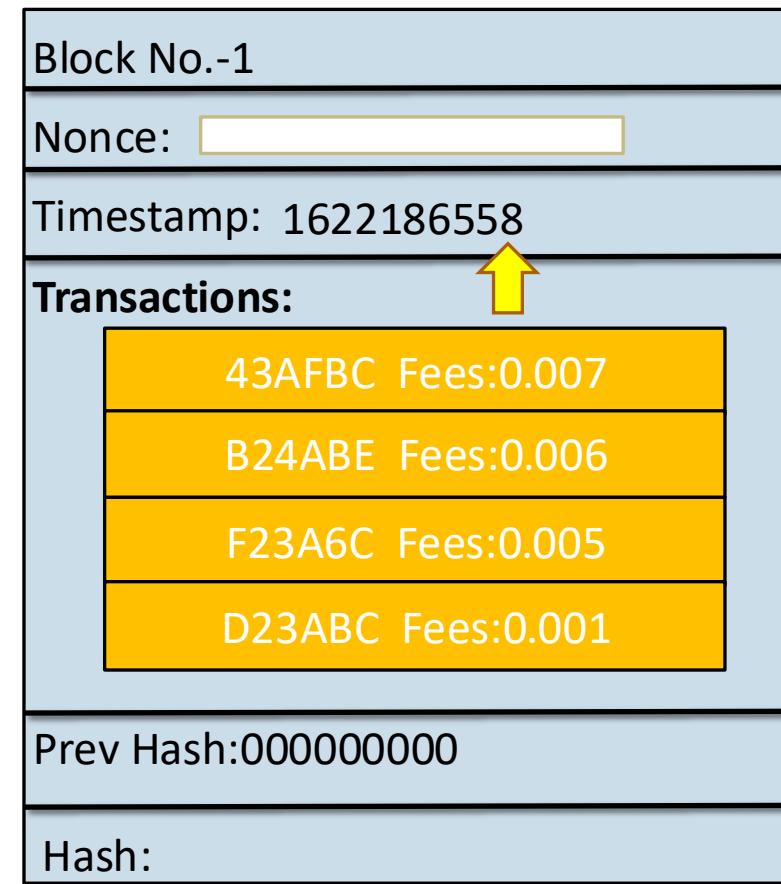
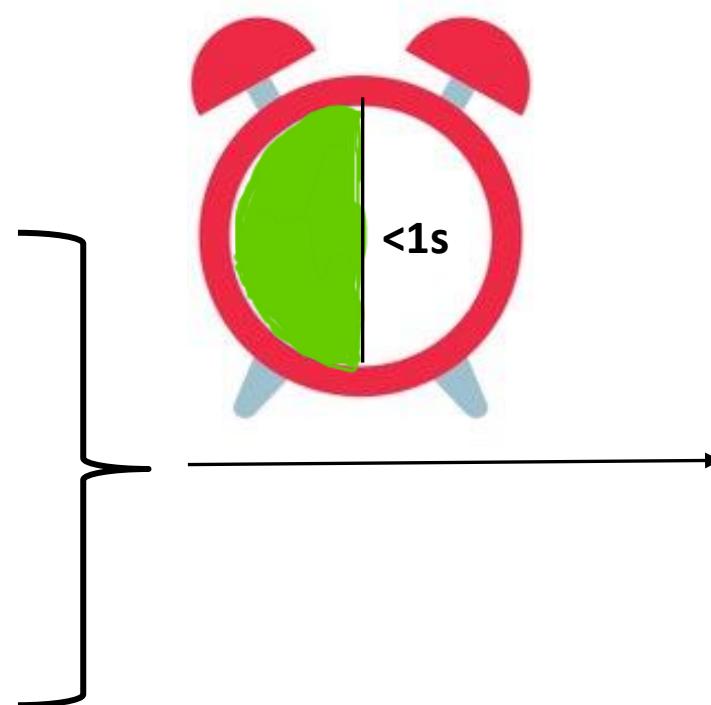
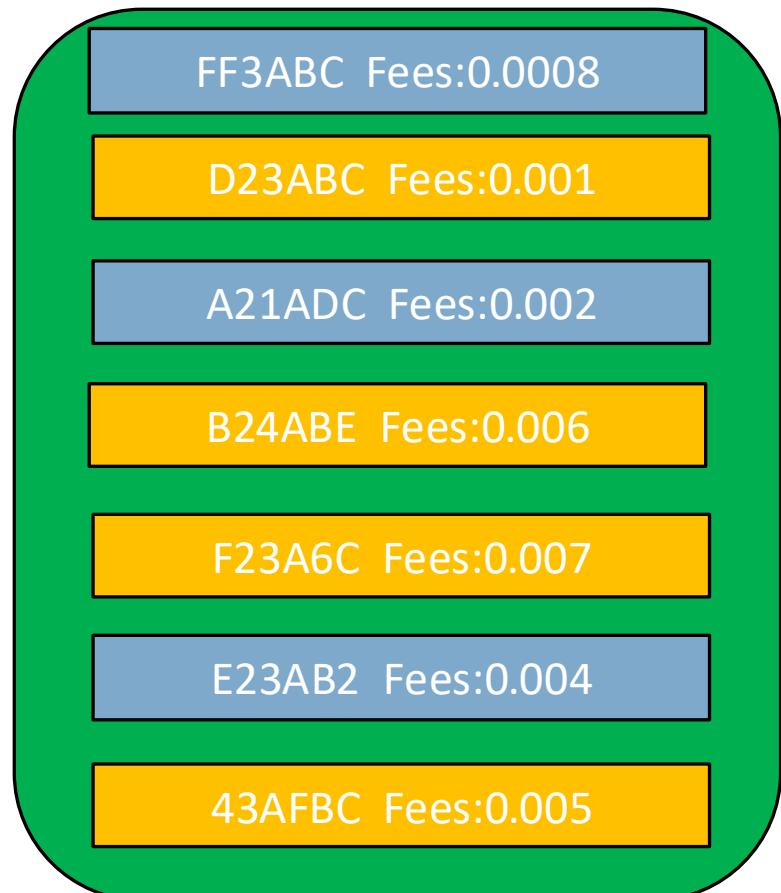
How actually mining of transaction takes place?



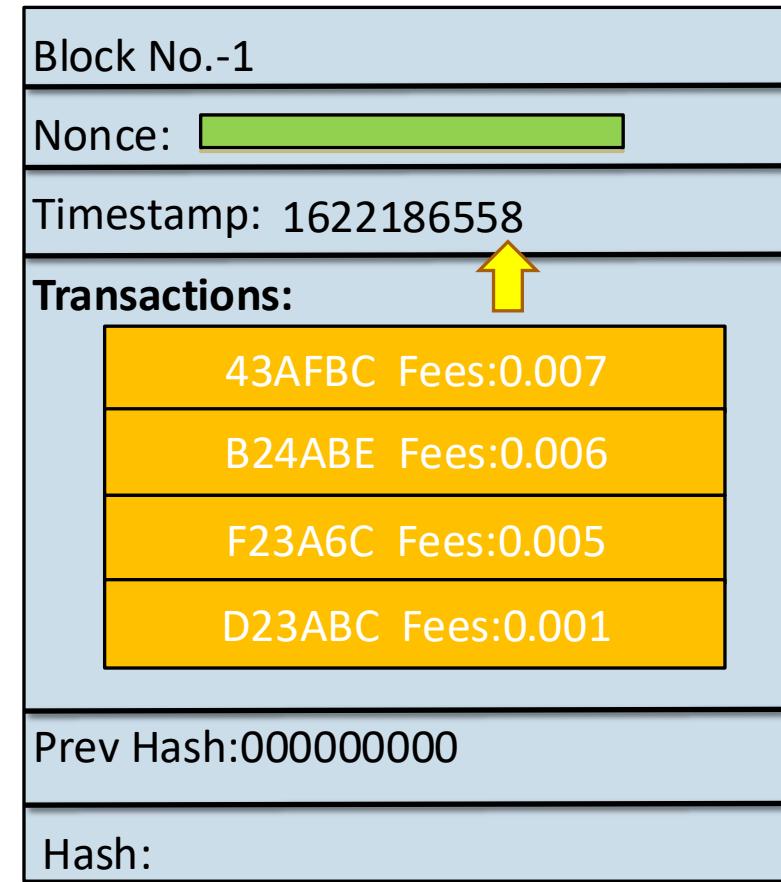
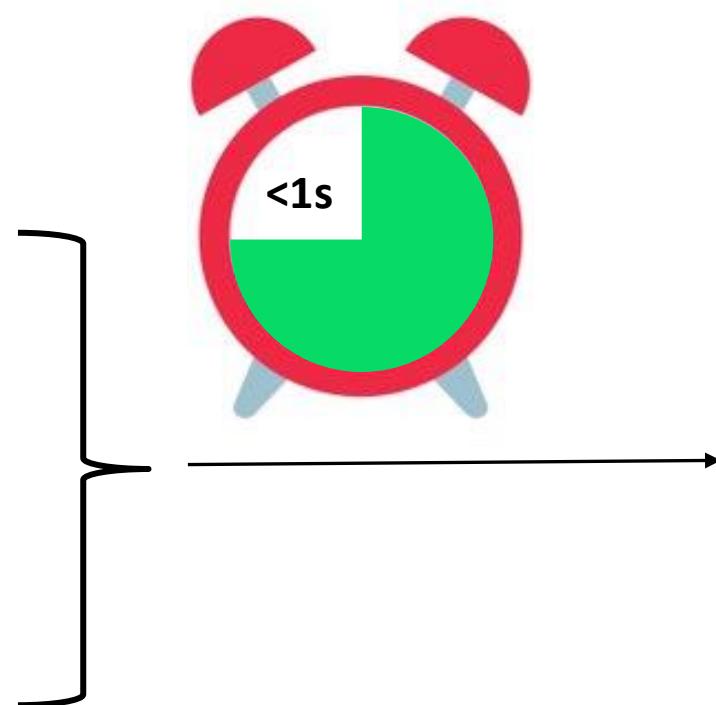
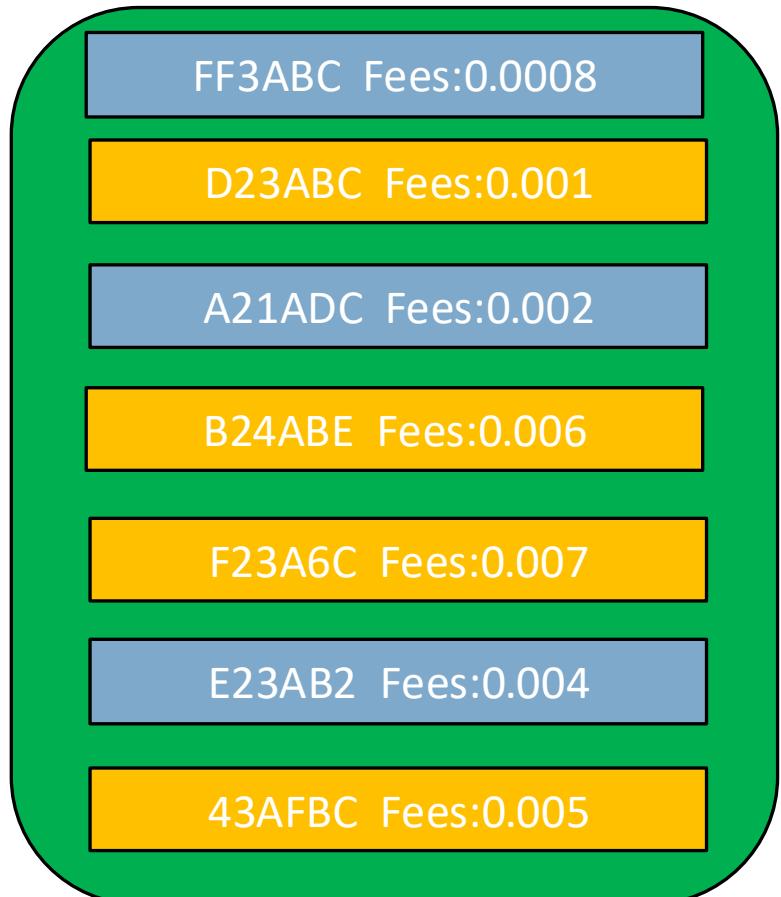
How actually mining of transaction takes place?



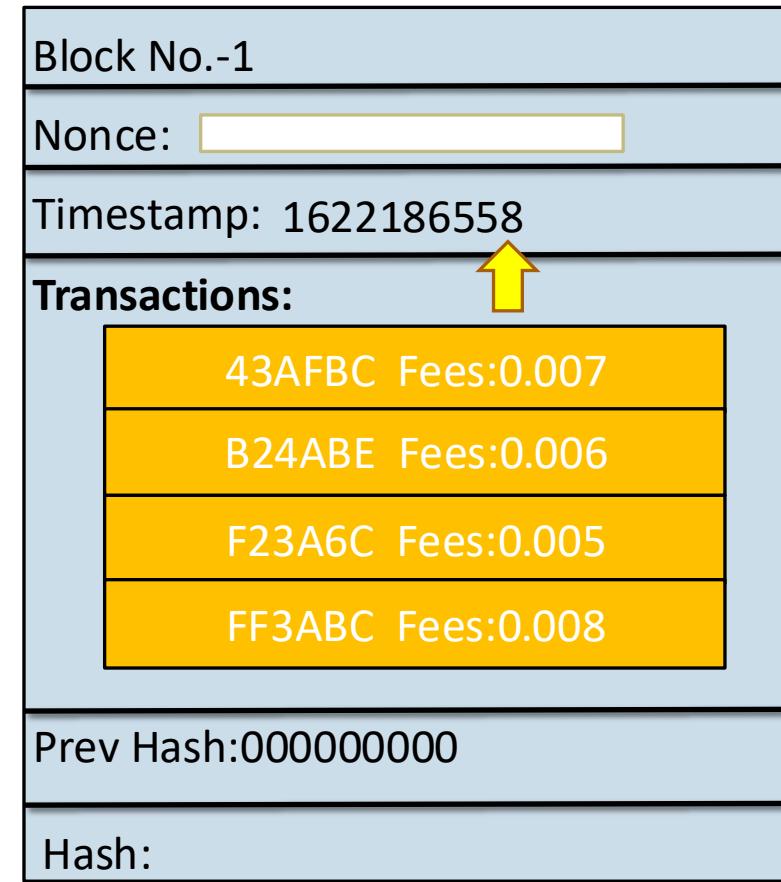
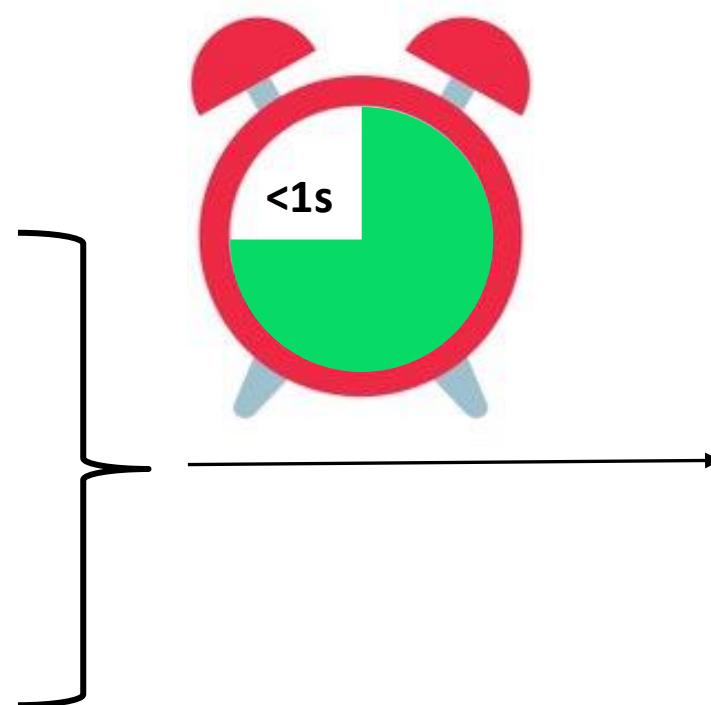
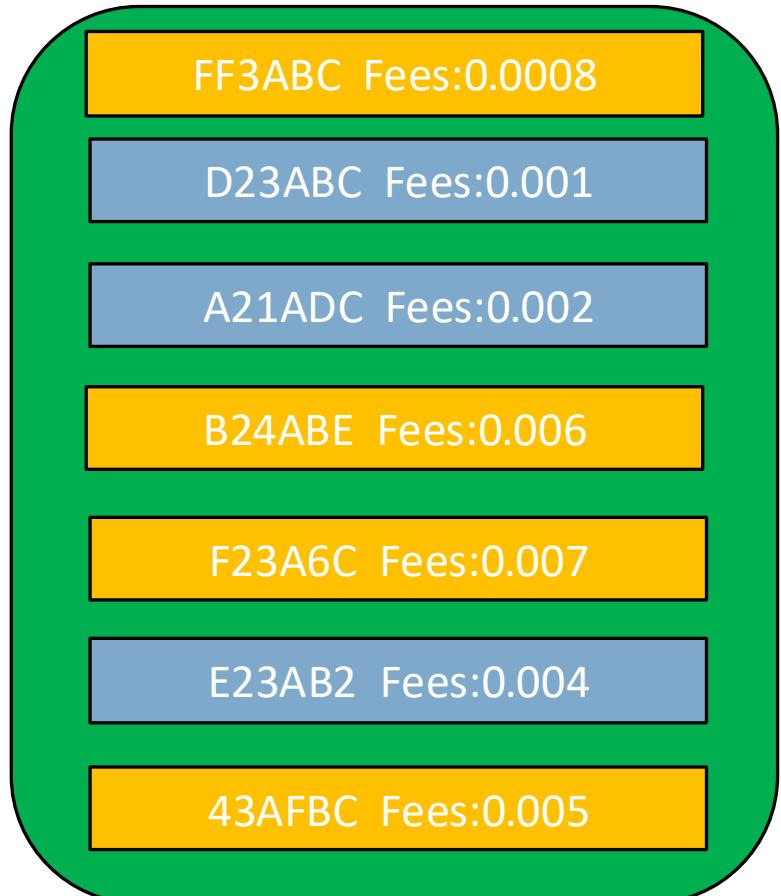
How actually mining of transaction takes place?



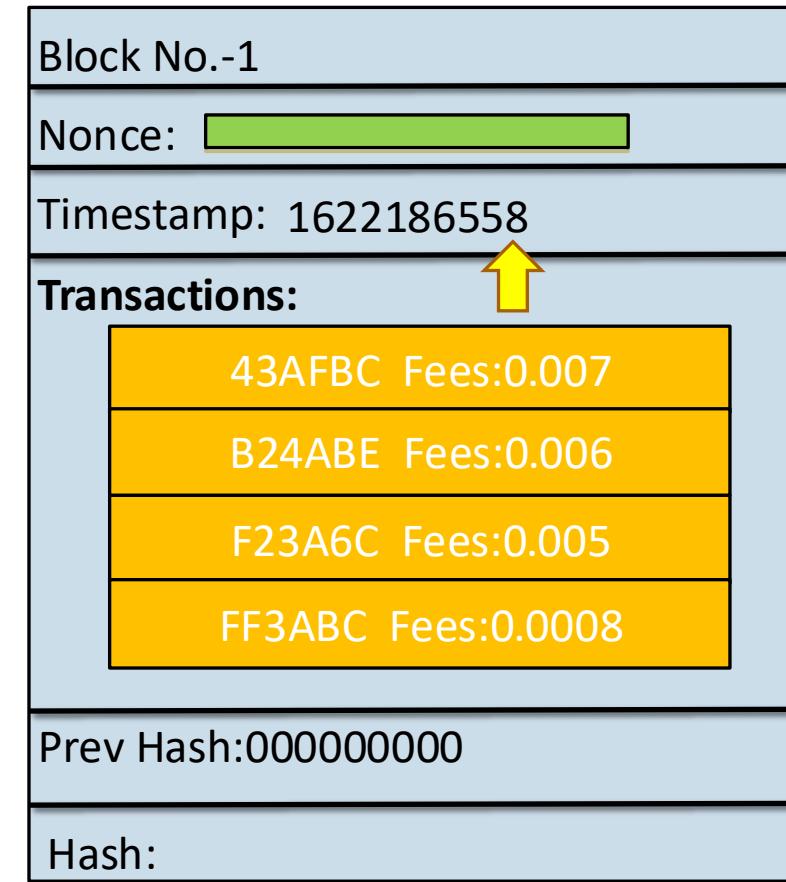
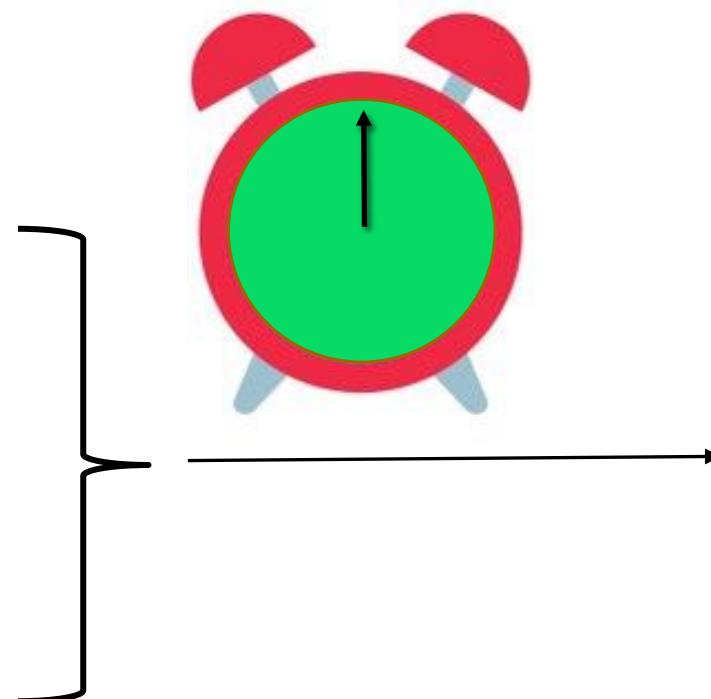
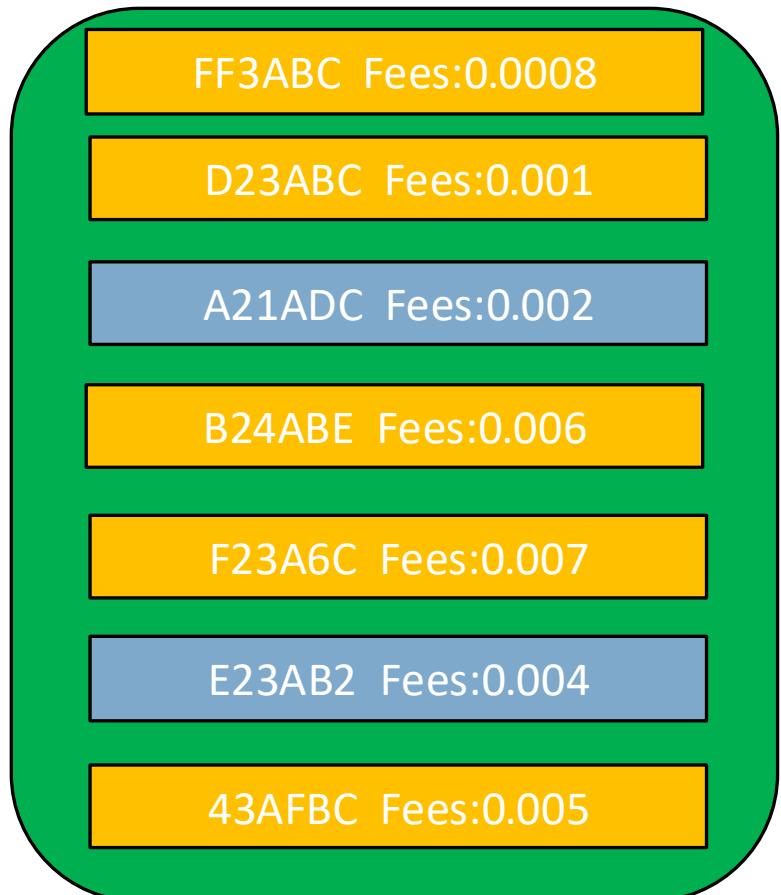
How actually mining of transaction takes place?



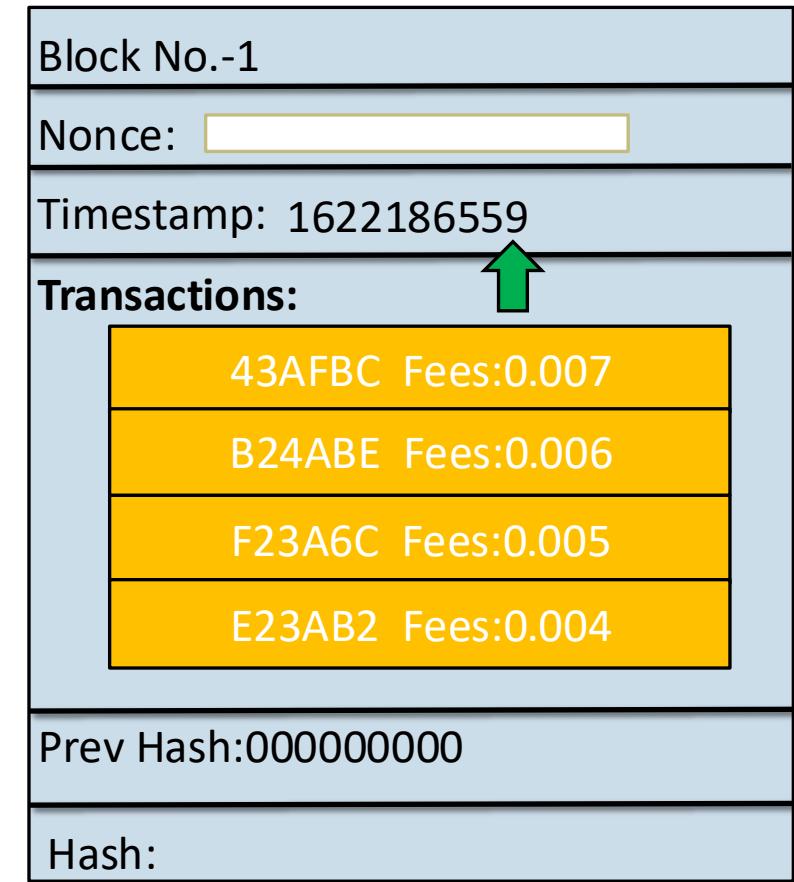
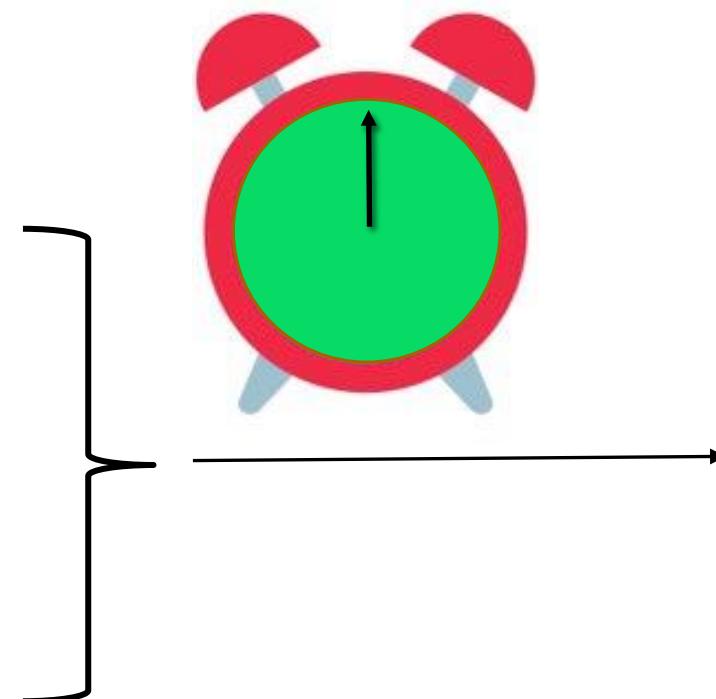
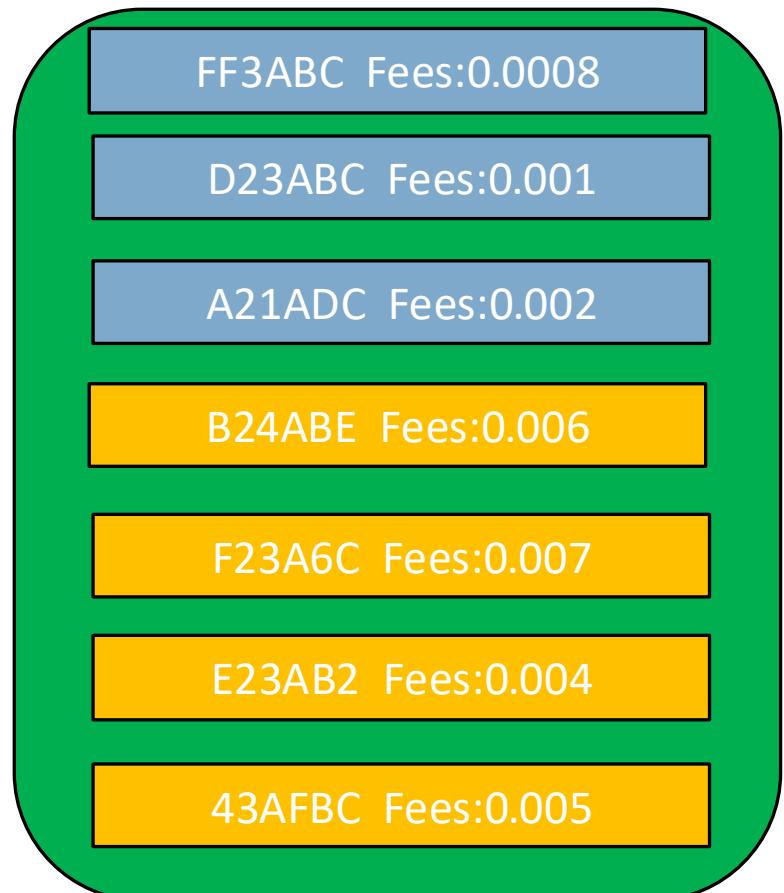
How actually mining of transaction takes place?



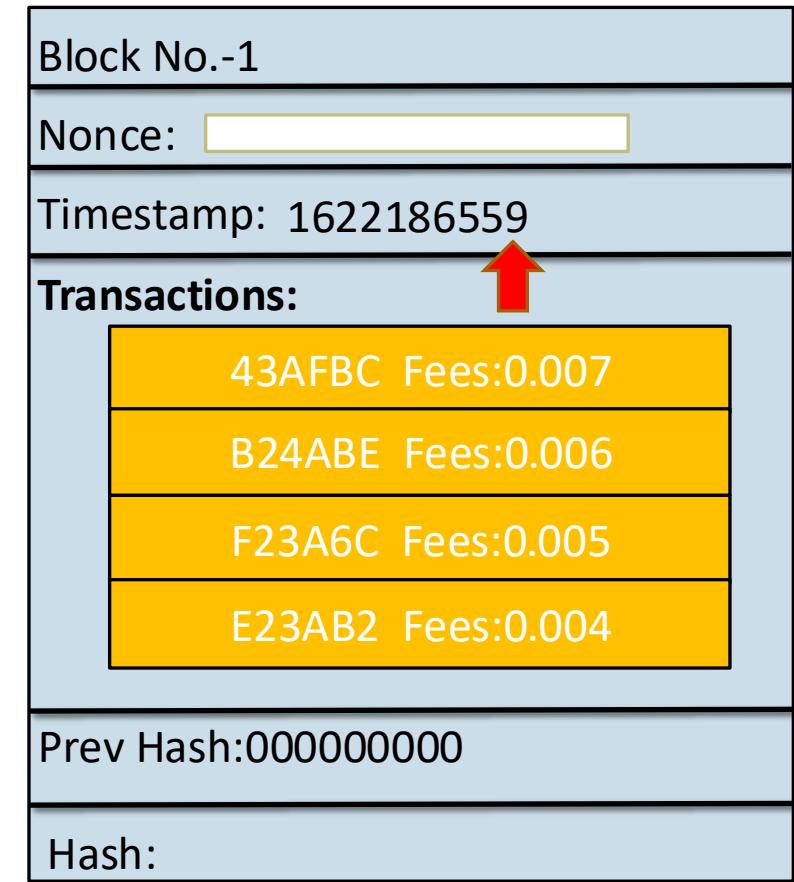
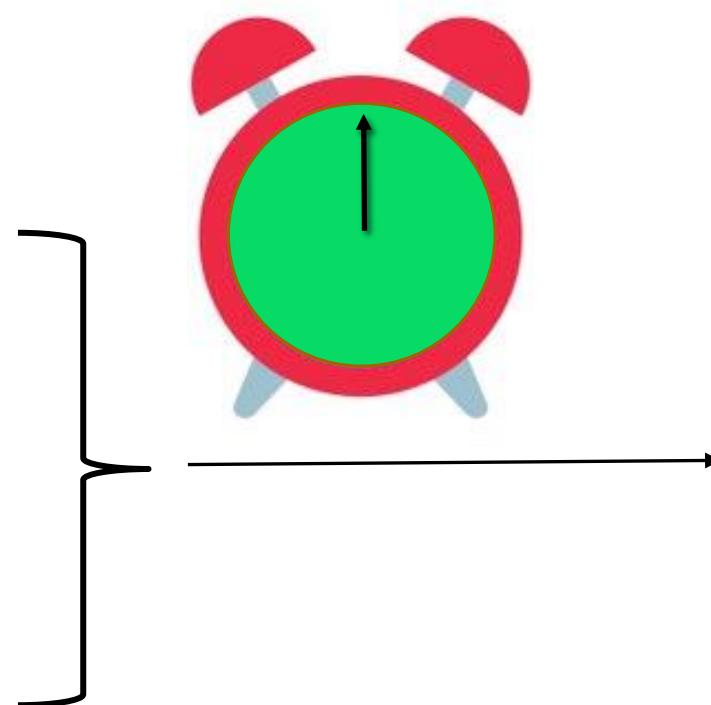
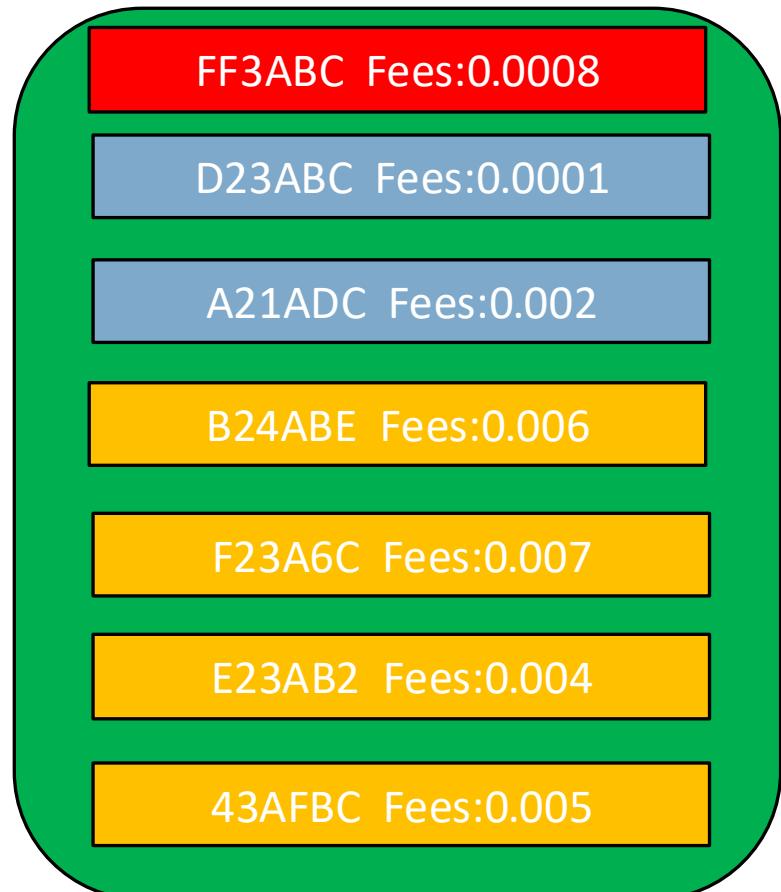
How actually mining of transaction takes place?



How actually mining of transaction takes place?

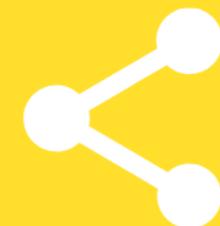


How actually mining of transaction takes place?



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

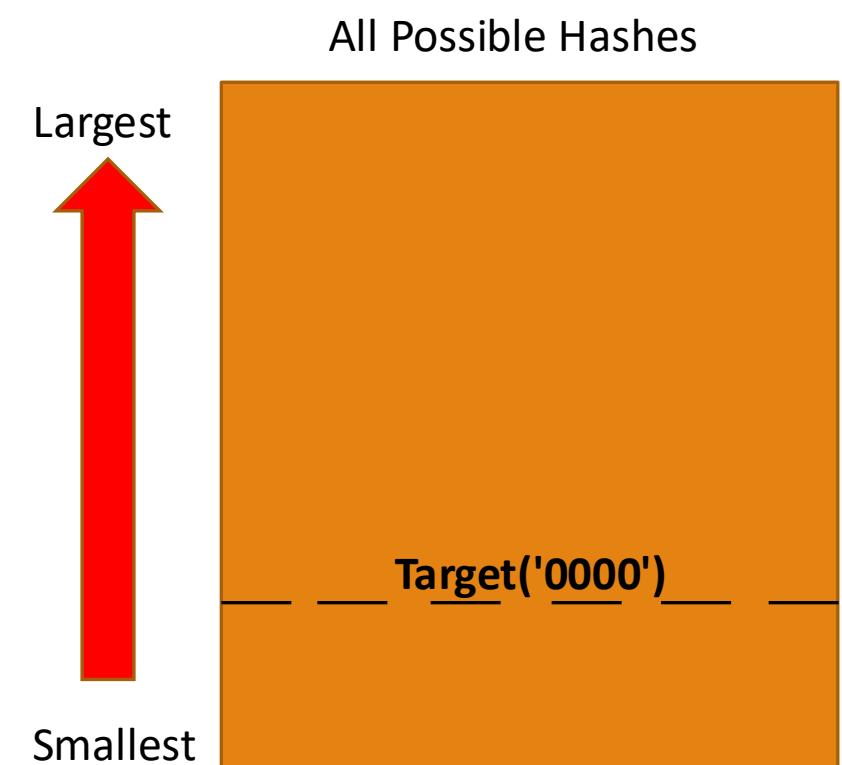


A large, semi-transparent circular graphic is positioned on the left side of the slide. It features a grid pattern and is filled with binary code (0s and 1s) in a light blue color. The graphic has a futuristic, digital aesthetic.

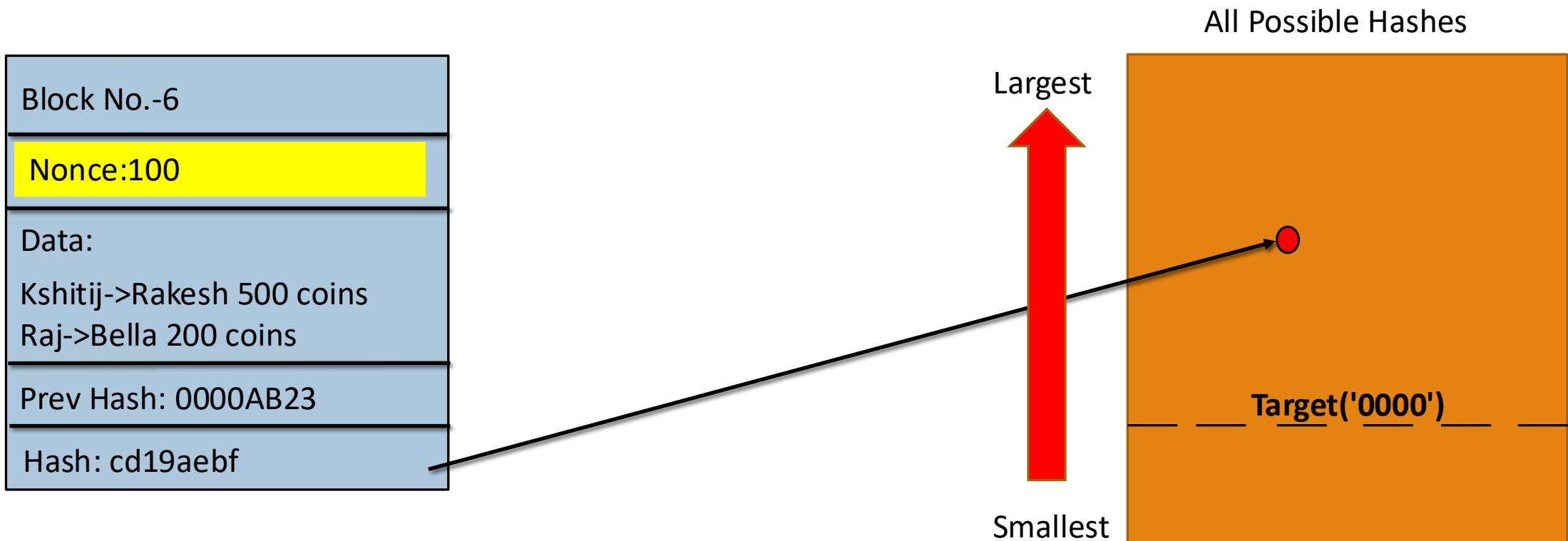
CPUs Vs GPUs Vs ASICs

How Mining Works ?

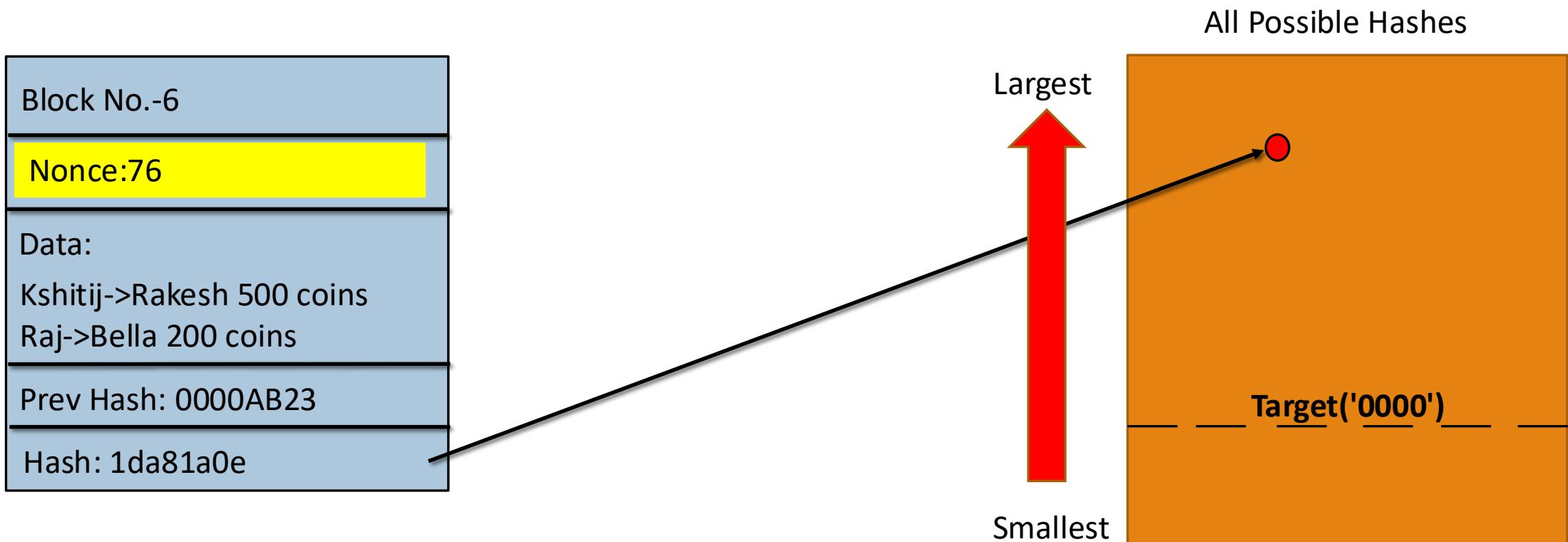
Block No.-6
Nonce:
Data: Kshitij->Rakesh 500 coins Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: cd19aebf



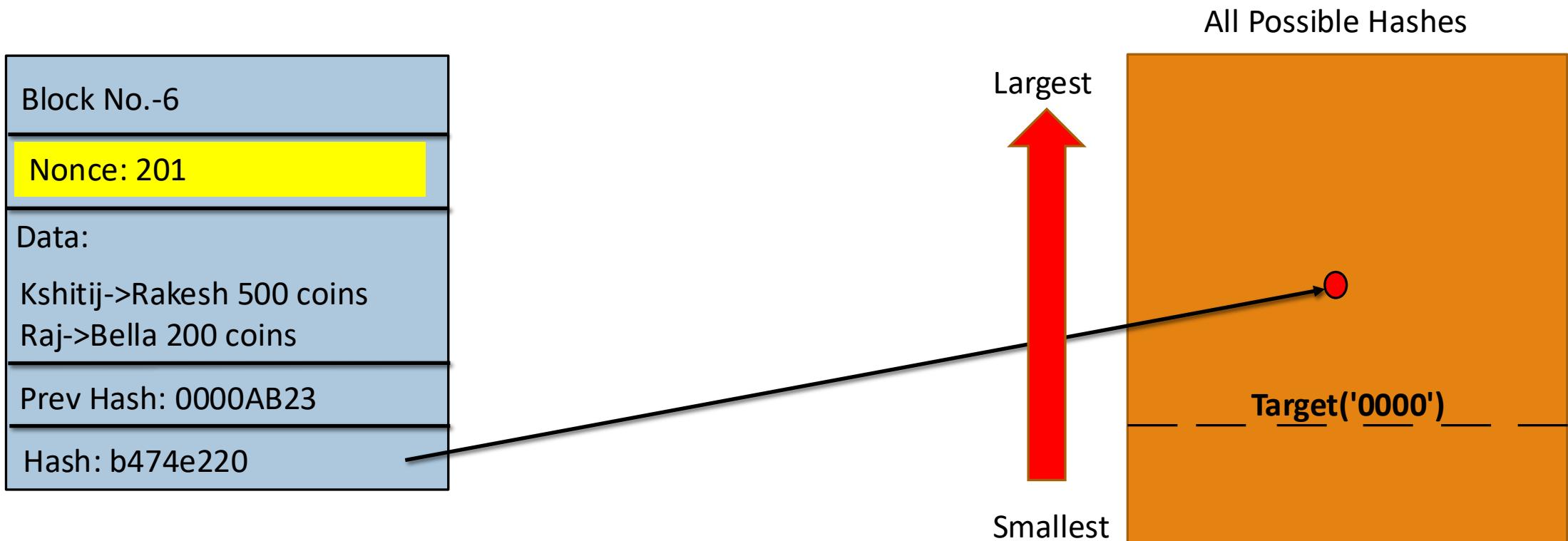
How Mining Works ?



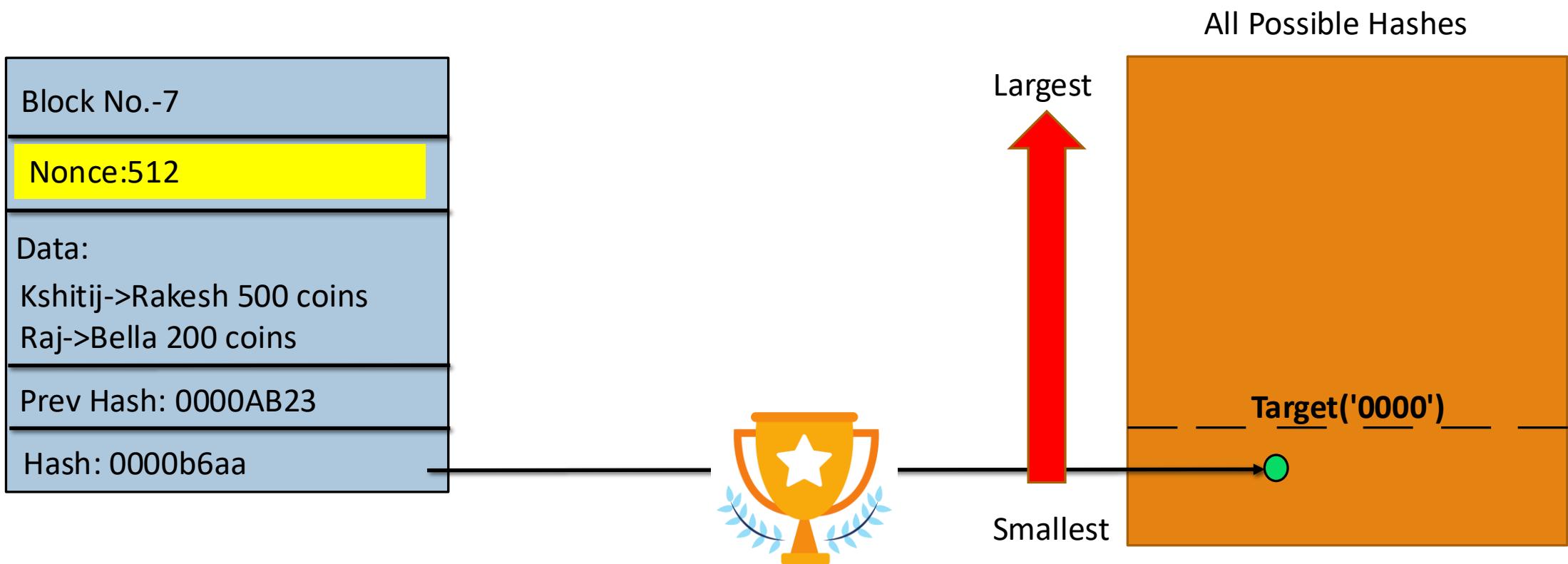
How Mining Works ?



How Mining Works ?



How Mining Works ?

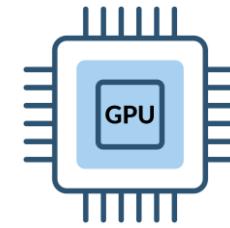


CPUs Vs GPUs Vs ASICs

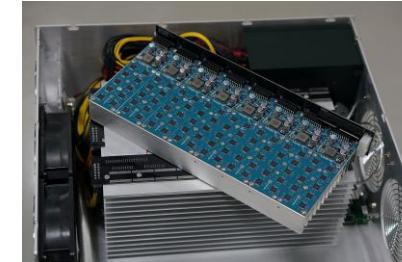
CPU < 10 MH/s



GPU< 1 GH/s



ASIC> 110 TH/s



**GIVE THIS VIDEO
A THUMBS-UP !**

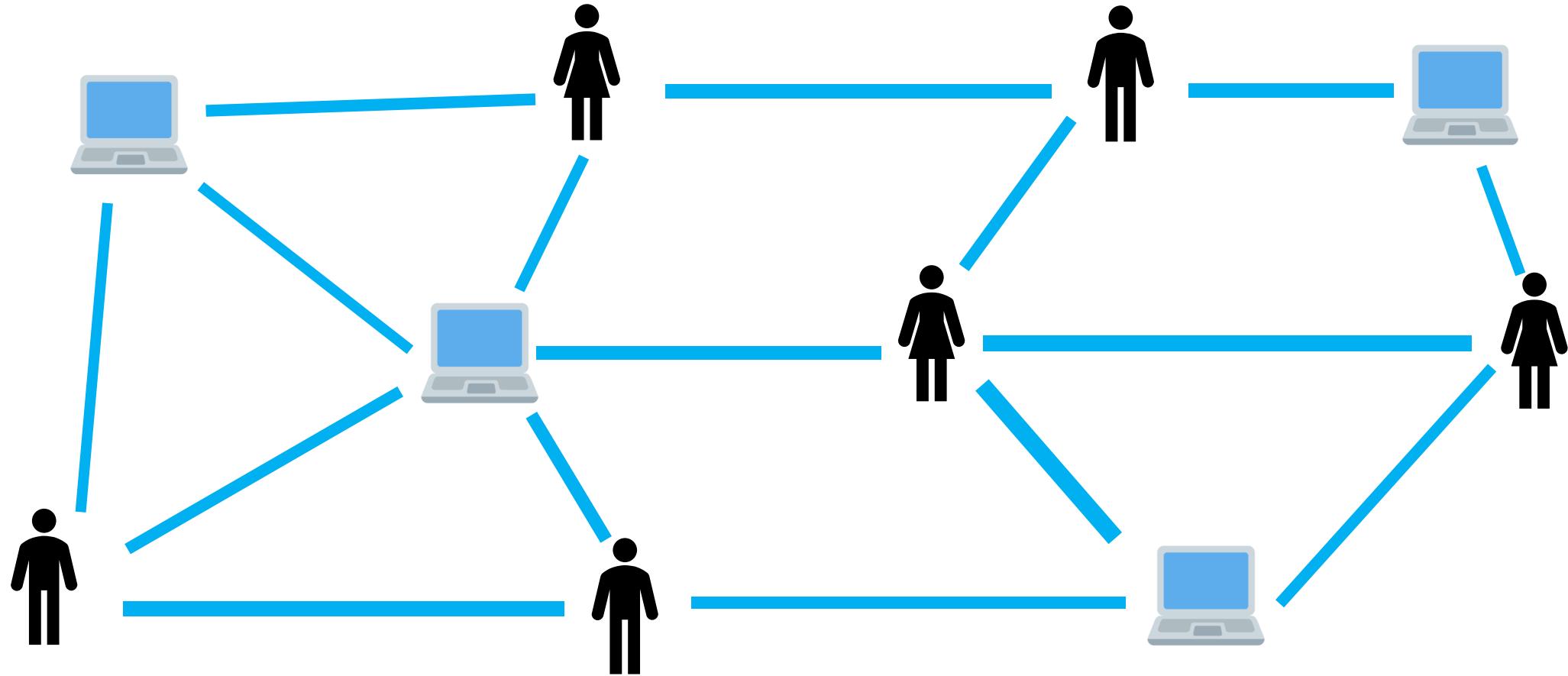
CODE EATER



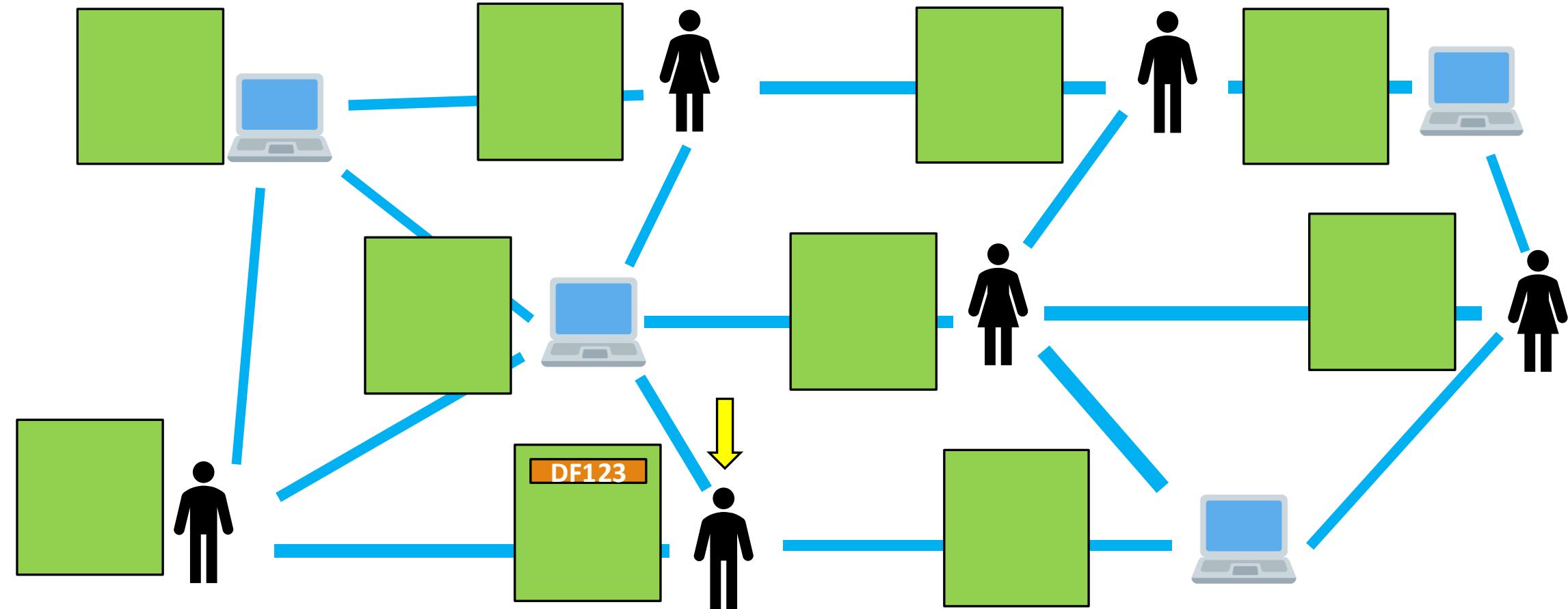
A complex, abstract digital background featuring a circular pattern of concentric arcs and lines. The background is a dark teal color with a grid overlay. Numerous binary digits (0s and 1s) are scattered across the image, appearing both within the circular design and in the surrounding space. The overall effect is futuristic and technical.

How mempool works?

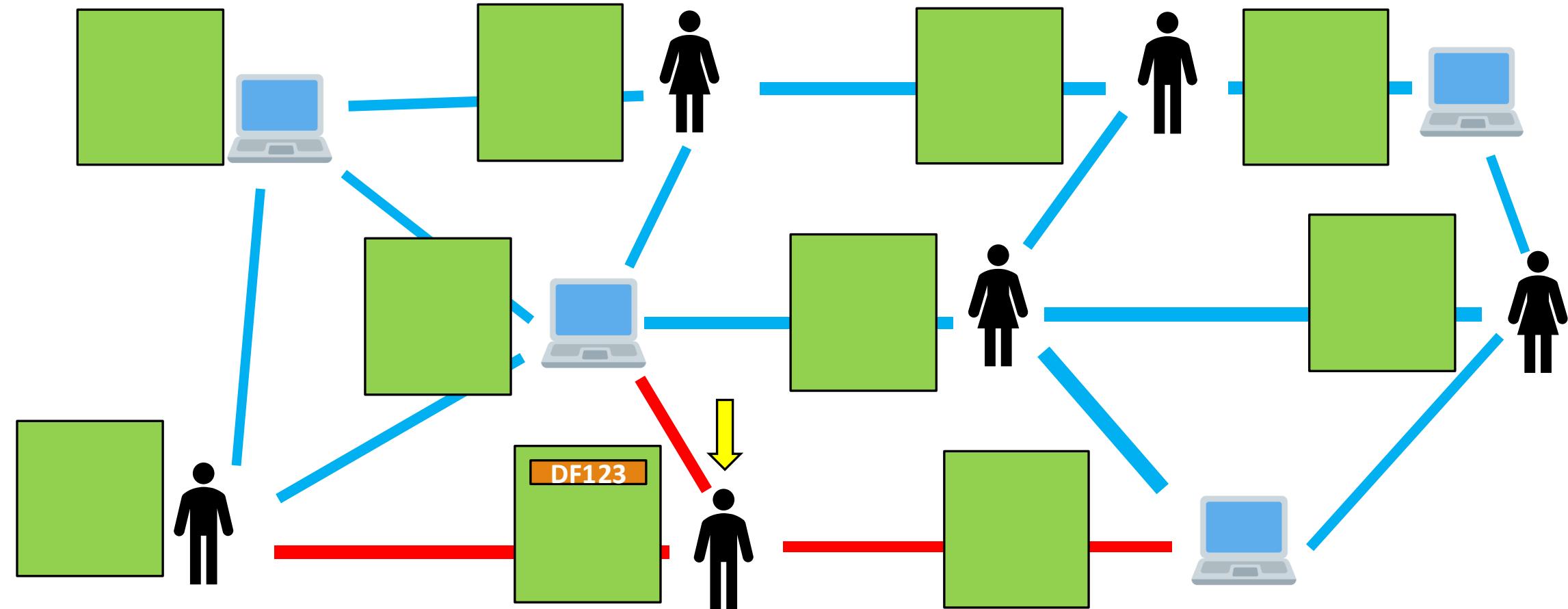
How do Mempool works?(Behind the scenes)



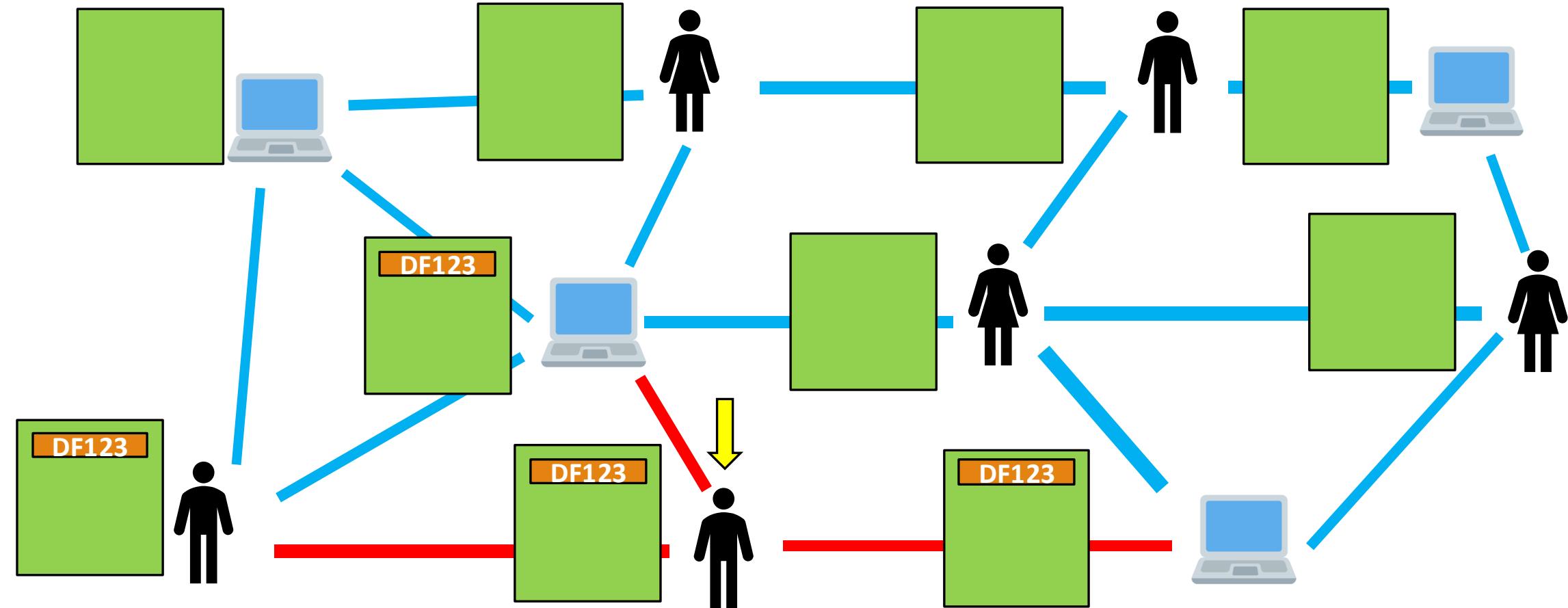
How do Mempool works?(Behind the scenes)



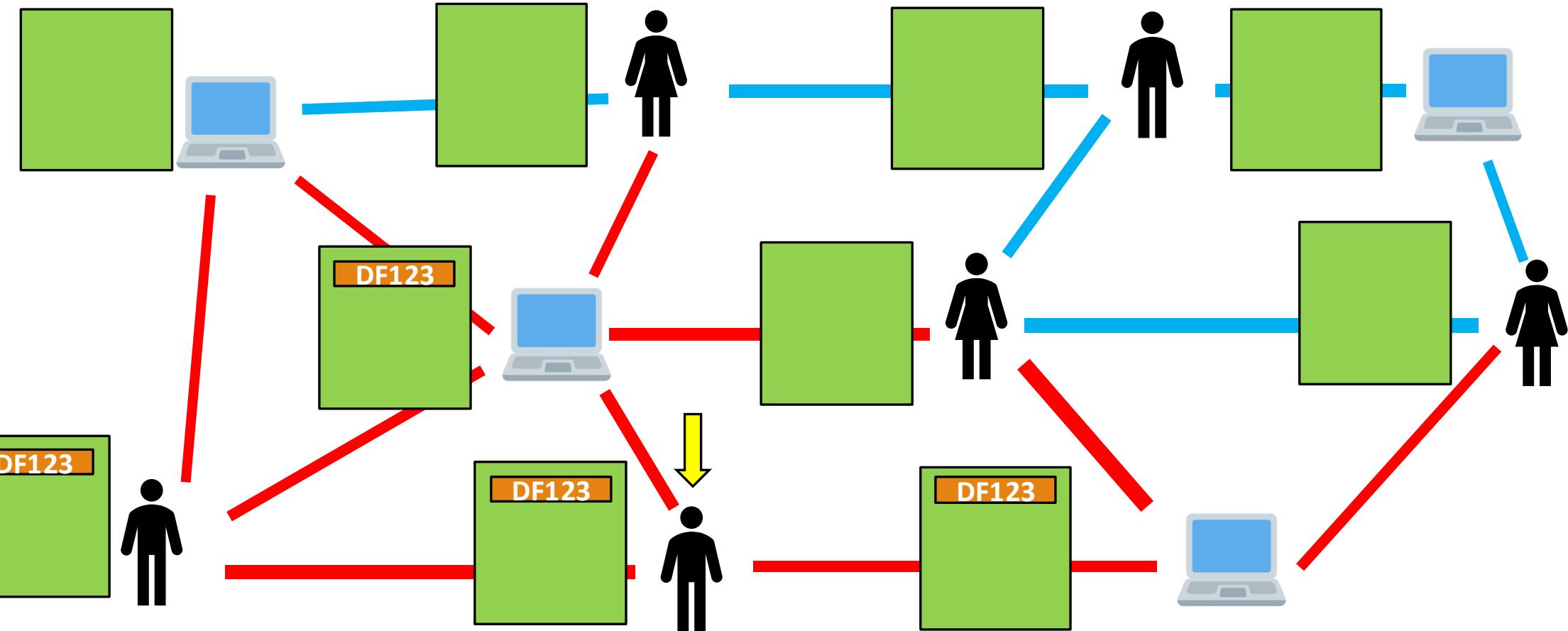
How do Mempool works?(Behind the scenes)



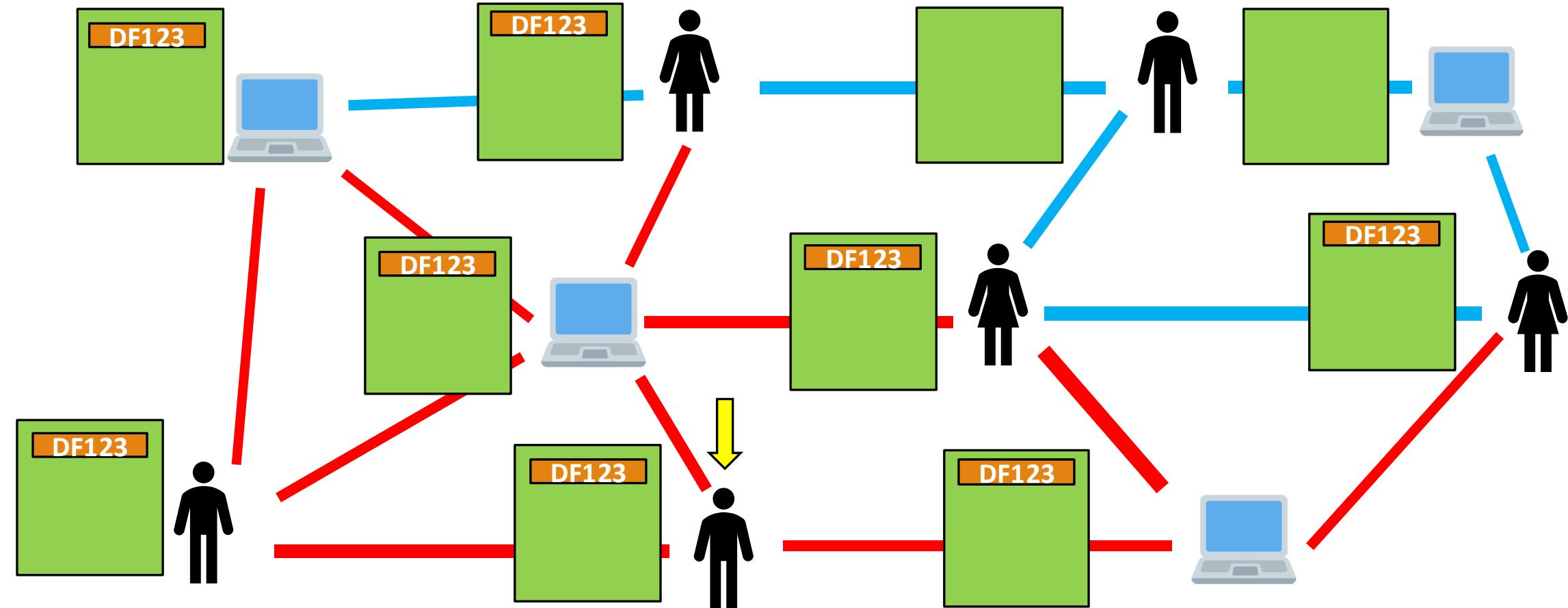
How do Mempool works?(Behind the scenes)



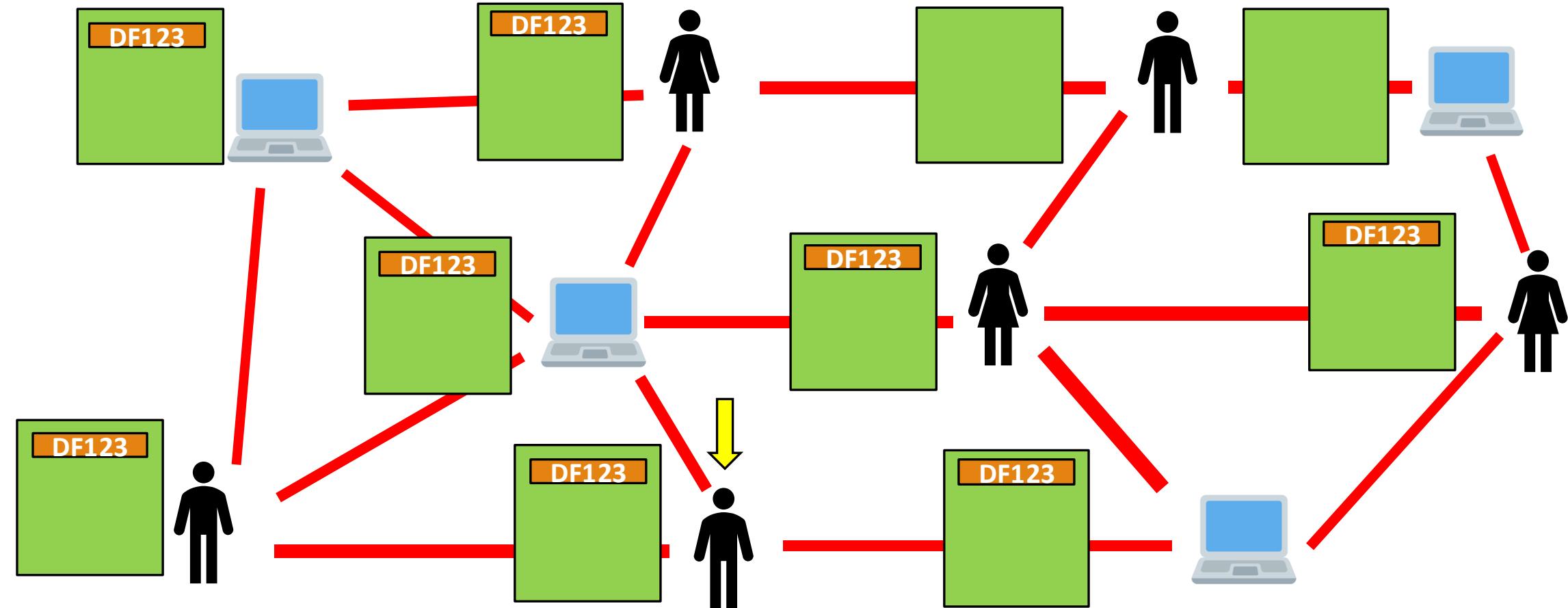
How do Mempool works?(Behind the scenes)



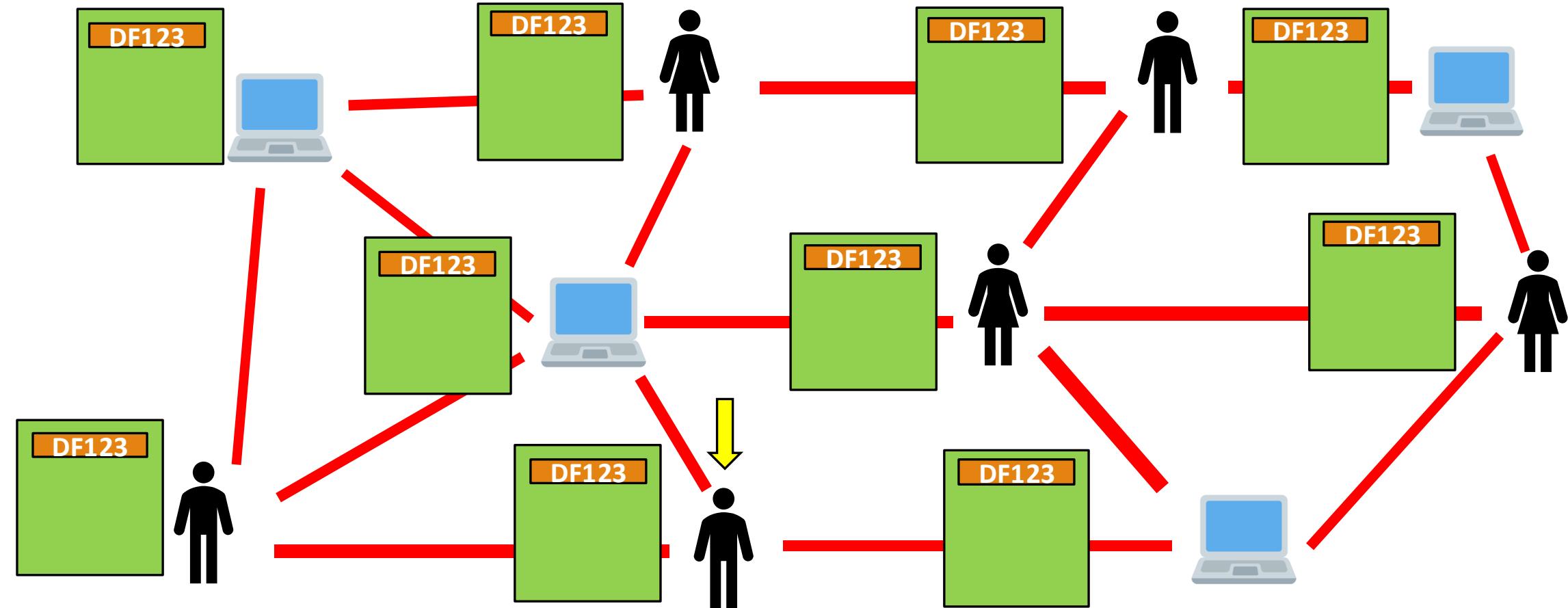
How do Mempool works?(Behind the scenes)



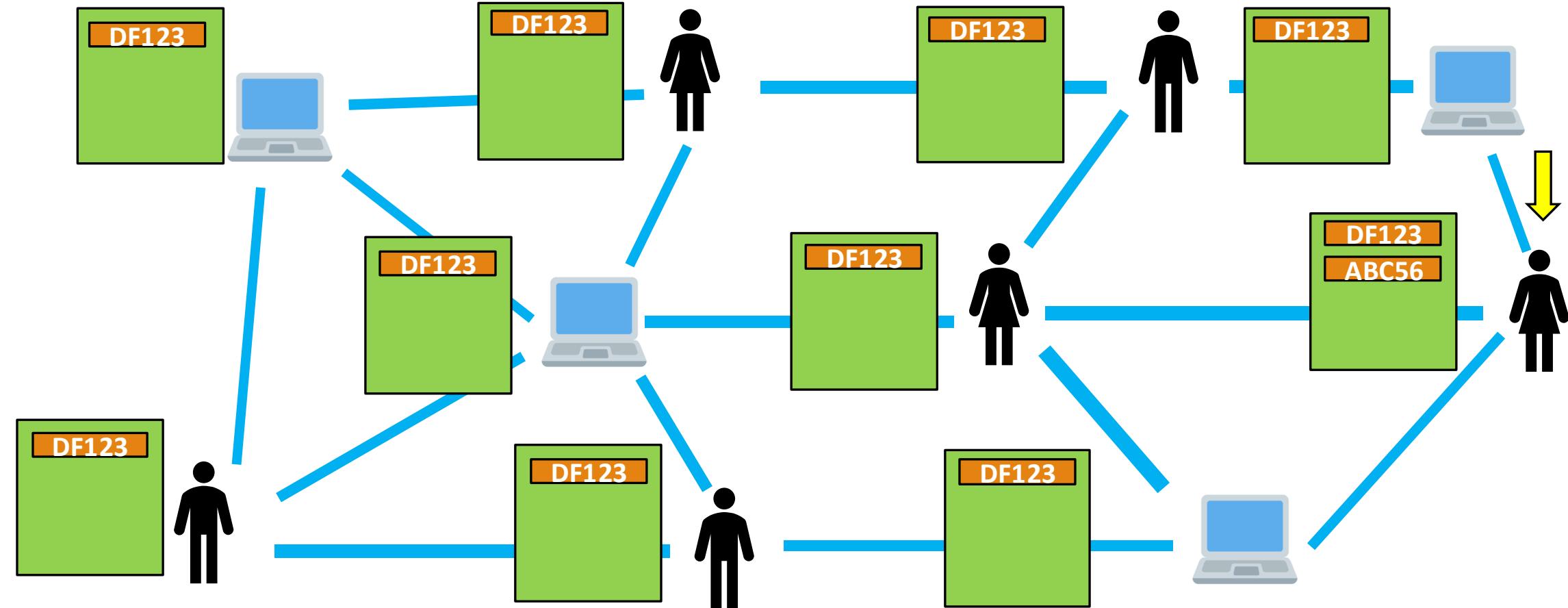
How do Mempool works?(Behind the scenes)



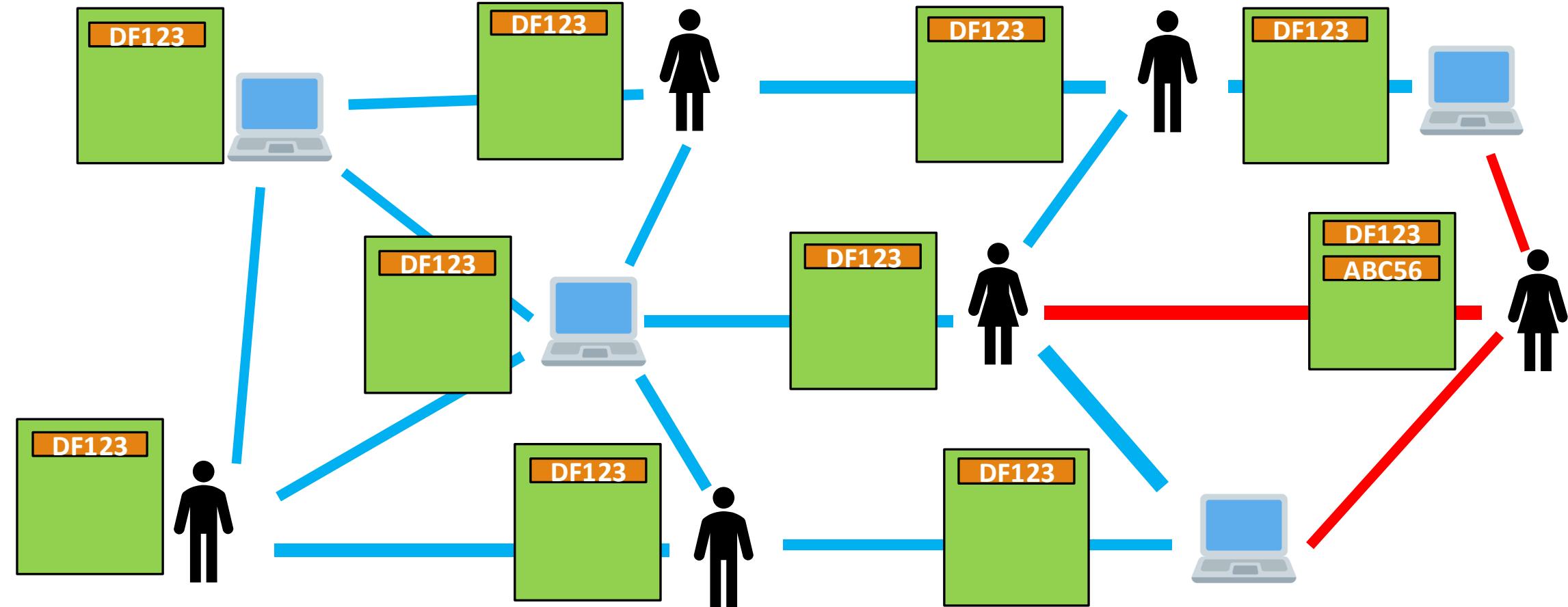
How do Mempool works?(Behind the scenes)



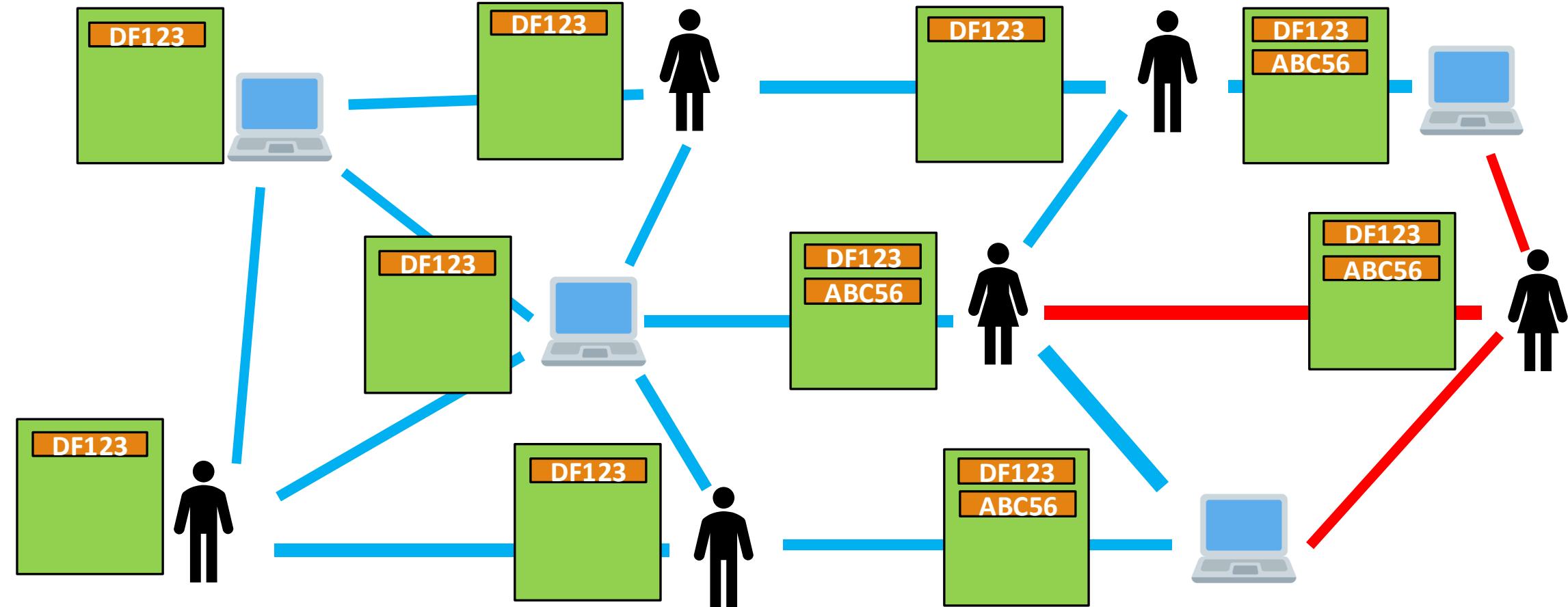
How do Mempool works?(Behind the scenes)



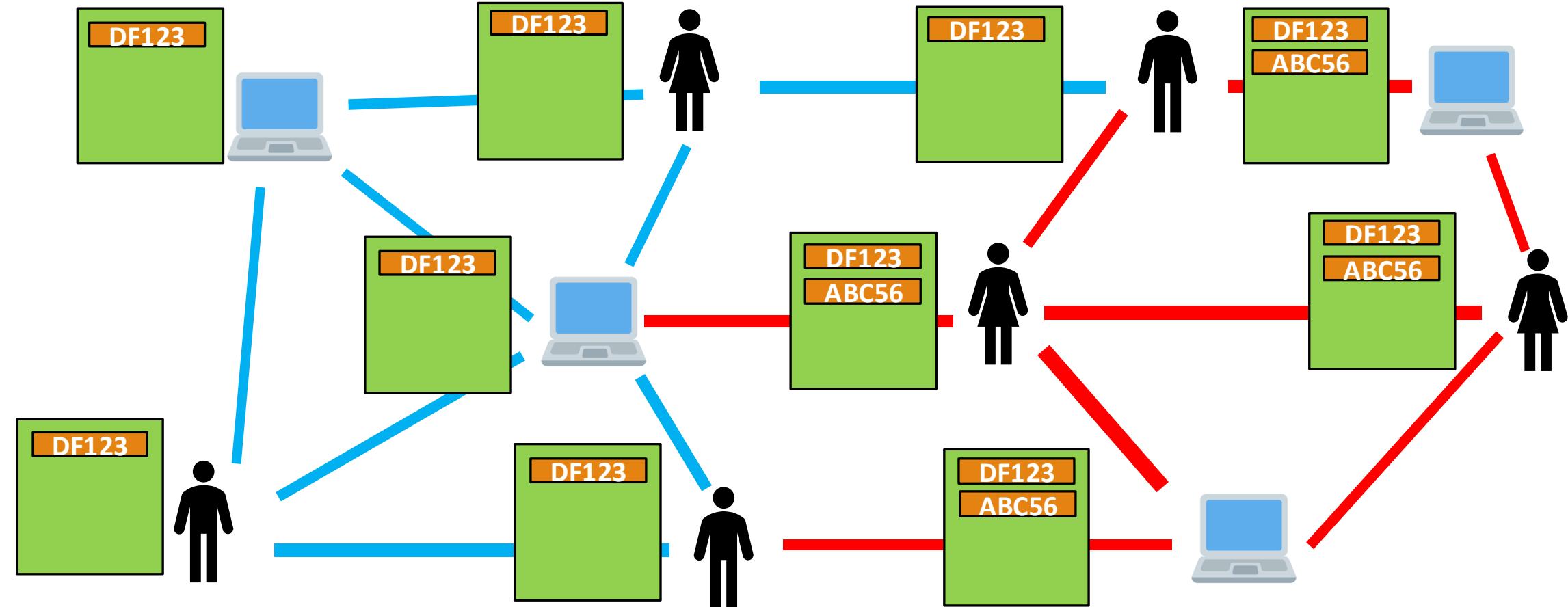
How do Mempool works?(Behind the scenes)



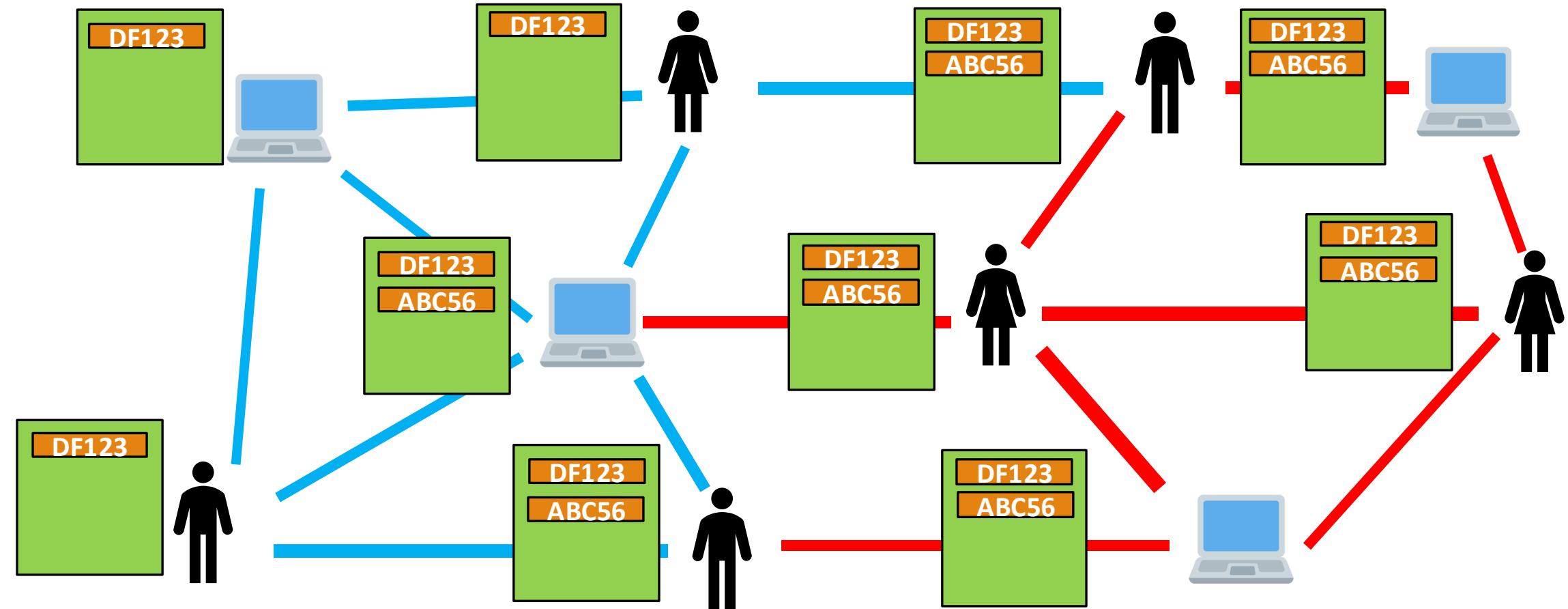
How do Mempool works?(Behind the scenes)



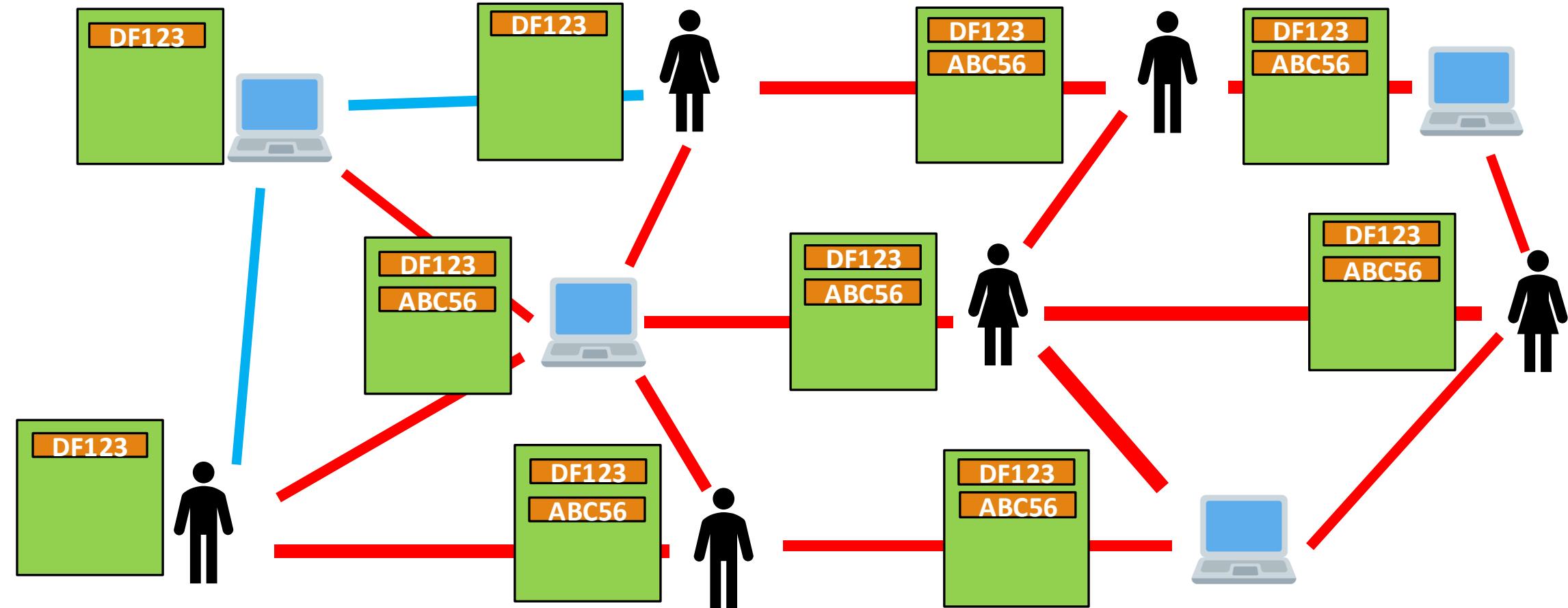
How do Mempool works?(Behind the scenes)



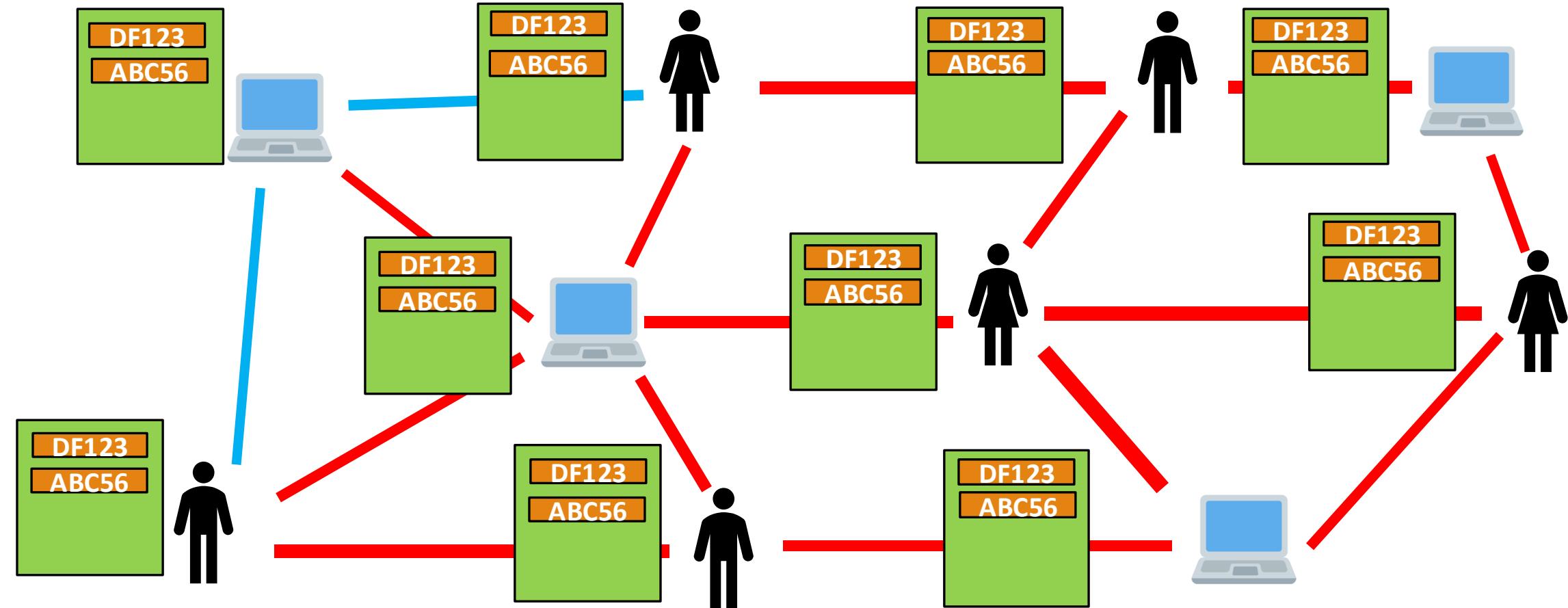
How do Mempool works?(Behind the scenes)



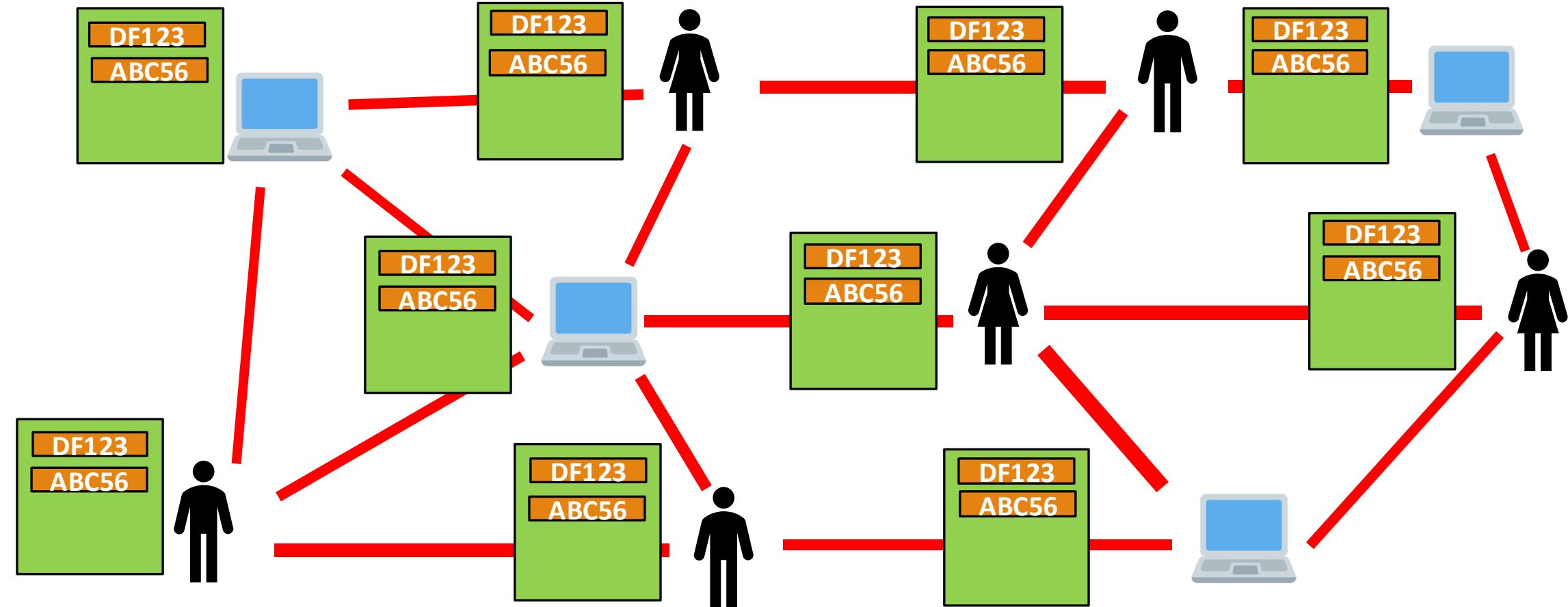
How do Mempool works?(Behind the scenes)



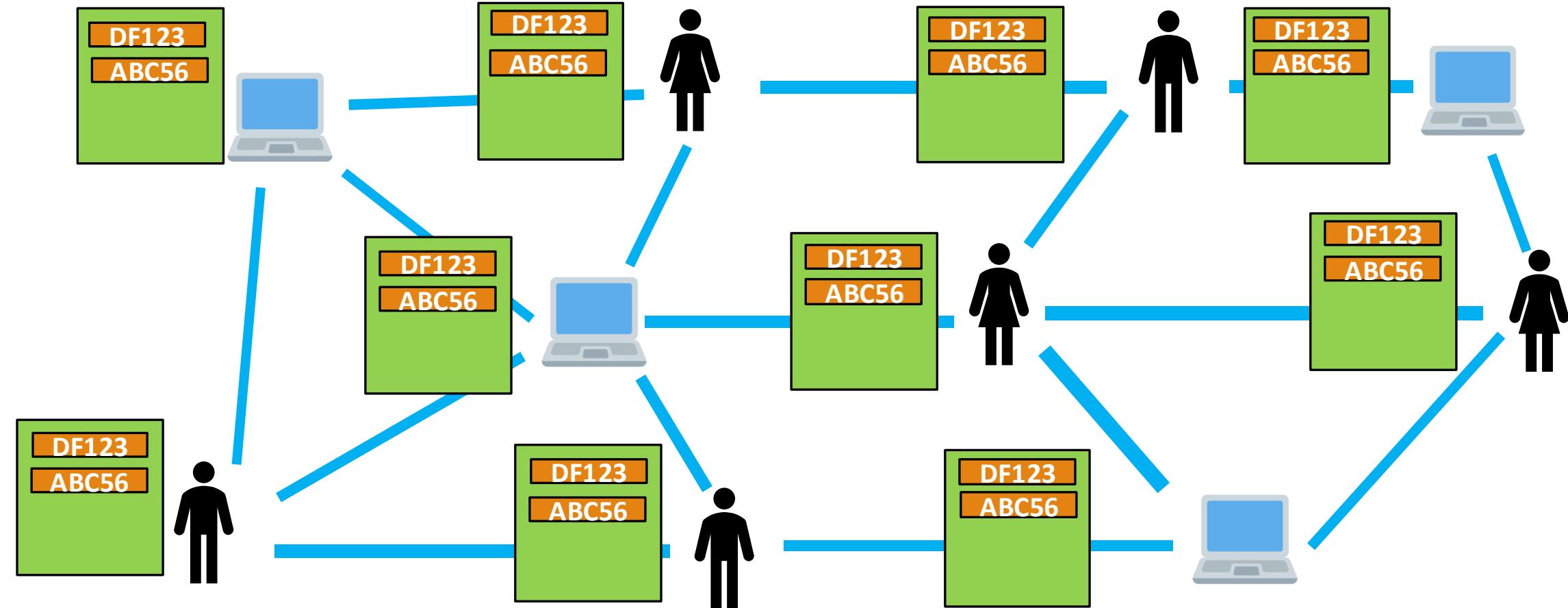
How do Mempool works?(Behind the scenes)

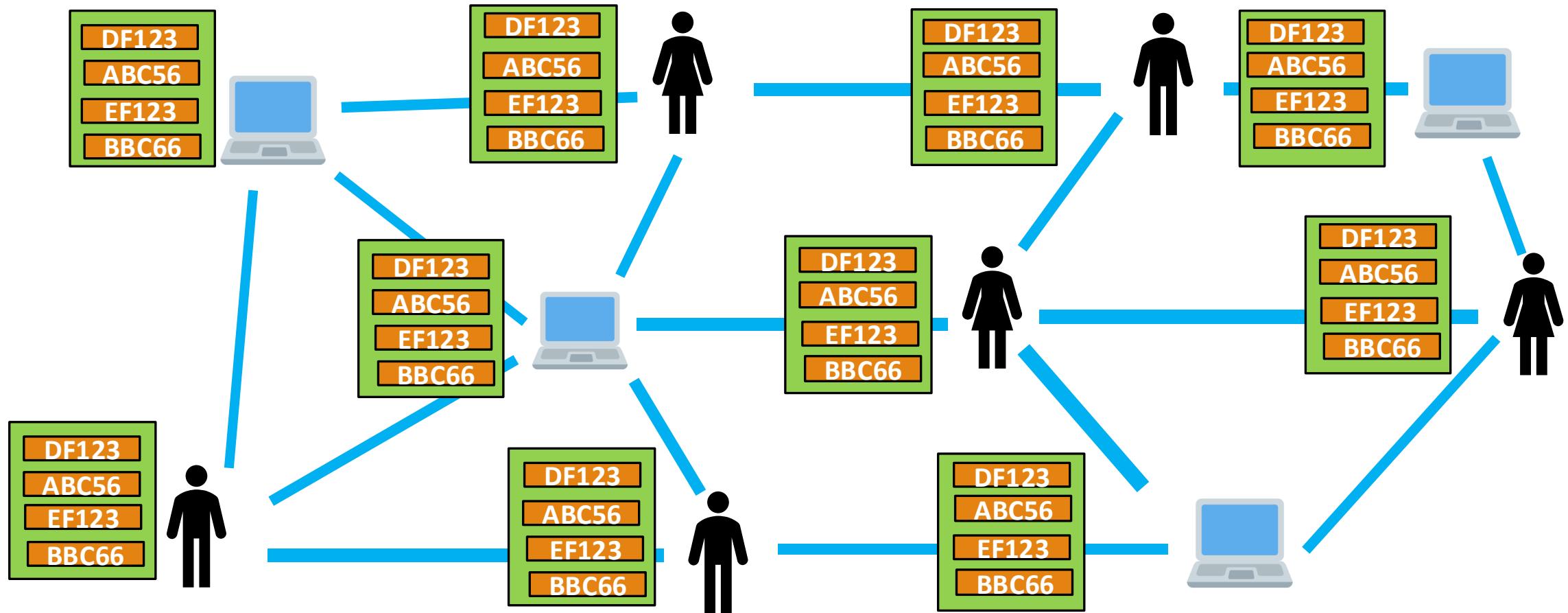


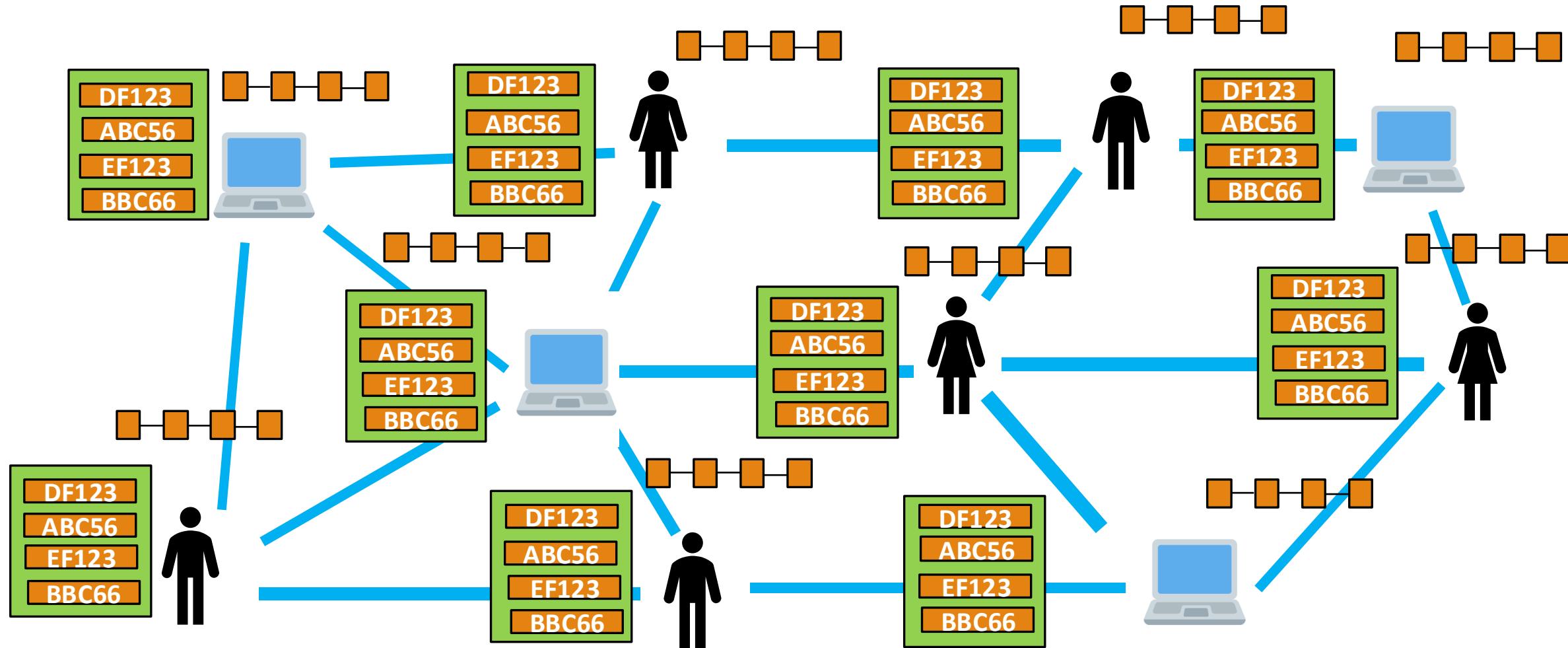
How do Mempool works?(Behind the scenes)

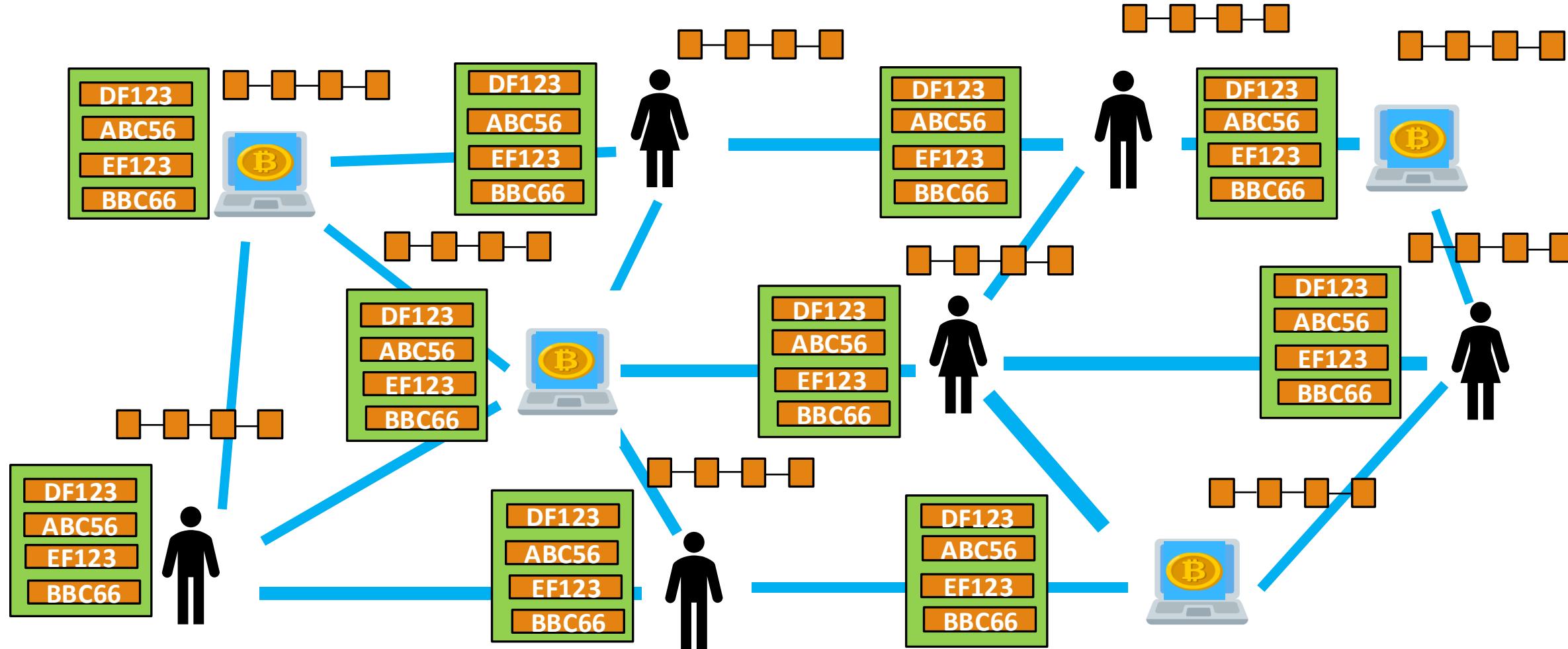


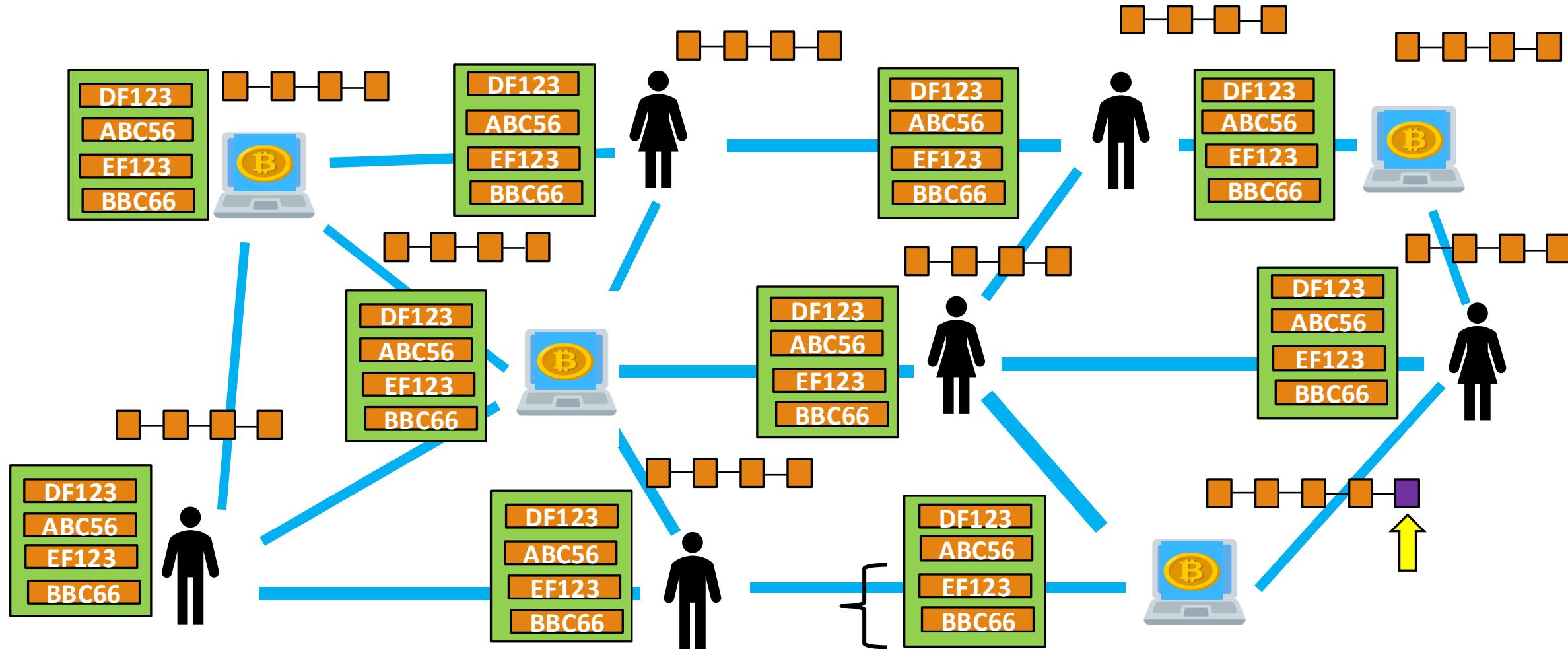
How do Mempool works?(Behind the scenes)

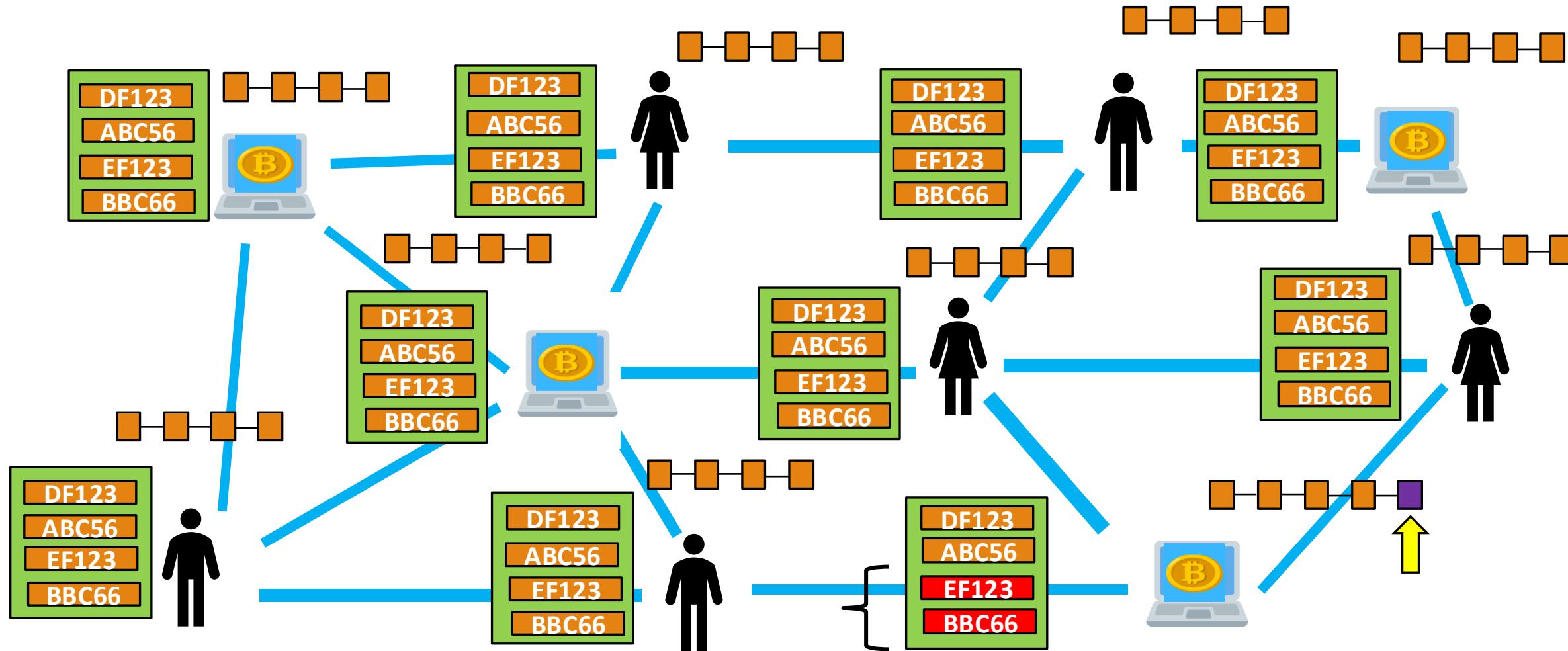


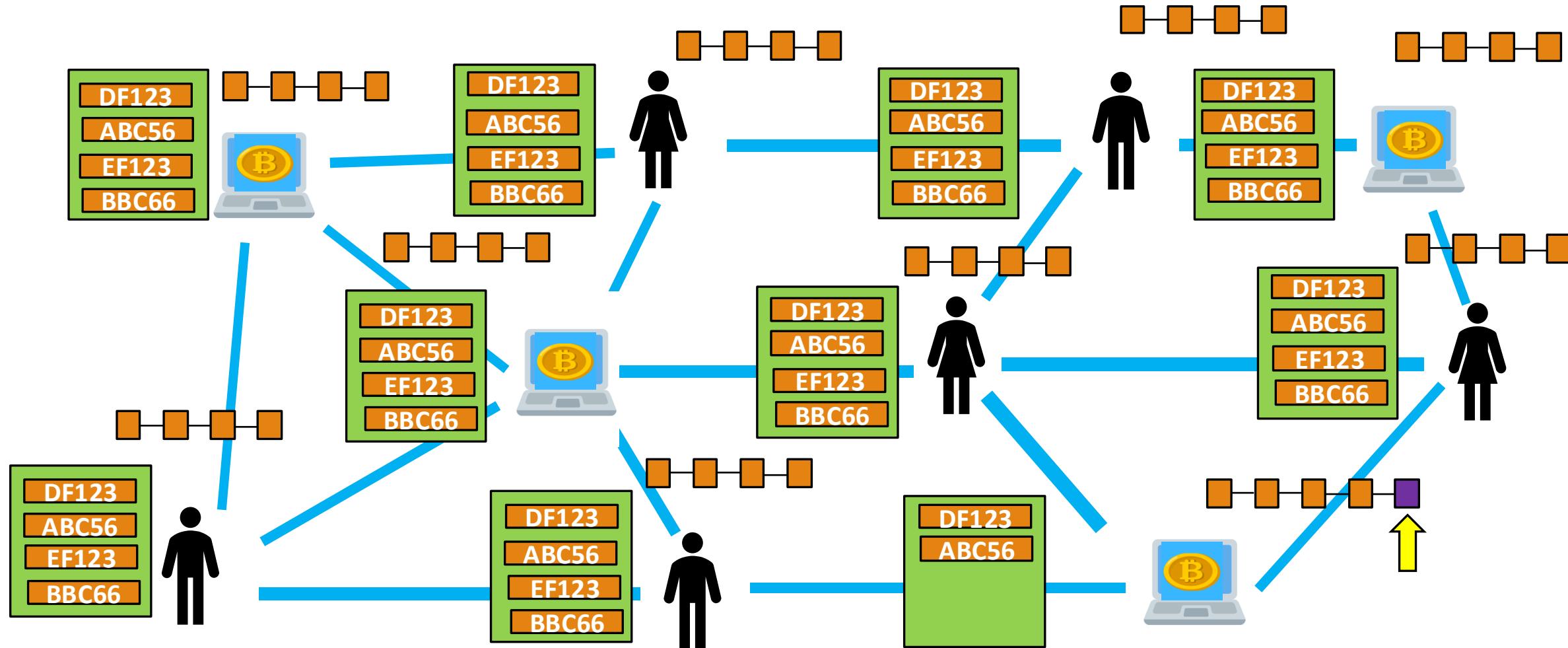


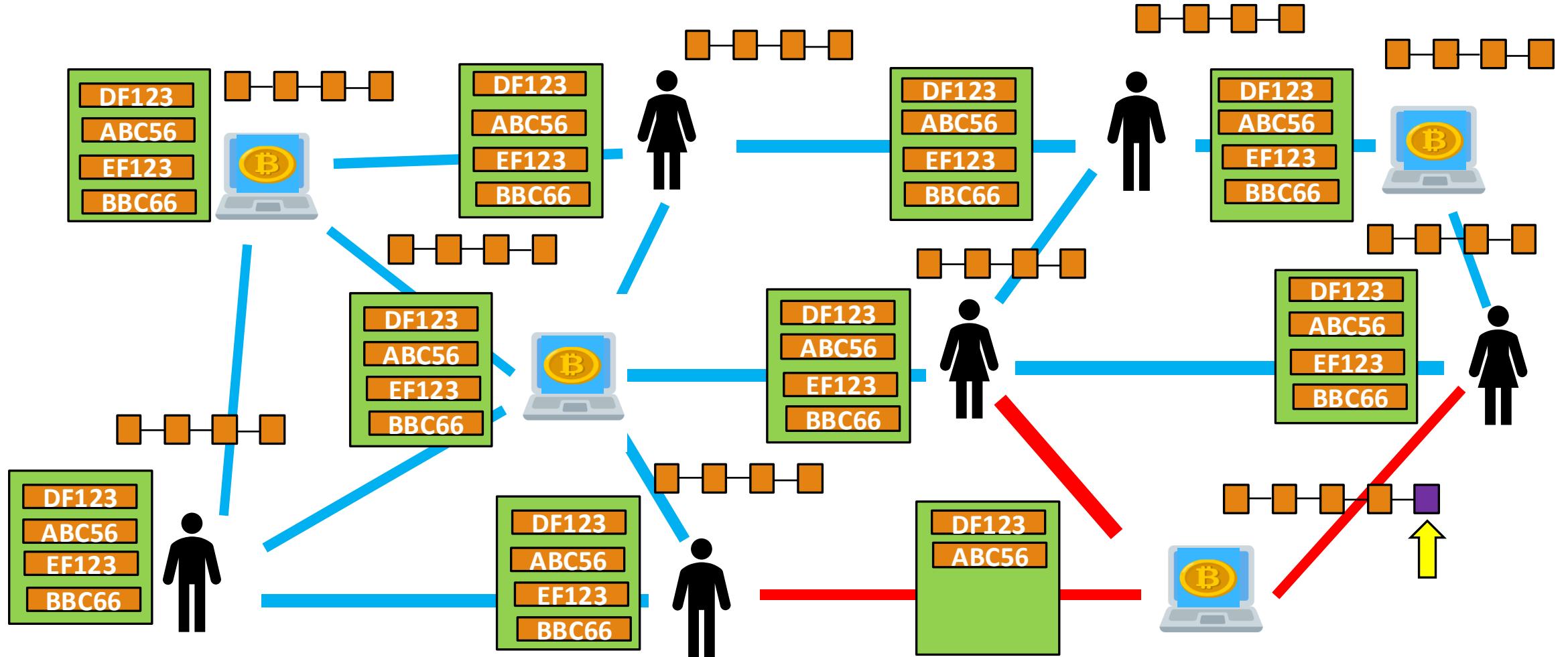


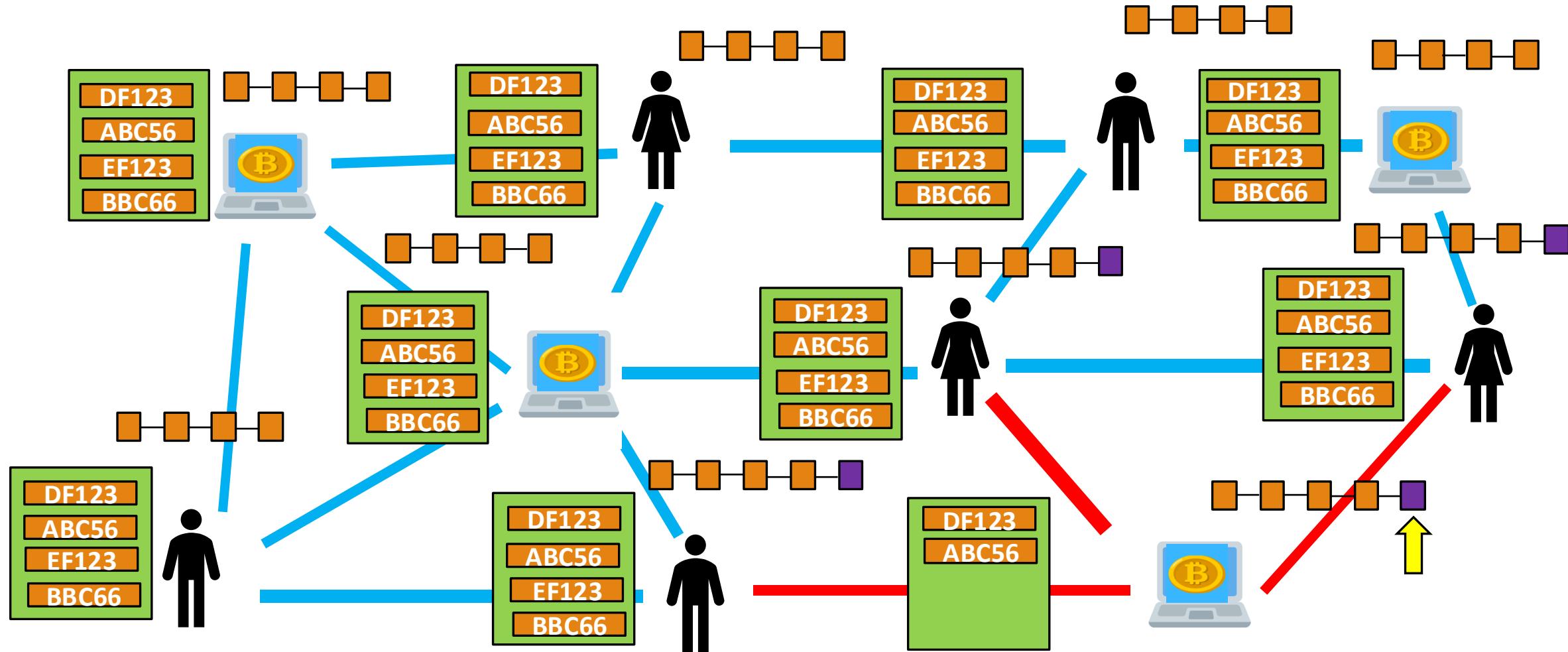


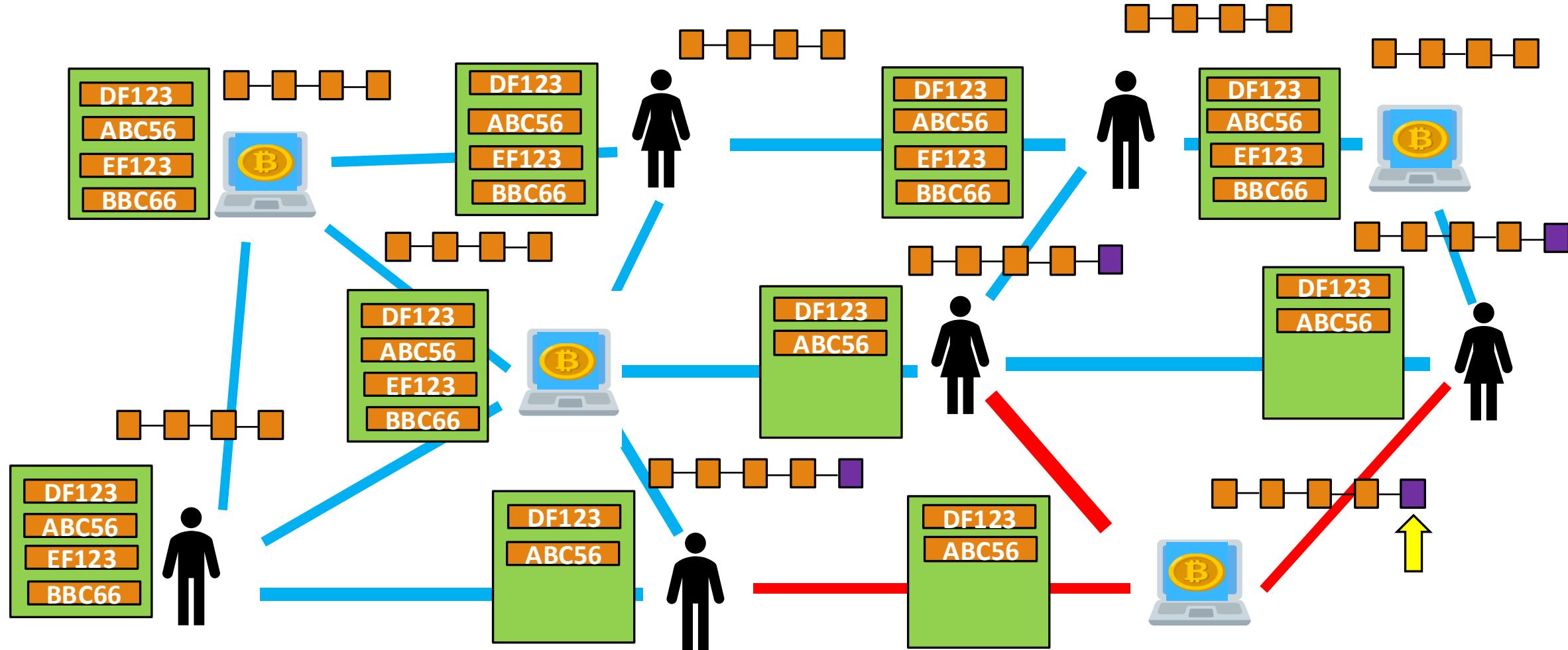


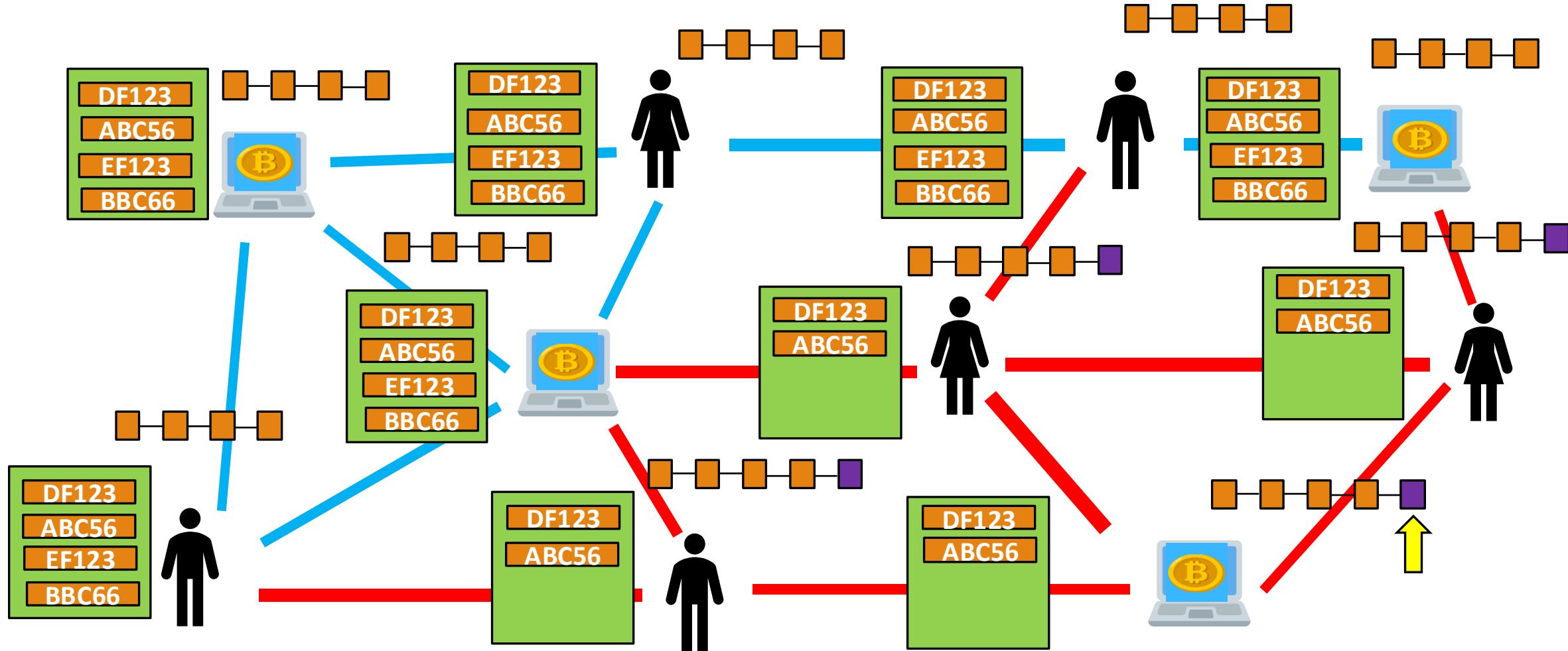


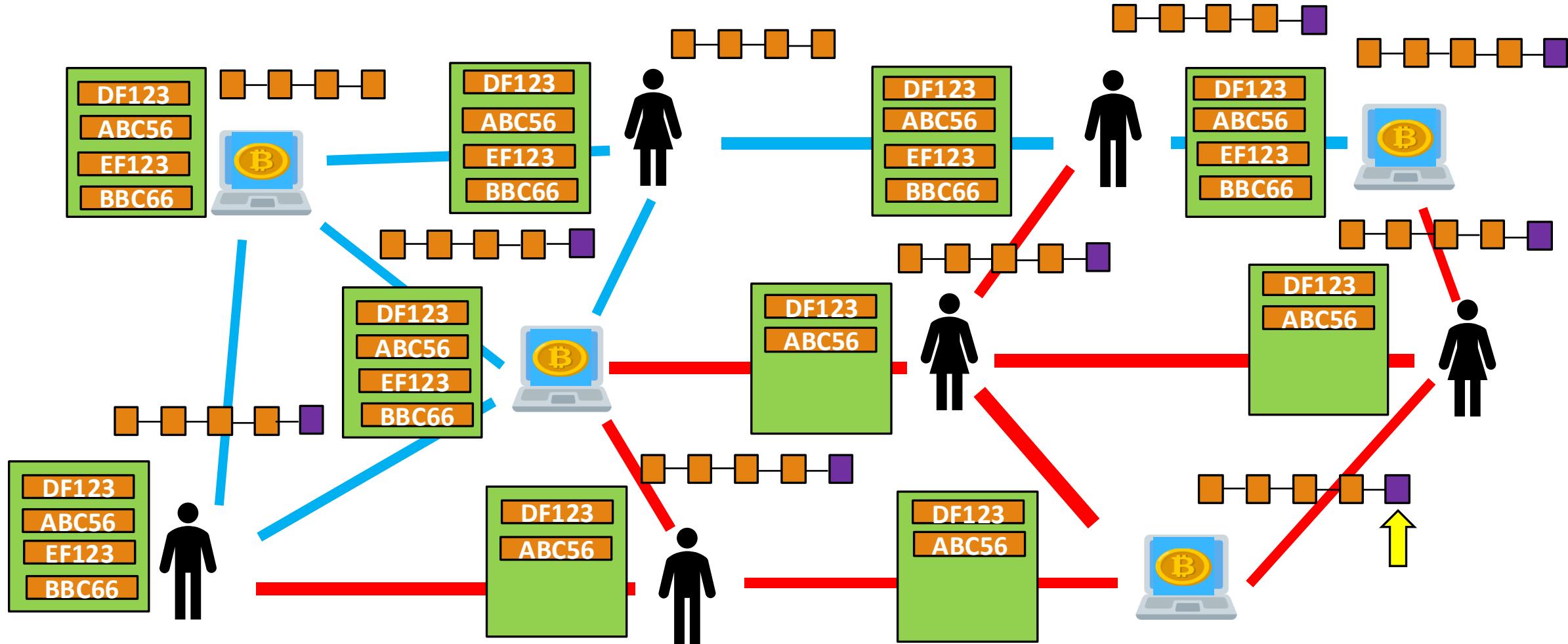


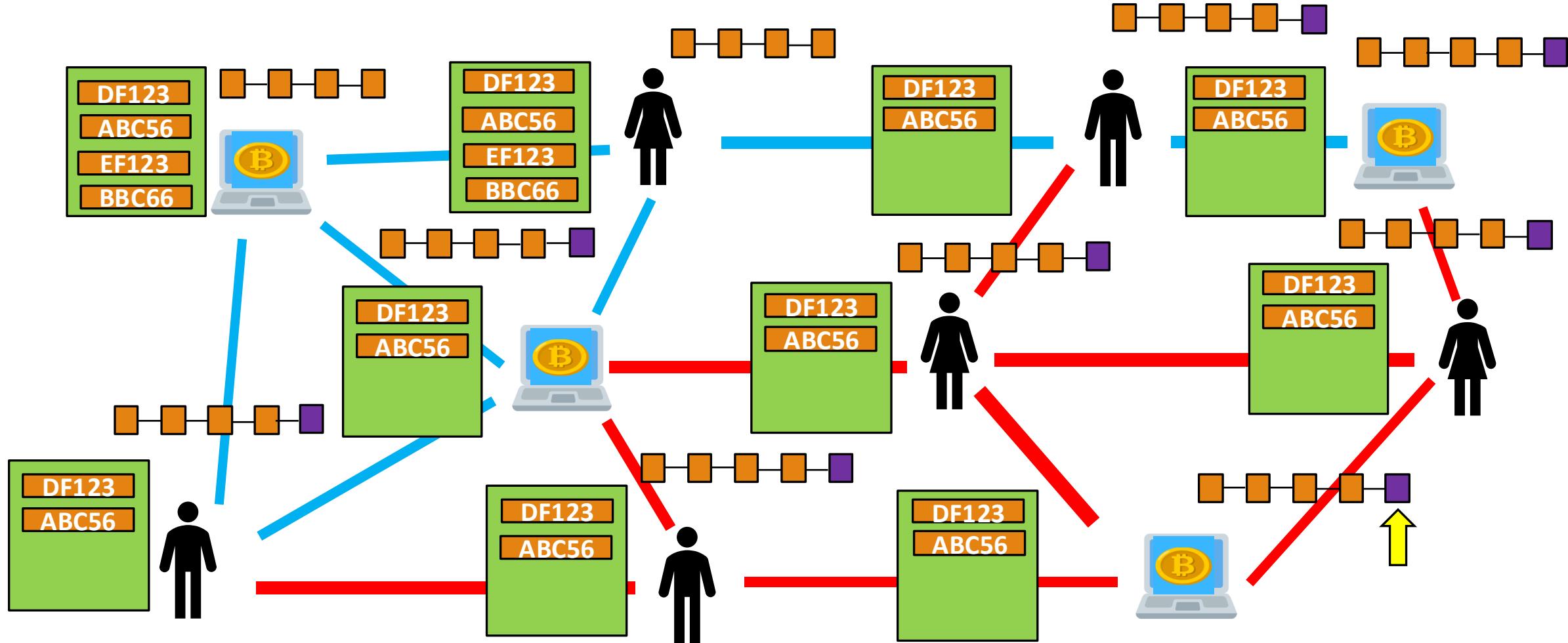


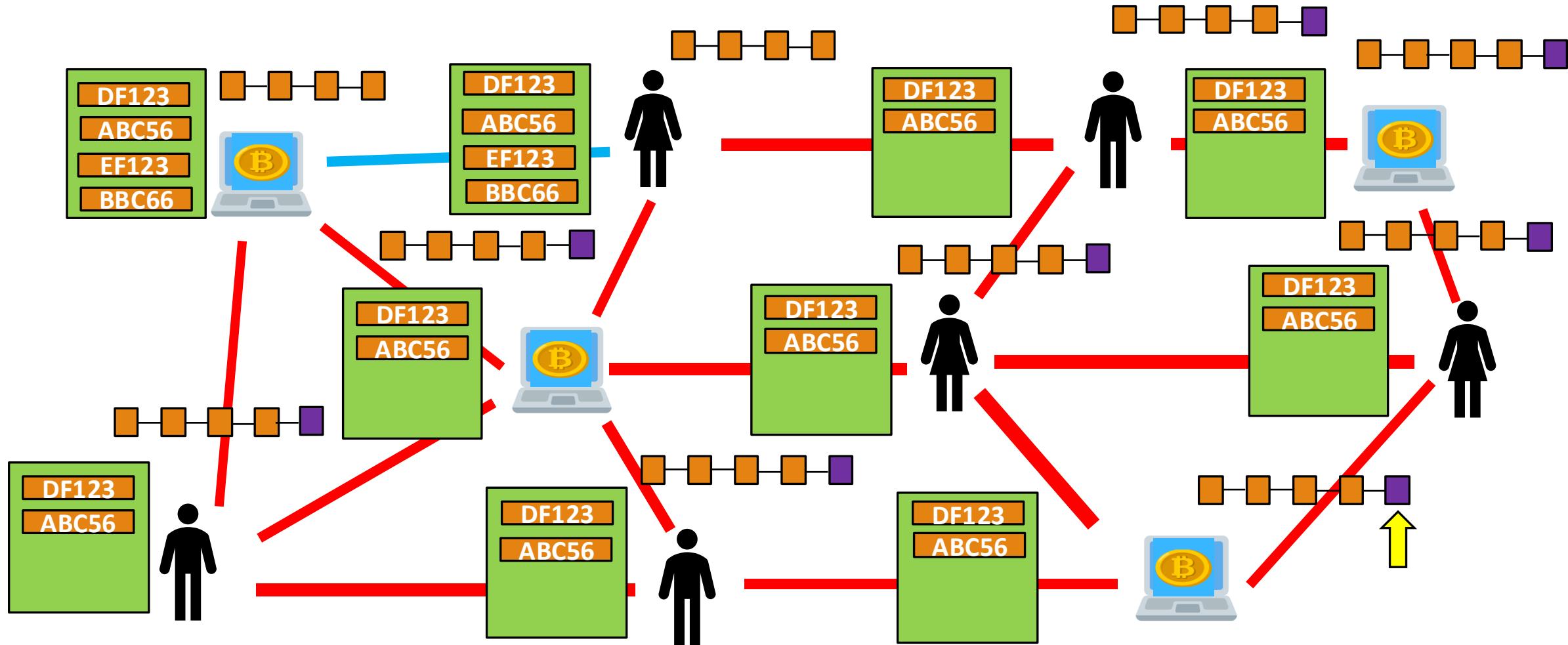


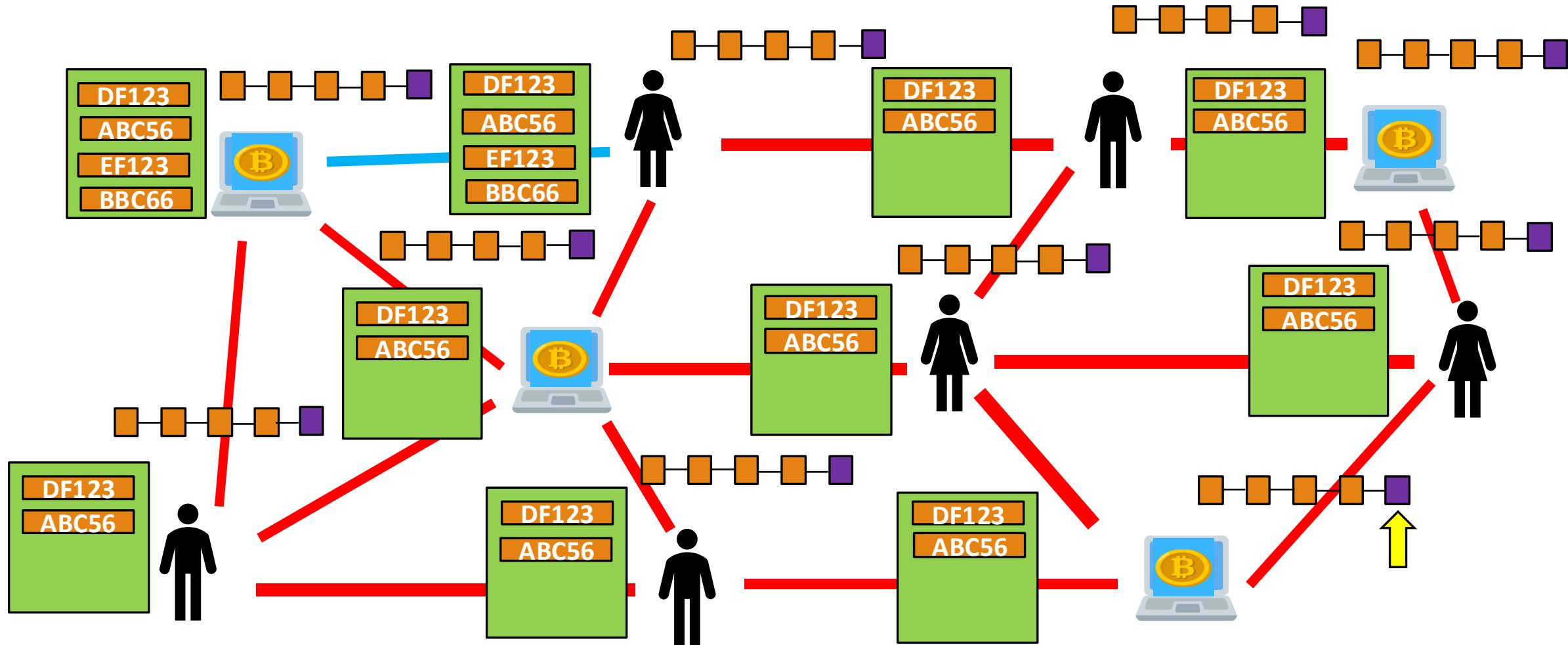


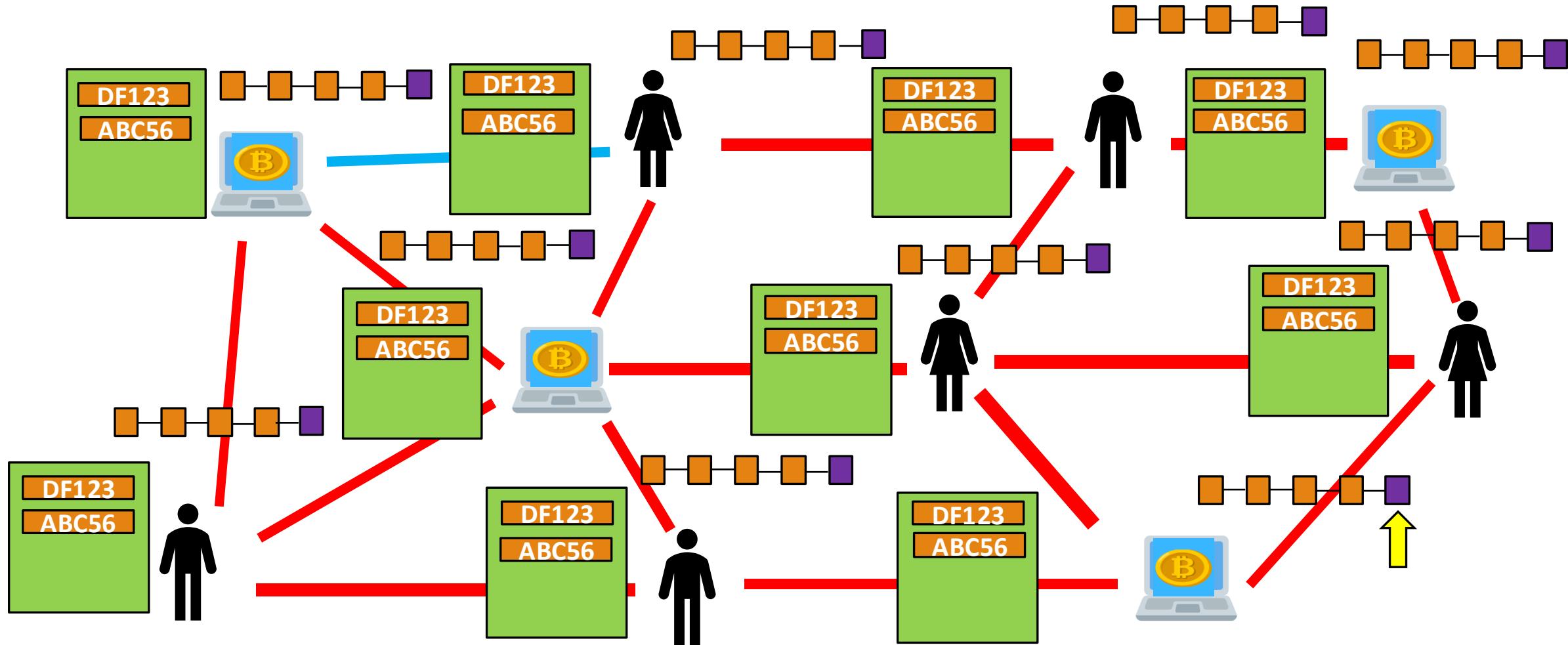


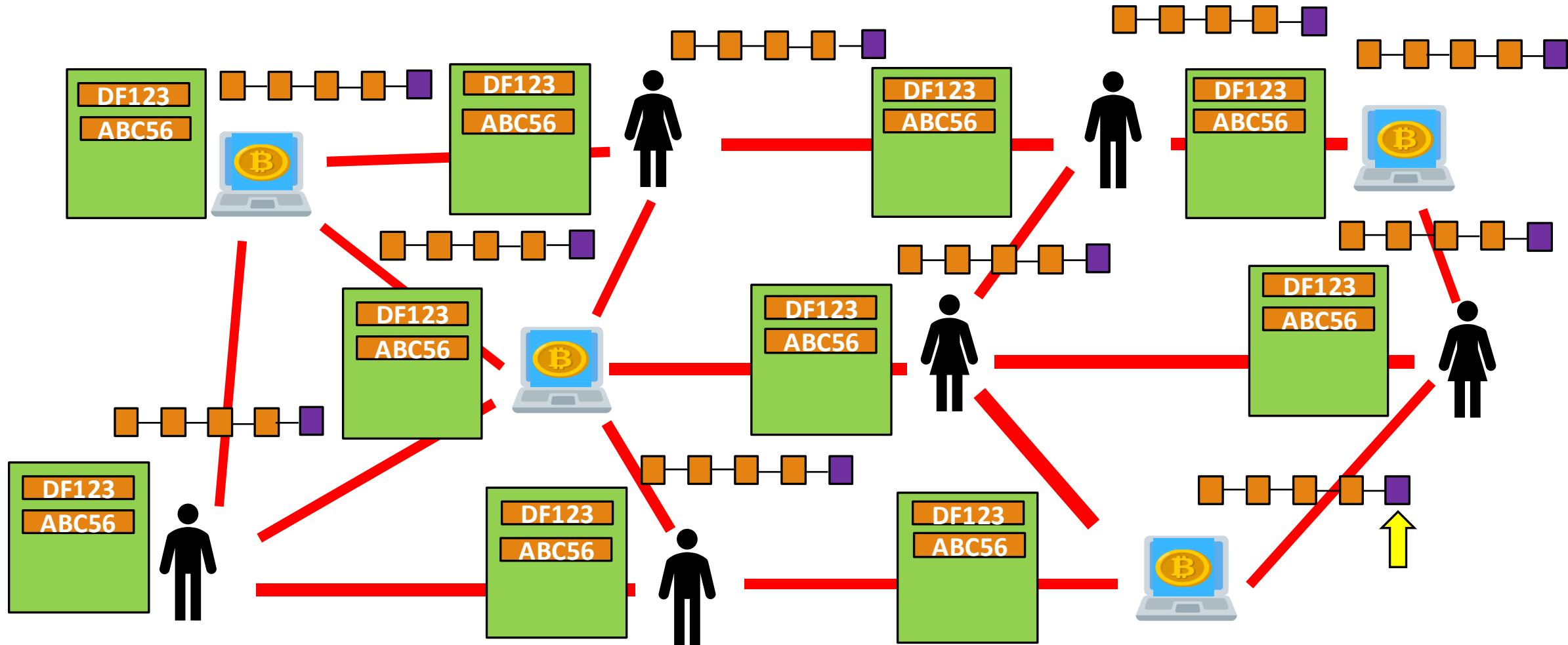


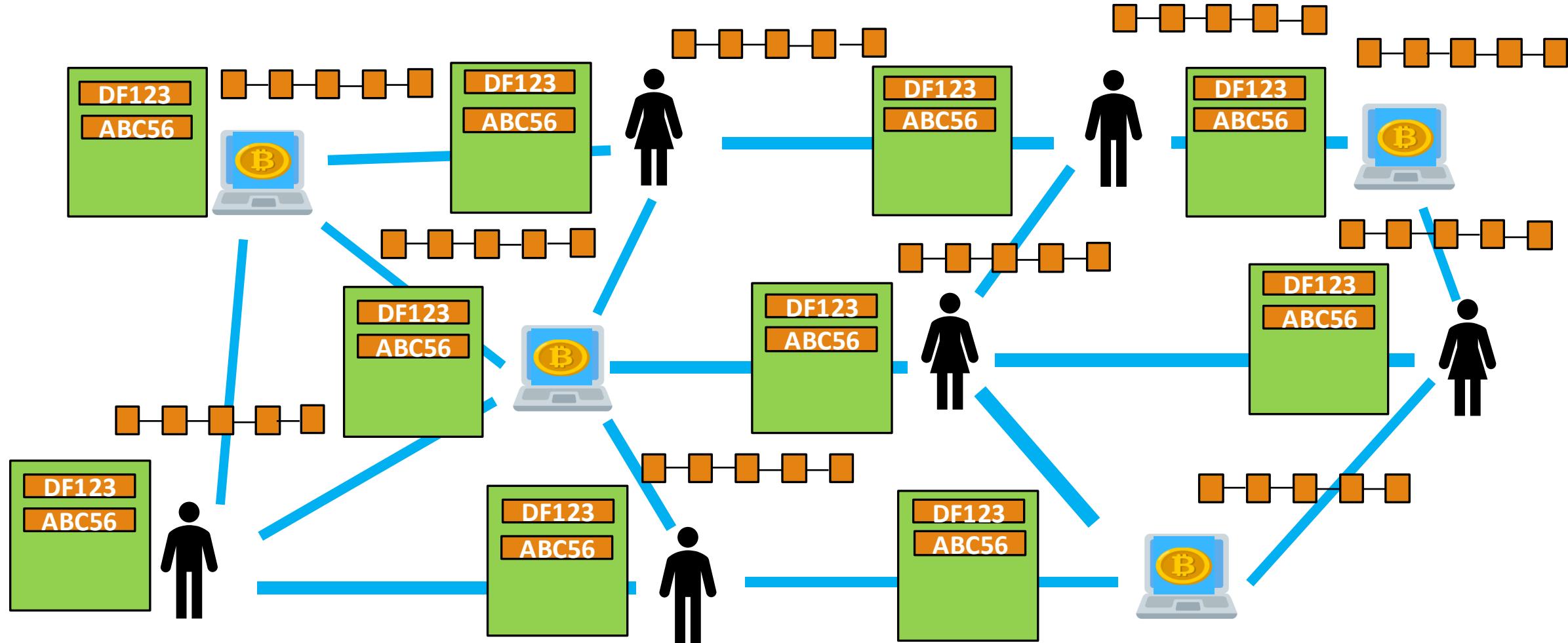






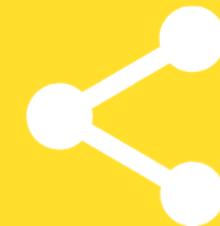






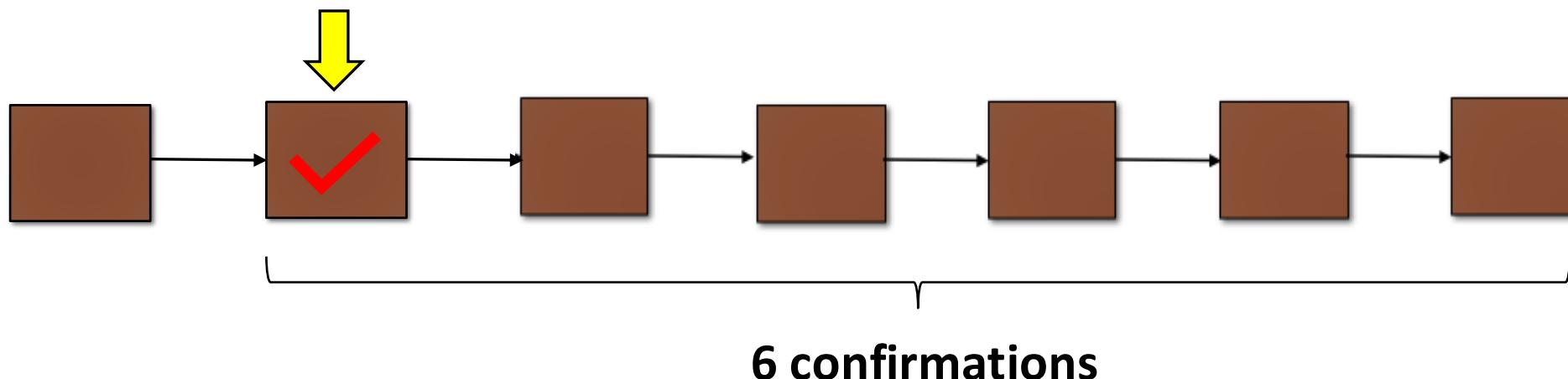
**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



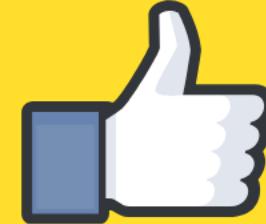
Orphaned Blocks

- It does not matter who minded the block first. The only thing that matters is who has the longest chain.
- Ideally wait for 6 confirmations before considering the transaction to be successful.

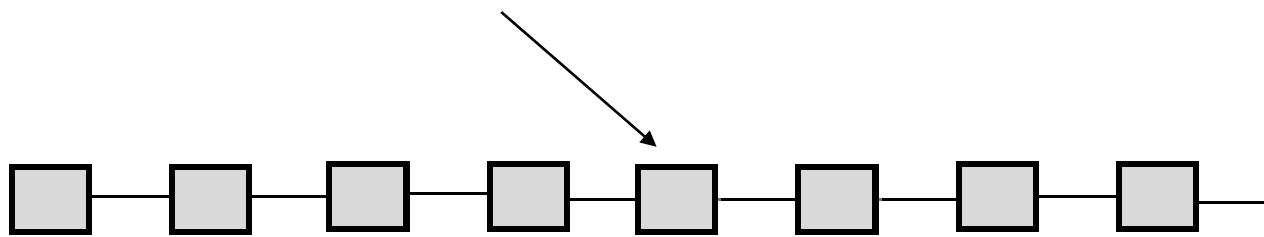


**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

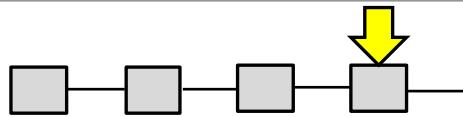


The 51% Attack

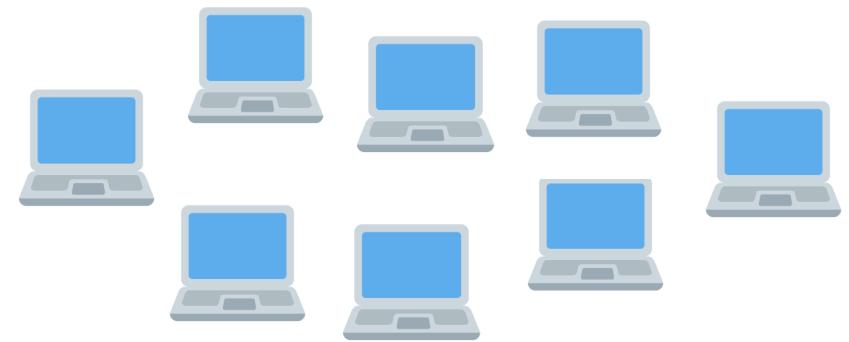
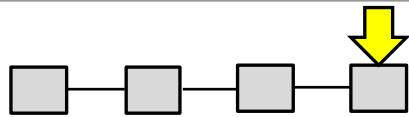


- The 51% attack is not about 51% of the network conspiracy against a single node as it is practically impossible.
- The 51% attack is about having the control over the hashing power.

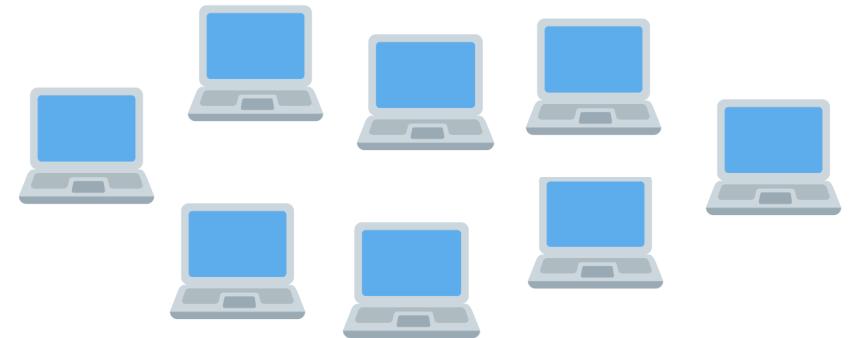
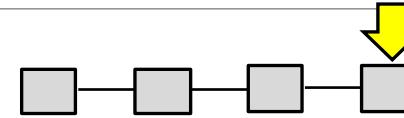
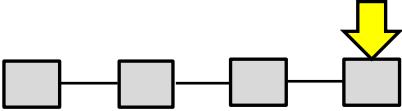
The 51% Attack



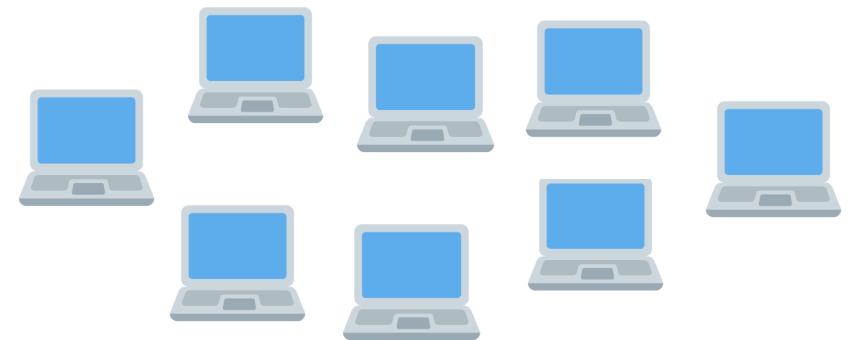
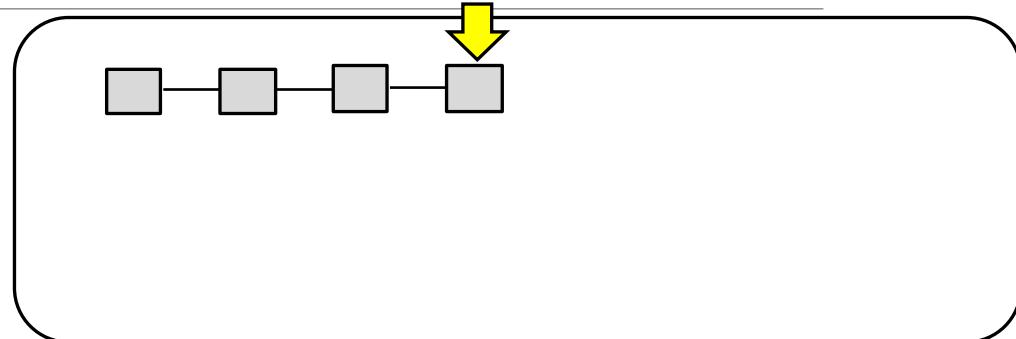
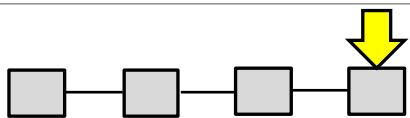
The 51% Attack



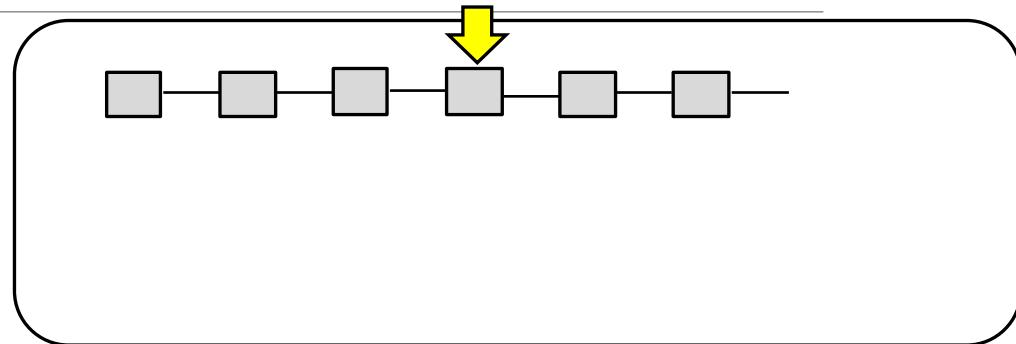
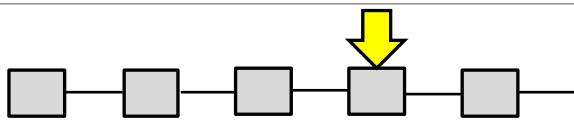
The 51% Attack



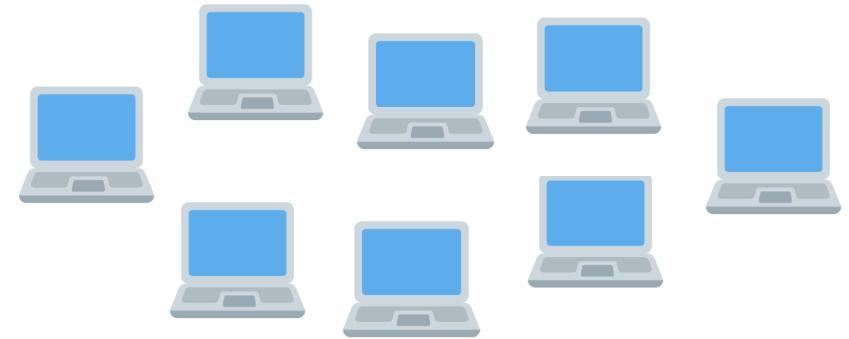
The 51% Attack



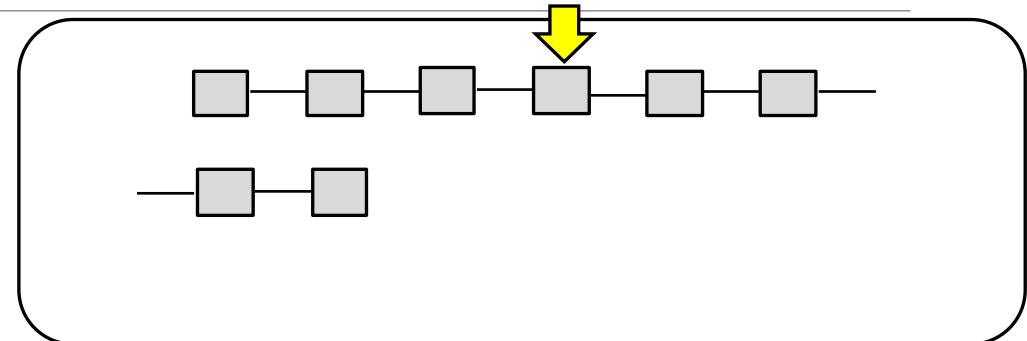
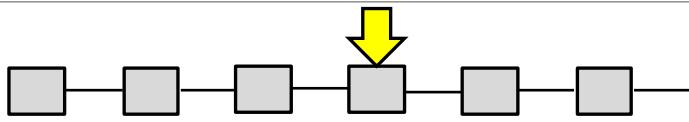
The 51% Attack



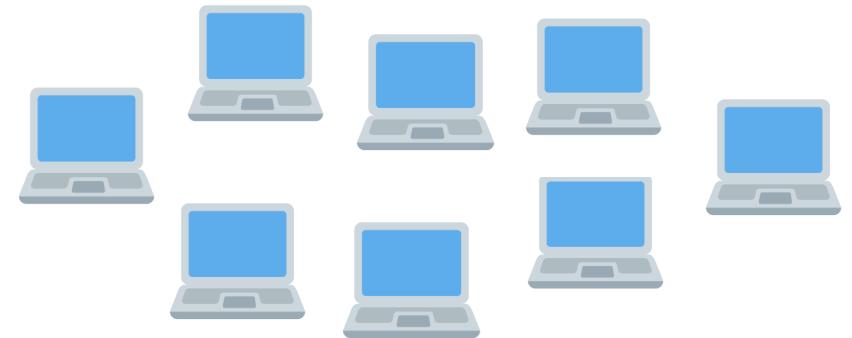
~~Broadcast~~



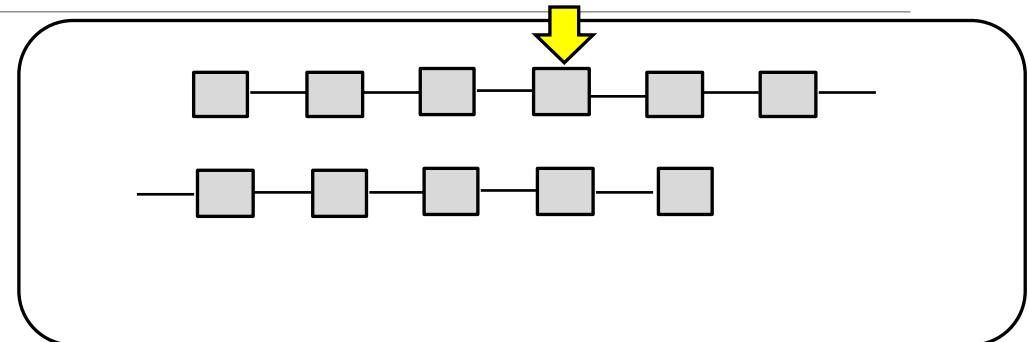
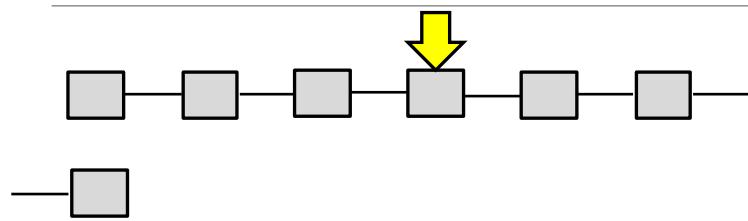
The 51% Attack



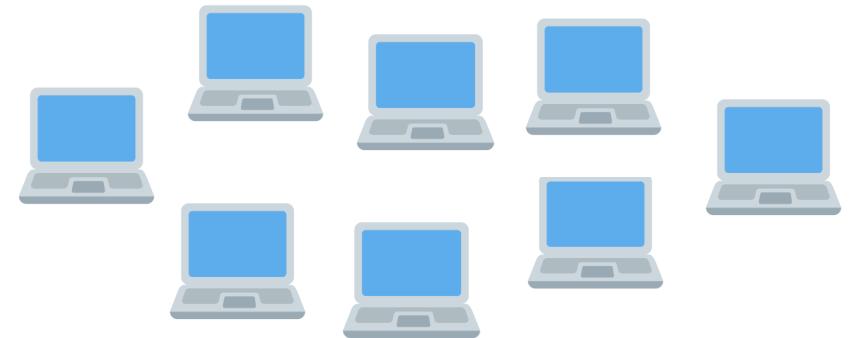
~~Broadcast~~



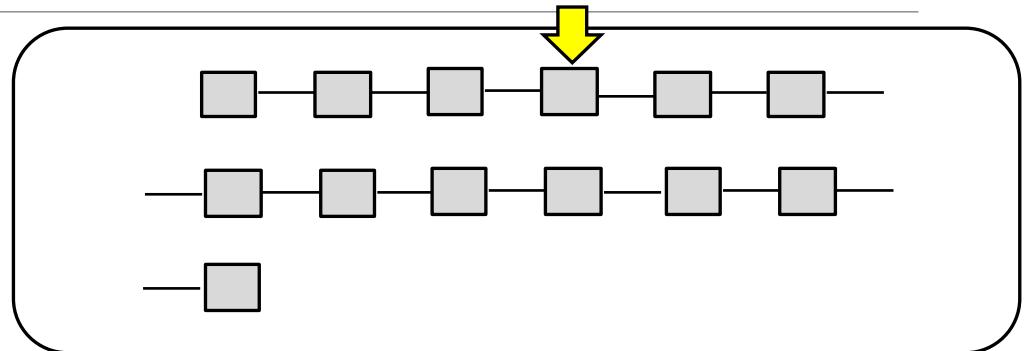
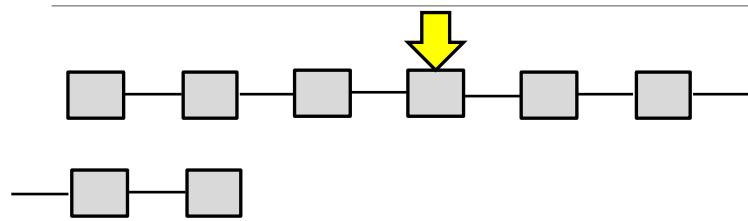
The 51% Attack



~~Broadcast~~



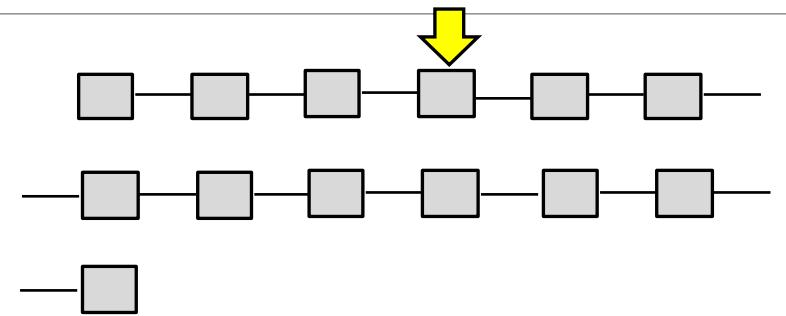
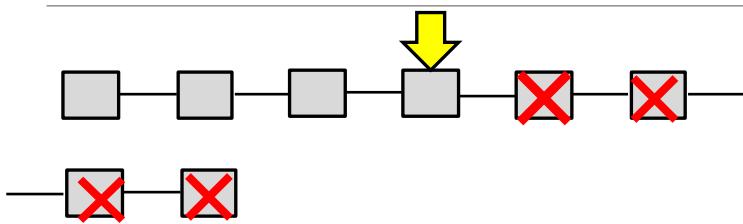
The 51% Attack



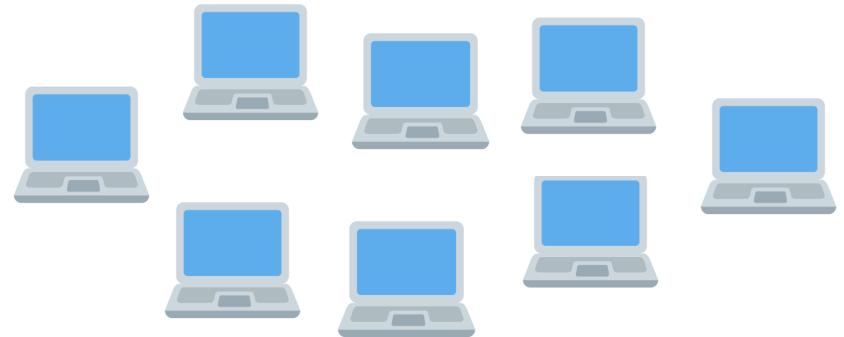
~~Broadcast~~



The 51% Attack



Broadcast



**GIVE THIS VIDEO
A THUMBS-UP !**

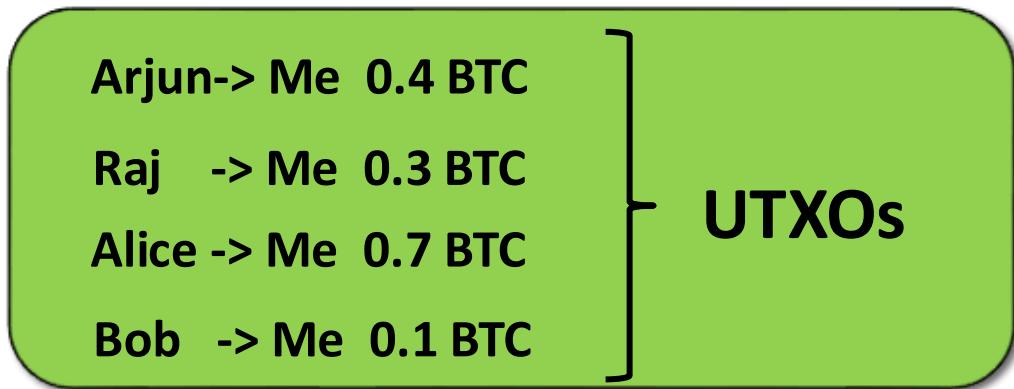
CODE EATER



A complex, abstract digital graphic serves as the background for the left half of the slide. It features a grid of blue and white squares, overlaid with several concentric circles. The innermost circle contains a series of binary digits (0s and 1s) arranged in a spiral pattern. The entire graphic has a dark, futuristic feel.

Transaction and UTXOs

Transaction and UTXOs



Let say I buy coffee for 0.5 BTC.



Transaction :

Input:

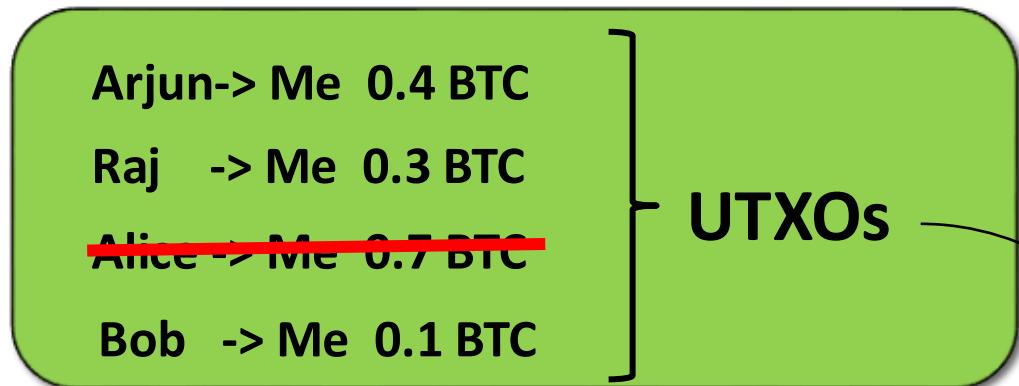
0.7 BTC from Alice

Output:

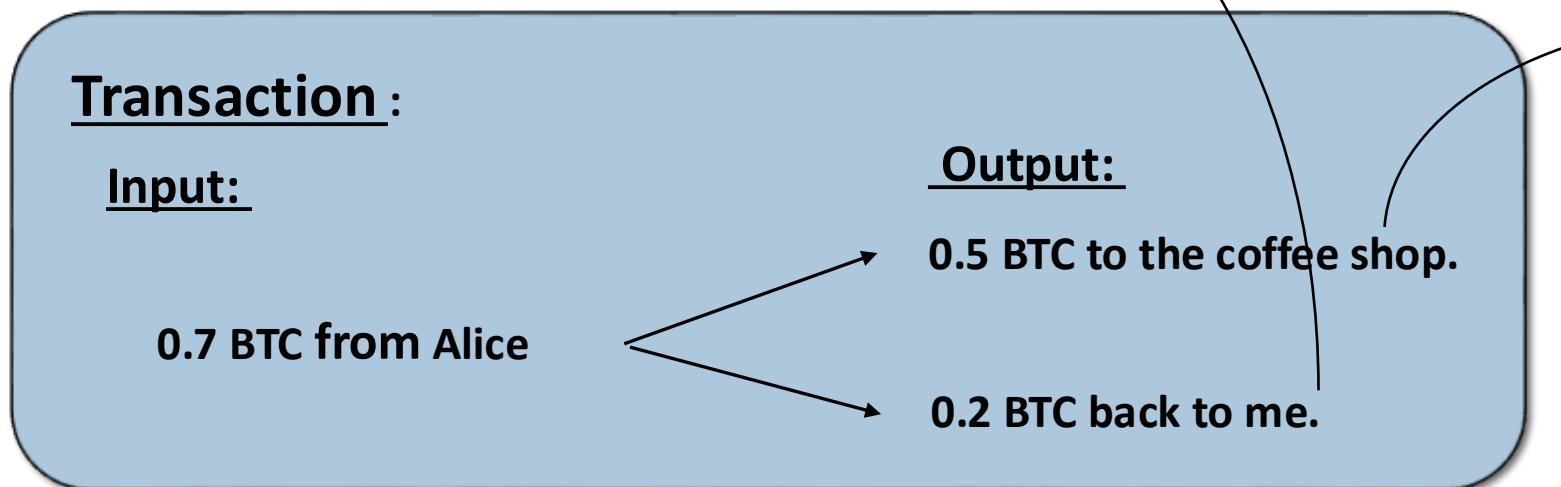
0.5 BTC to the coffee shop.

0.2 BTC back to me.

Transaction and UTXOs

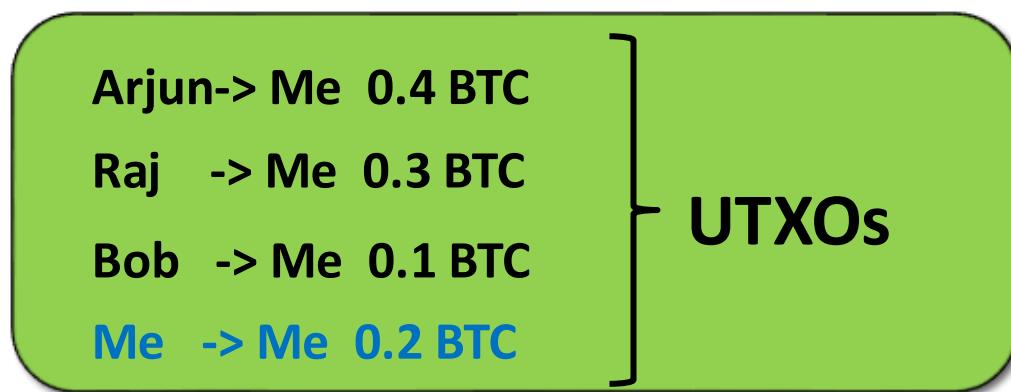


Let say I buy coffee for 0.5 BTC.

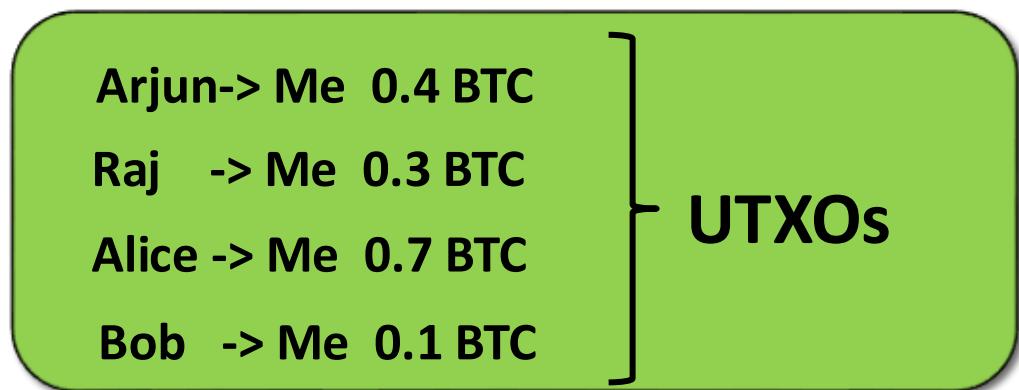


UTXO for the coffee shop.

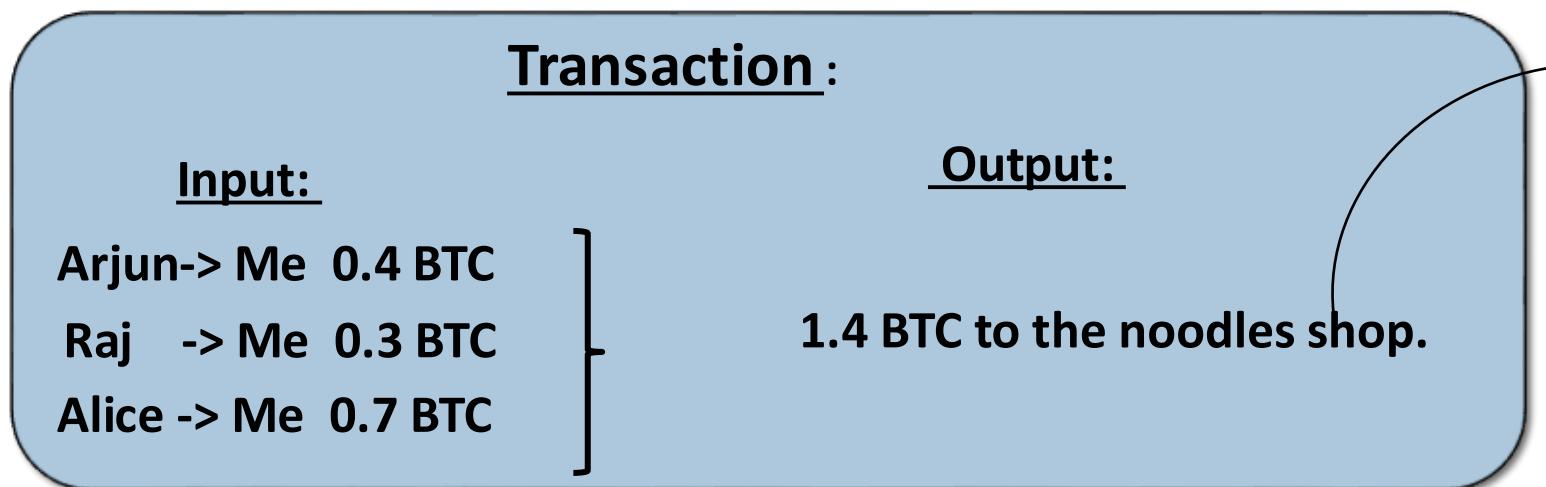
Transaction and UTXOs



Transaction and UTXOs



Let say I buy Noodles for 1.4 BTC.

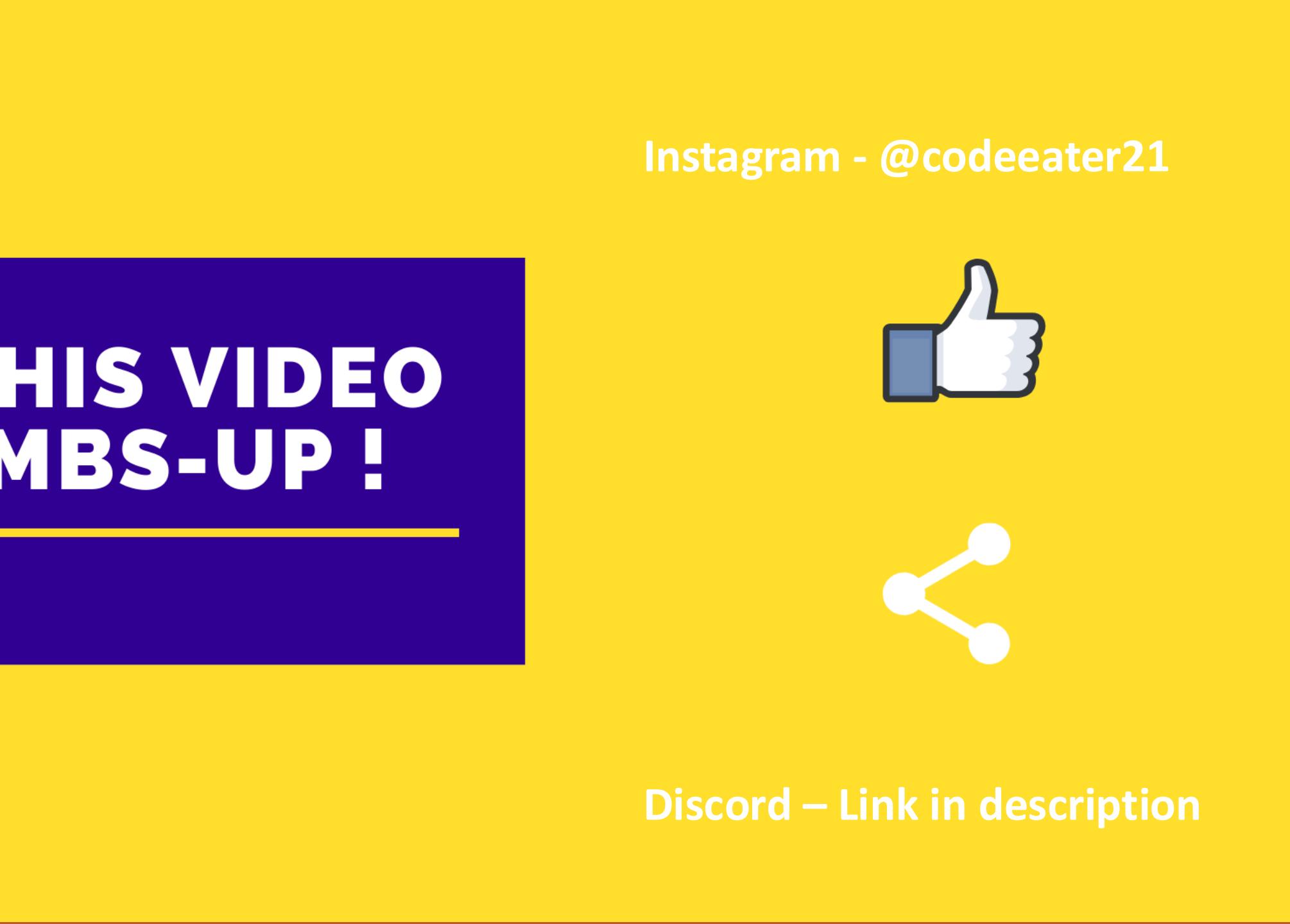


UTXO for the noodle shop.

Transaction and UTXOs

Bob → Me 0.1 BTC } UTXOs





GIVE THIS VIDEO A THUMBS-UP !

CODE EATER

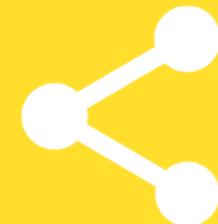
Instagram - @codeeater21



Discord – Link in description

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



A complex, abstract digital graphic serves as the background for the left half of the slide. It features a grid of blue squares and a circular interface with binary code (0s and 1s) displayed along its perimeter and in the center. The overall aesthetic is futuristic and technical.

Transaction Fee

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.

0.2 BTC back to me.

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.

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

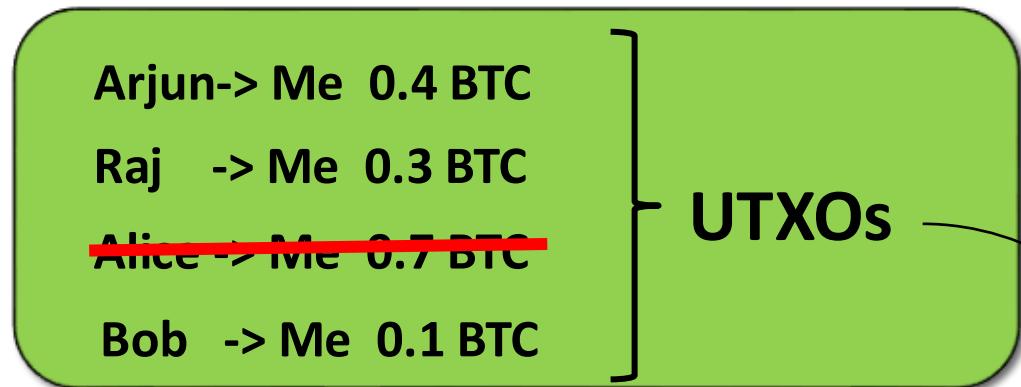
Output:

0.5 BTC to the coffee shop.

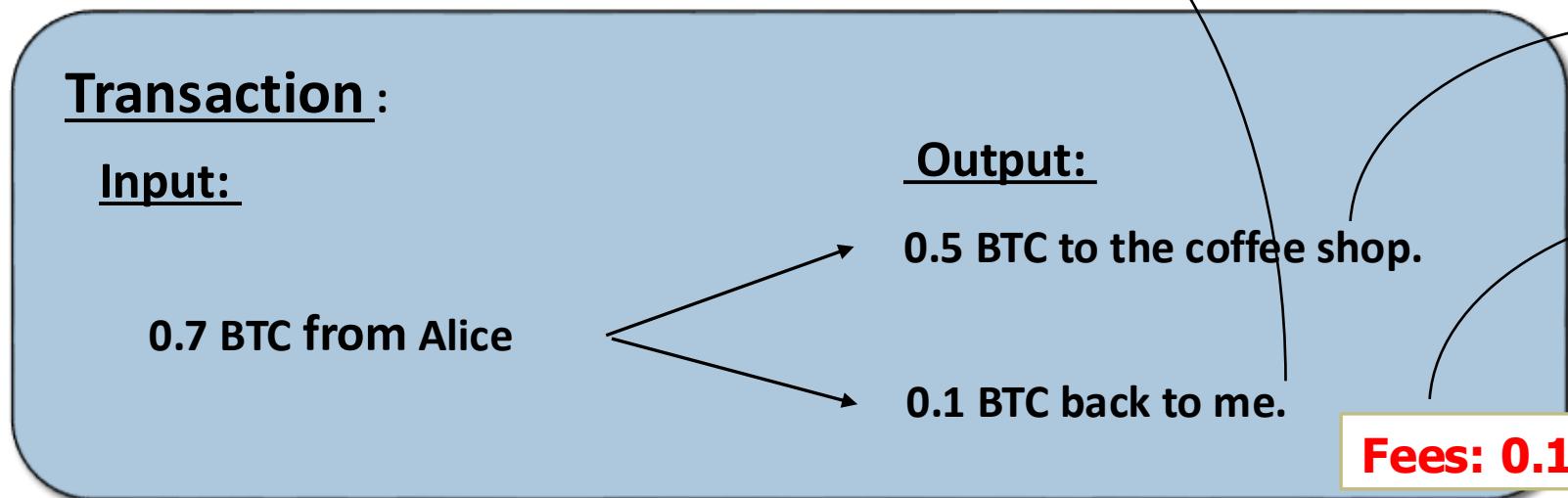
0.1 BTC back to me.

Fees: 0.1 BTC

Transaction Fee



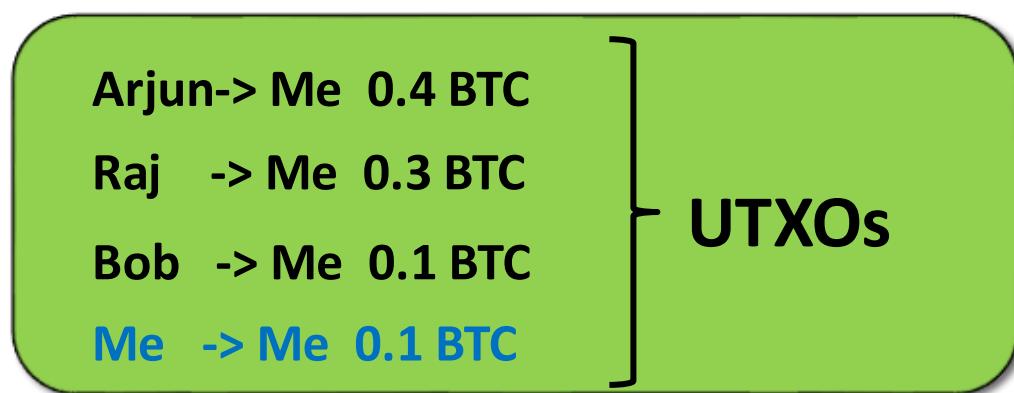
Let say I buy coffee for 0.5 BTC.



UTXO for the coffee shop.

UTXO for the miner.

Transaction Fee



**GIVE THIS VIDEO
A THUMBS-UP !**

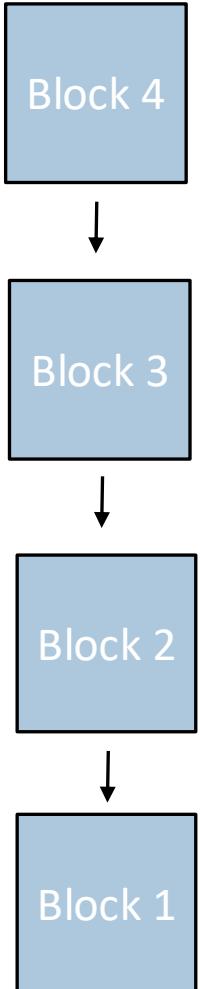
CODE EATER



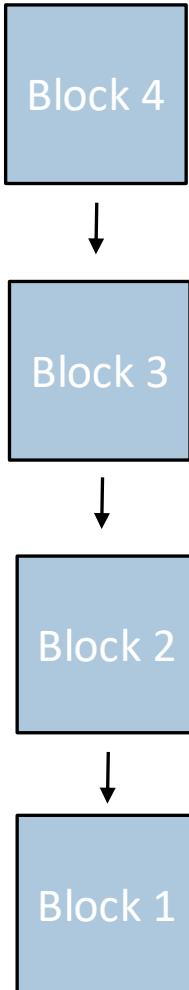


Cryptocurrency Wallet

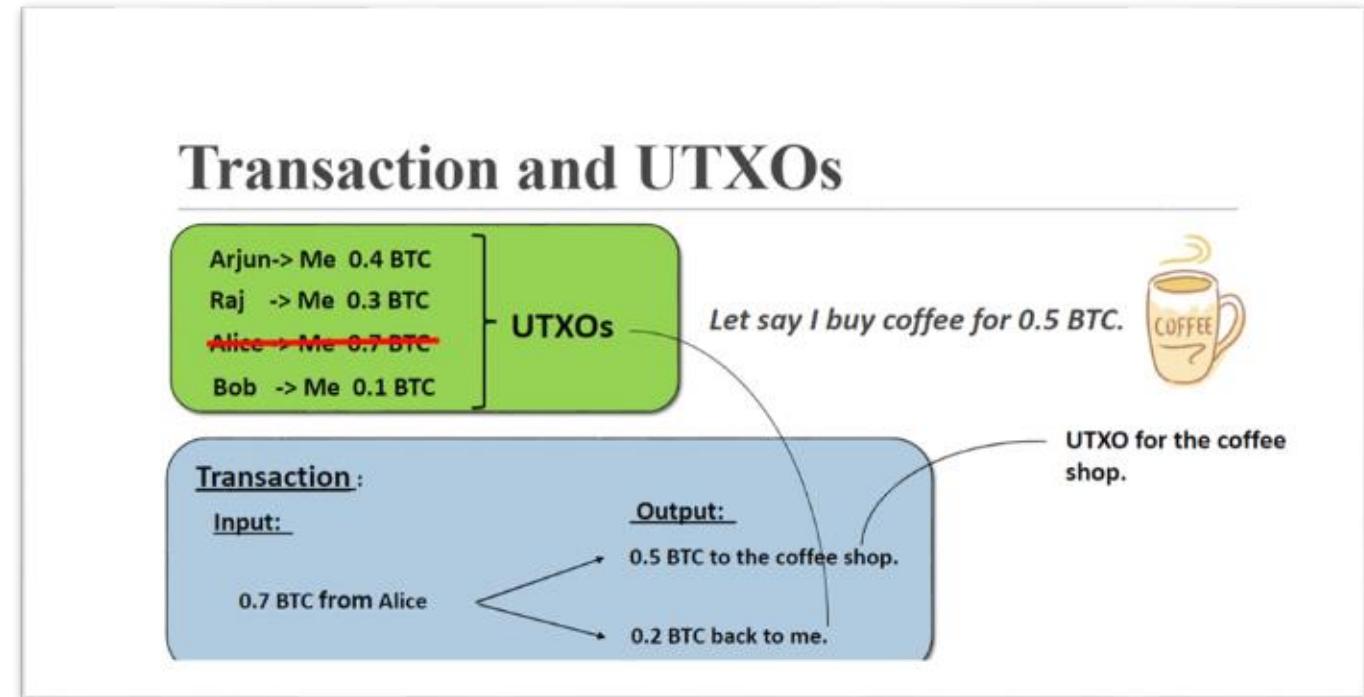
Cryptocurrency Wallets



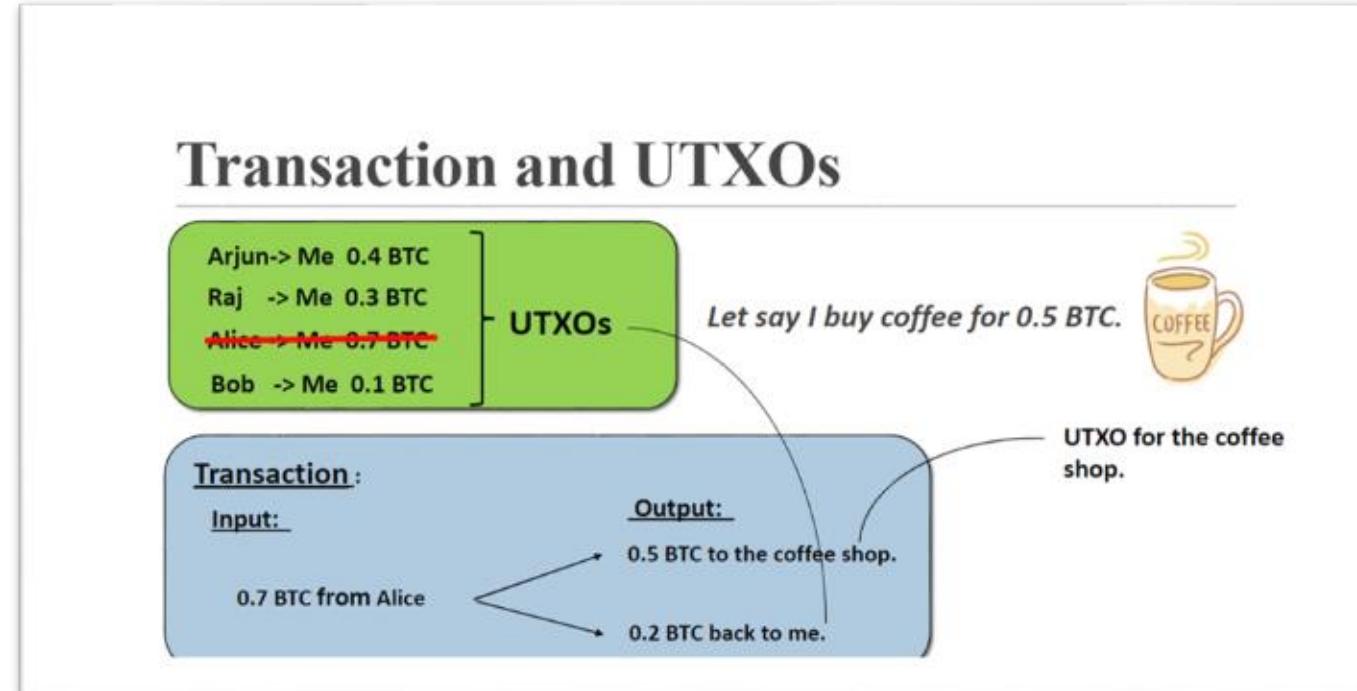
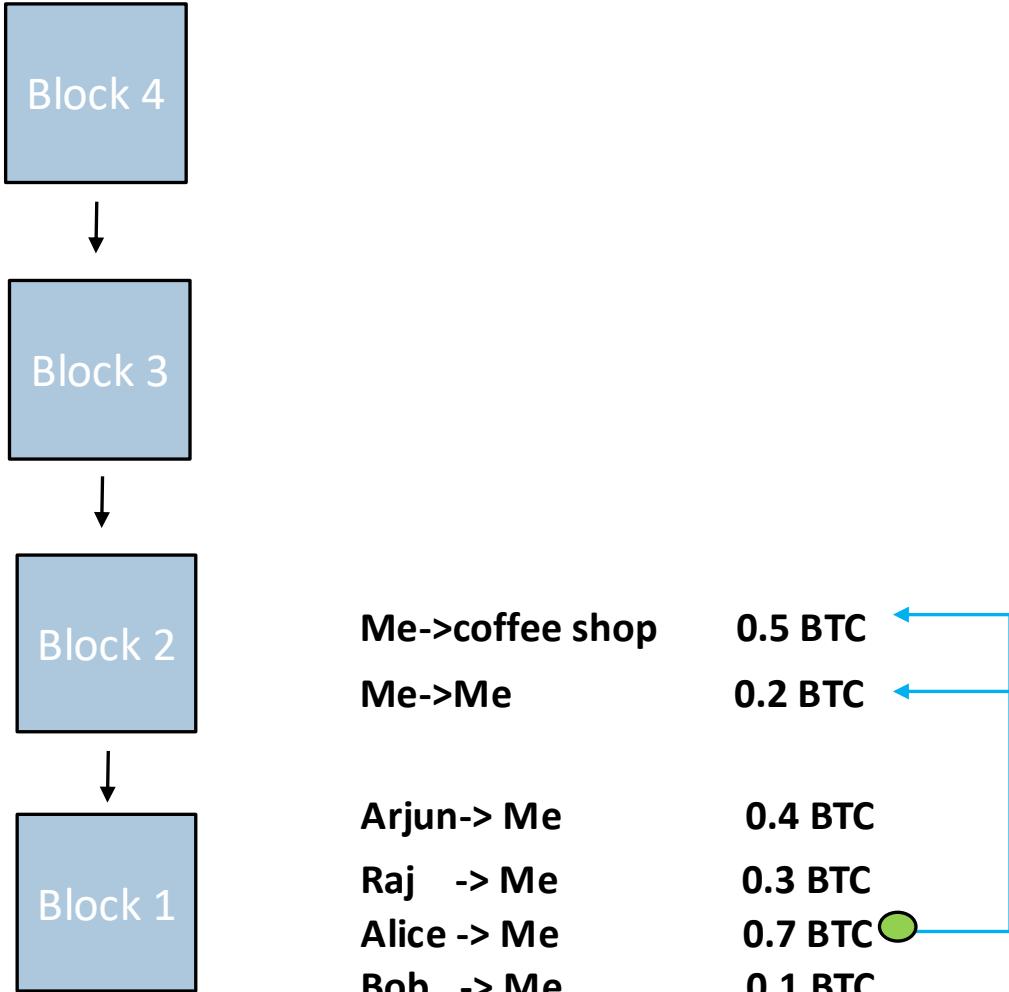
Cryptocurrency Wallets



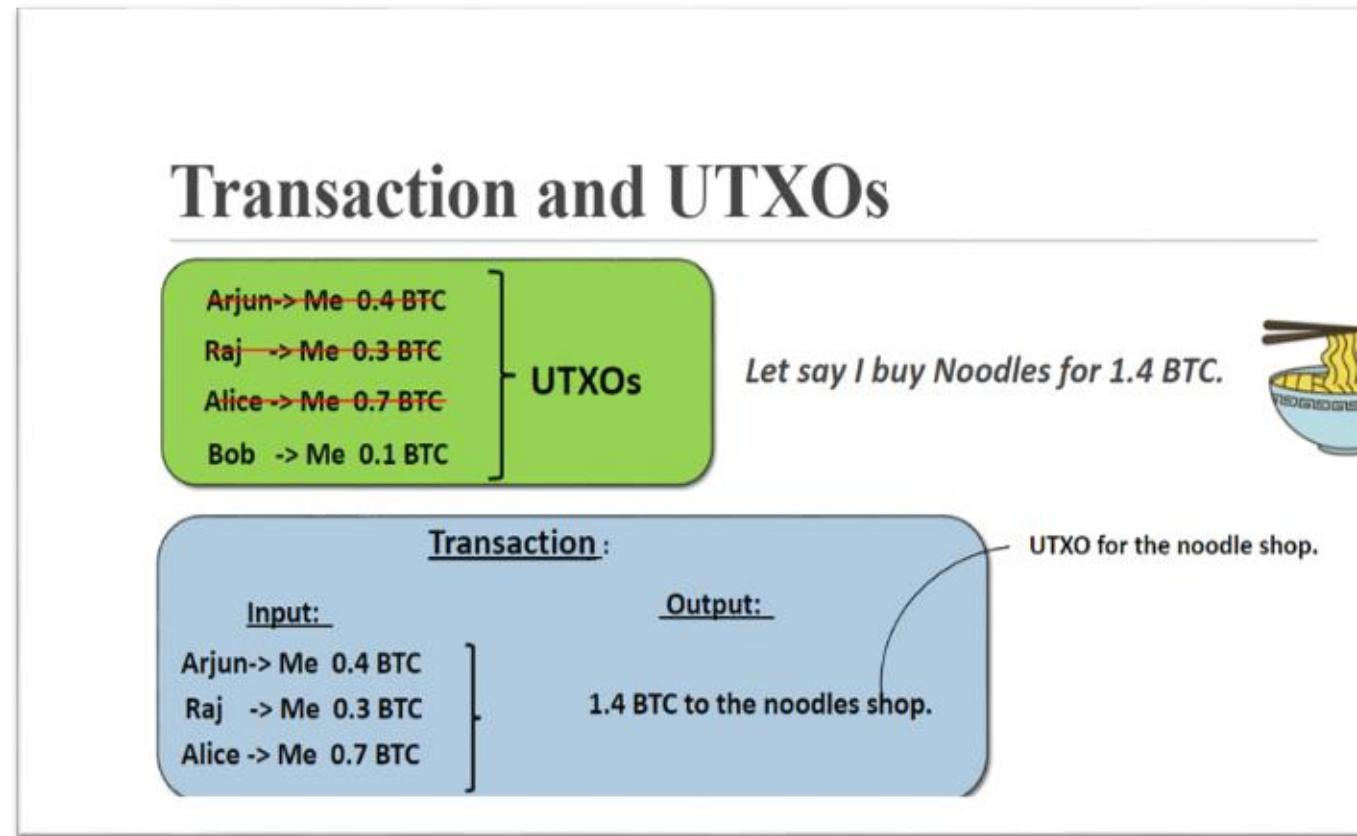
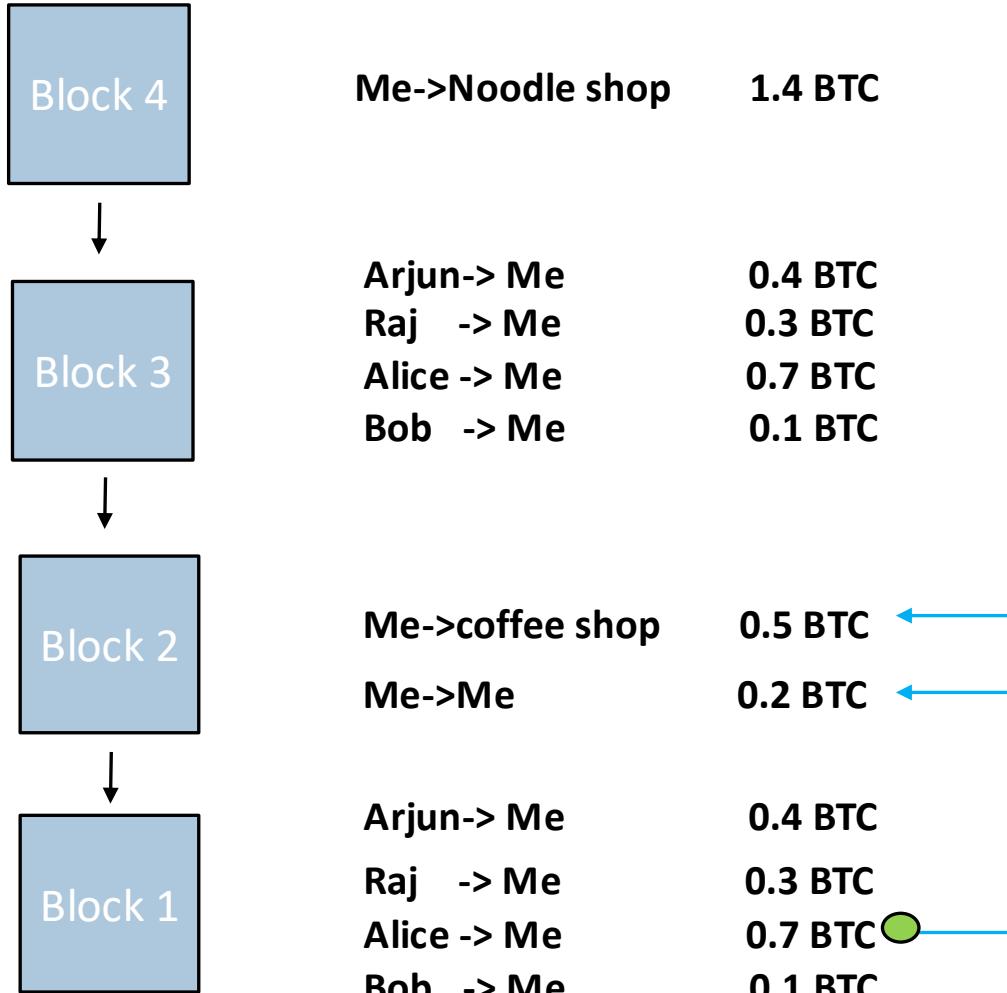
Me->coffee shop	0.5 BTC
Me->Me	0.2 BTC
Arjun-> Me	0.4 BTC
Raj -> Me	0.3 BTC
Alice -> Me	0.7 BTC
Bob -> Me	0.1 BTC



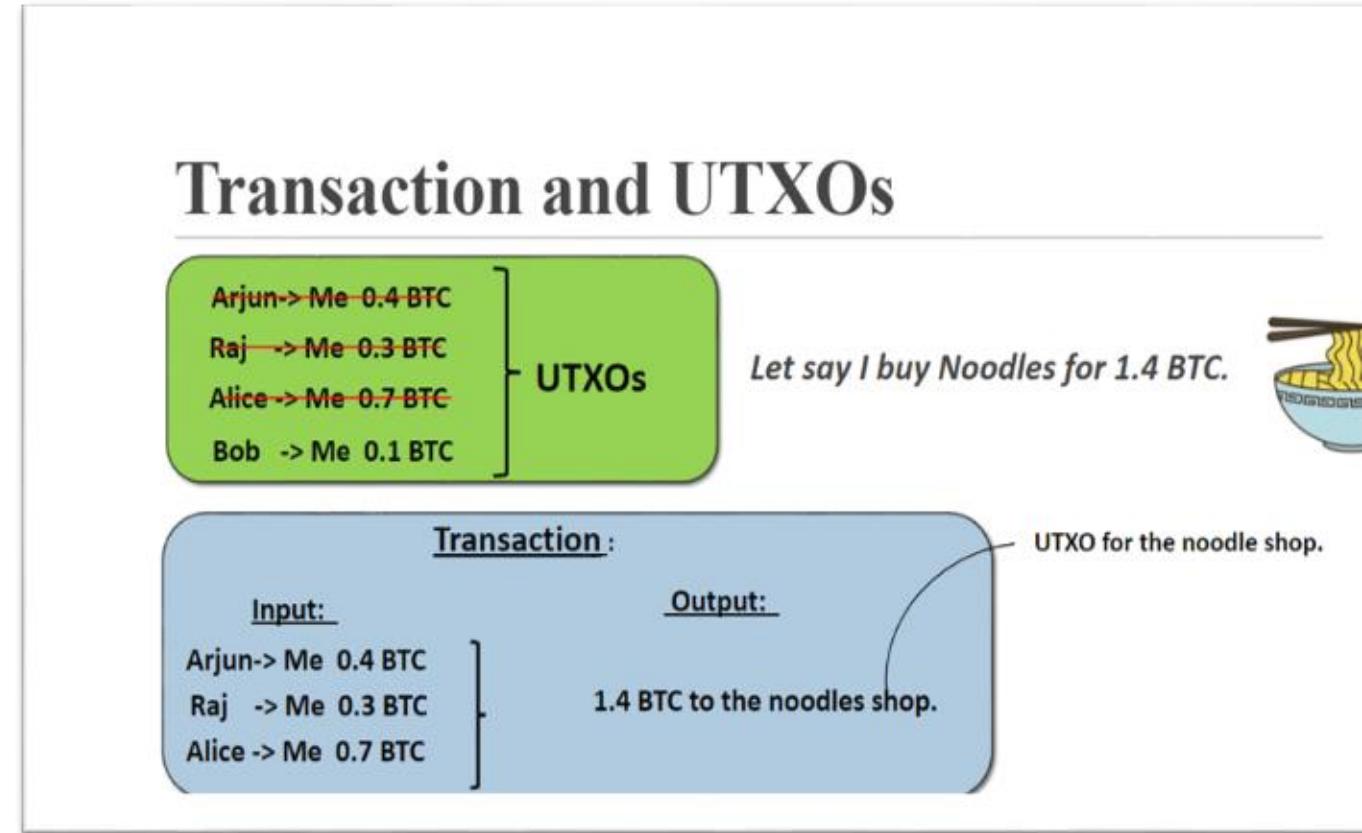
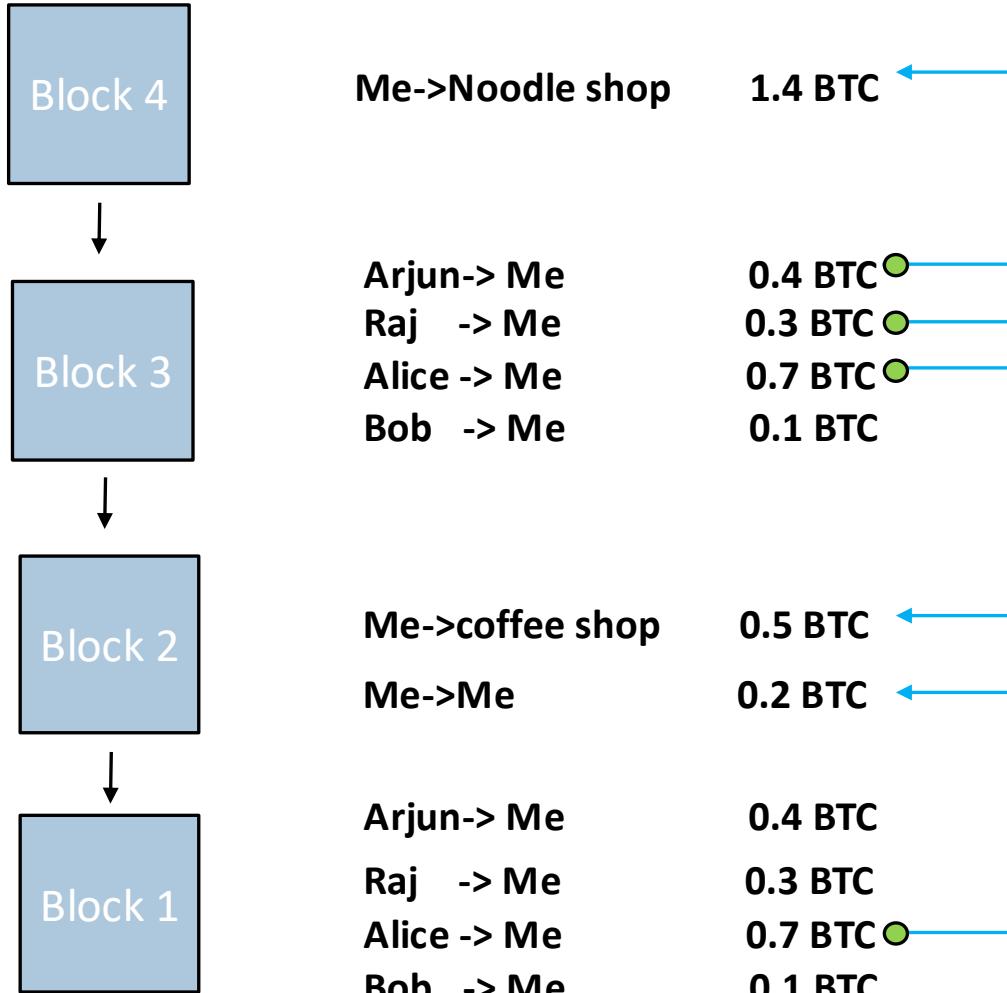
Cryptocurrency Wallets



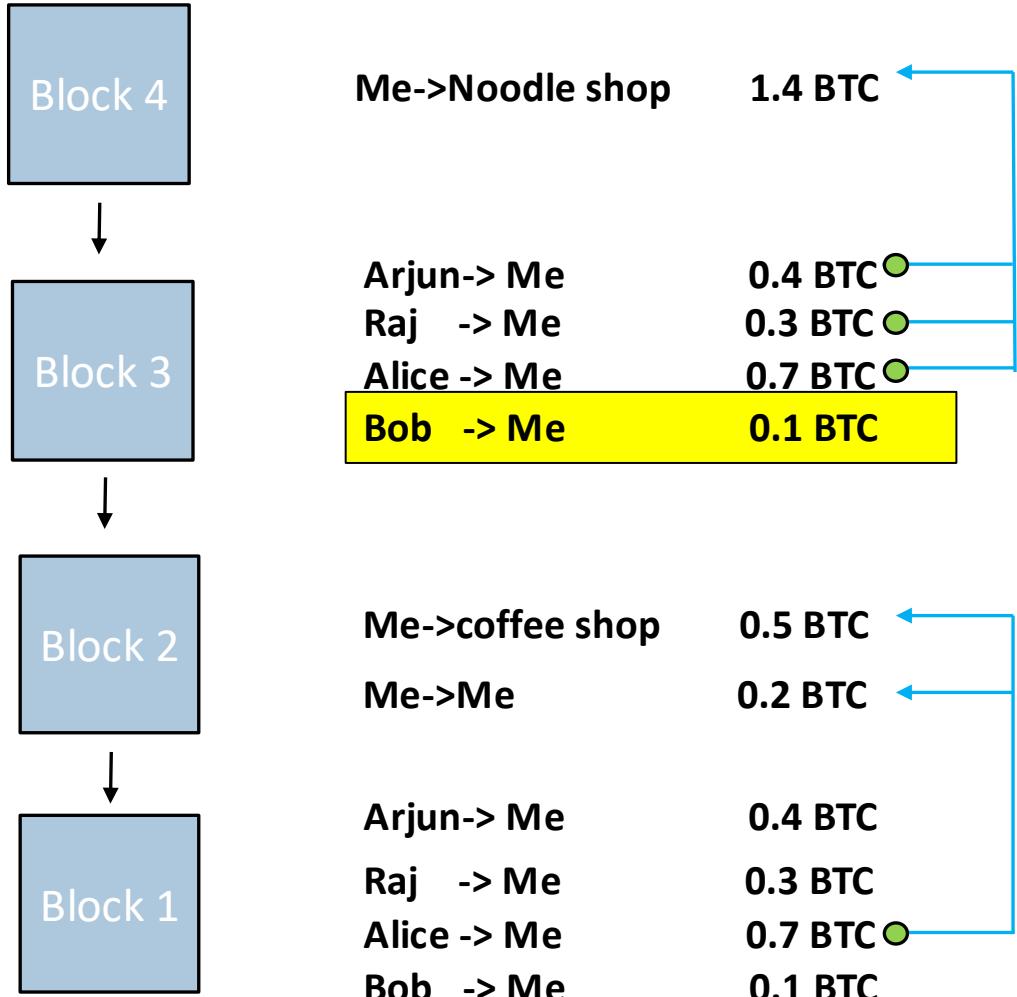
Cryptocurrency Wallets



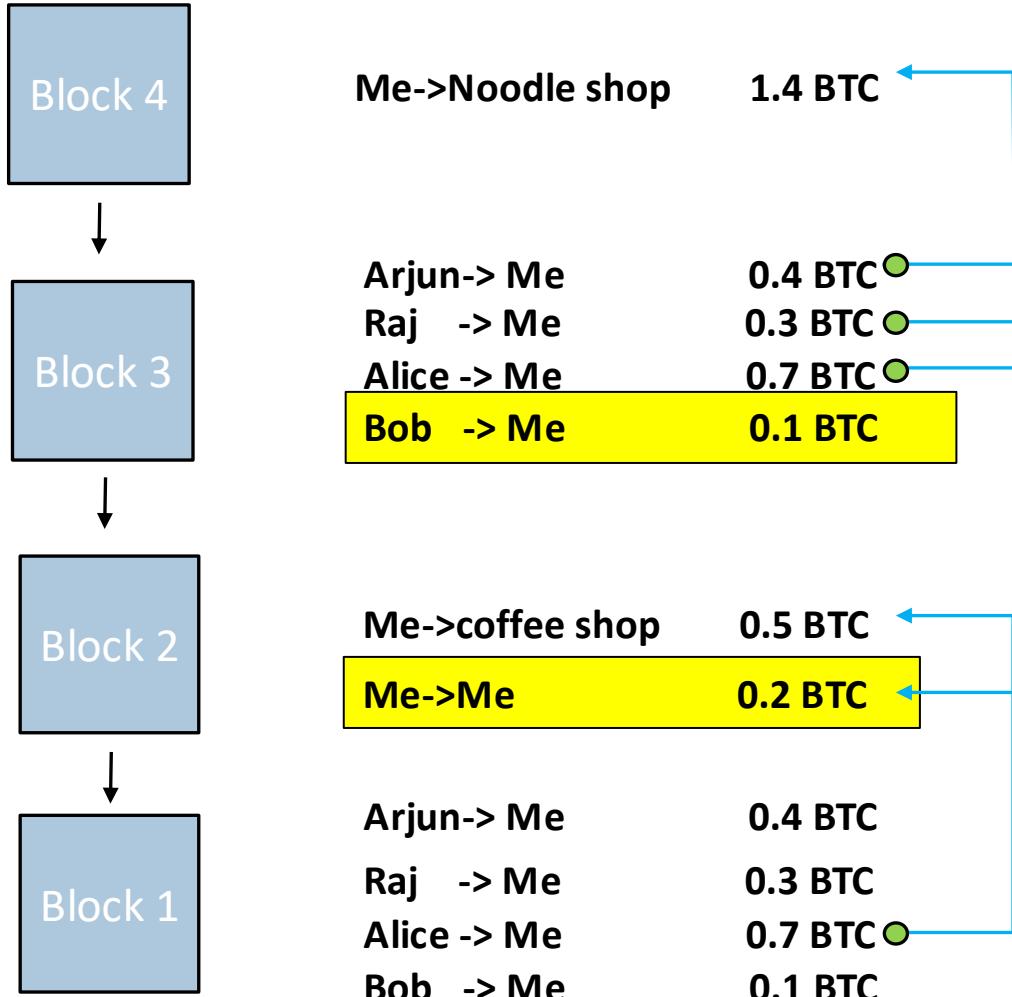
Cryptocurrency Wallets



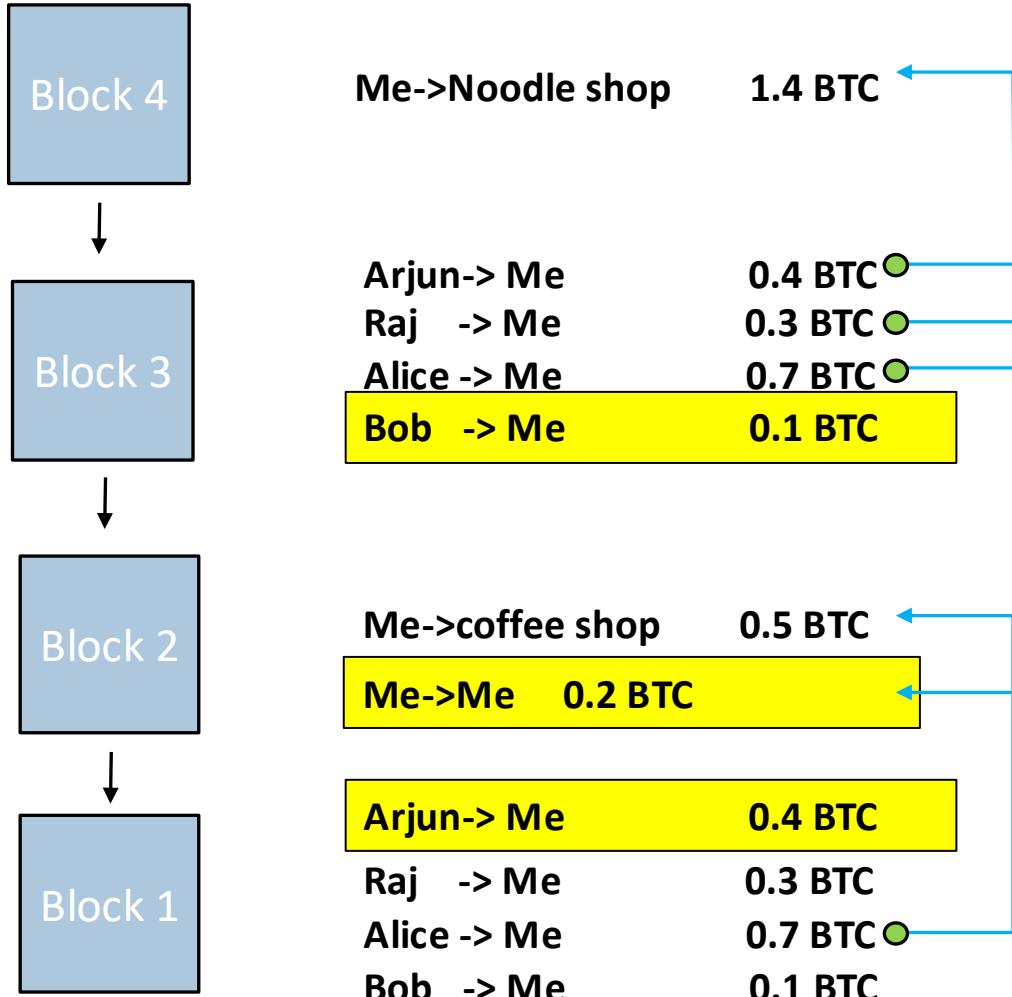
Cryptocurrency Wallets



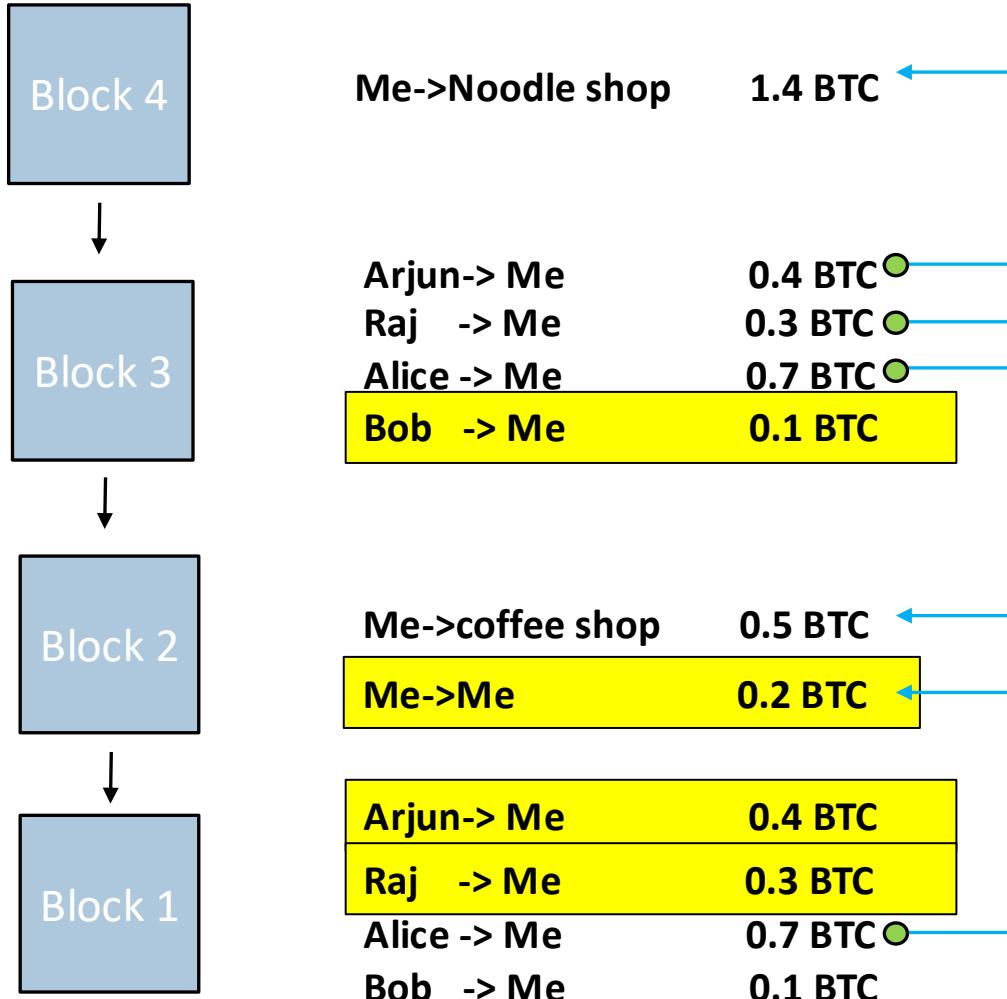
Cryptocurrency Wallets



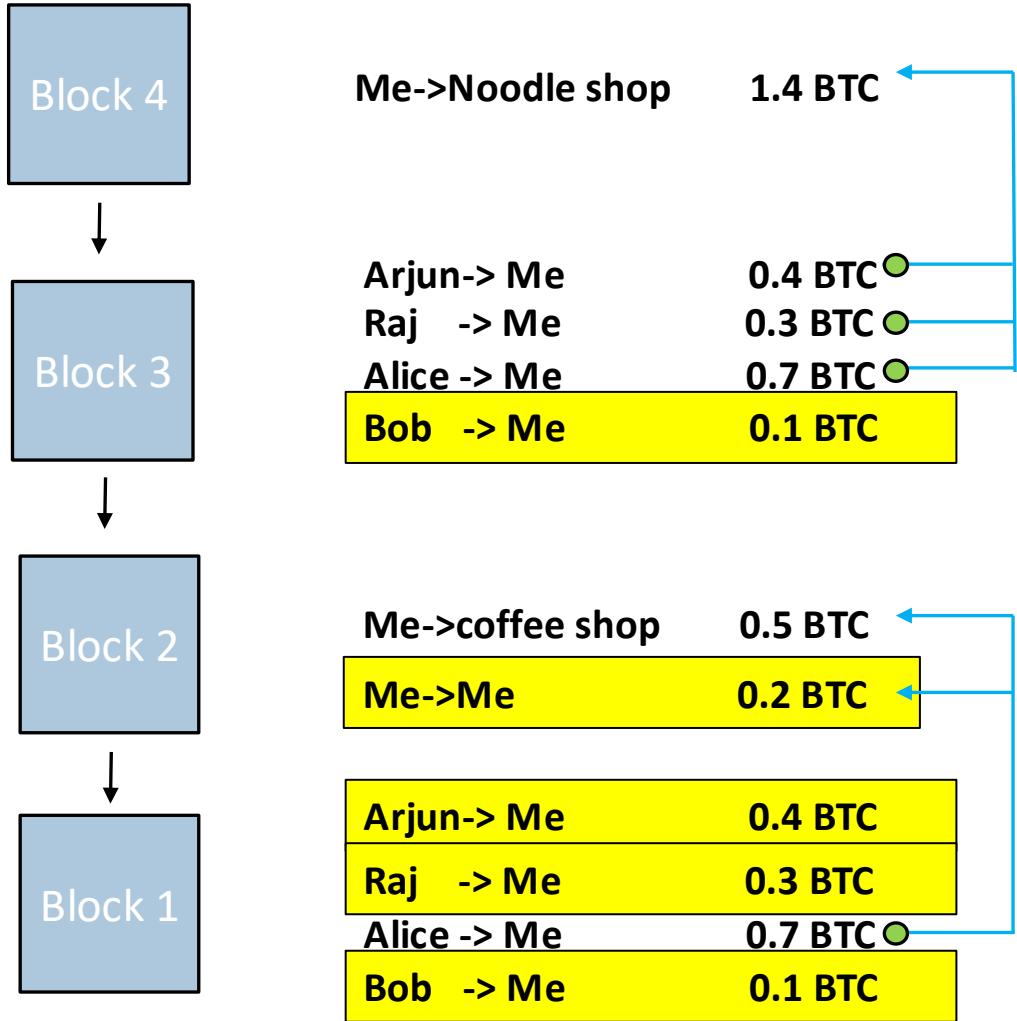
Cryptocurrency Wallets



Cryptocurrency Wallets

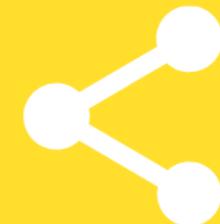


Cryptocurrency Wallets

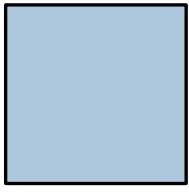


**GIVE THIS VIDEO
A THUMBS-UP !**

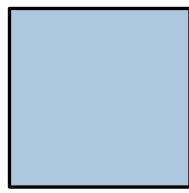
CODE EATER



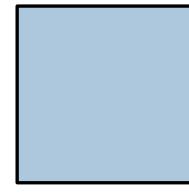
Cryptocurrency Wallets



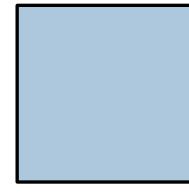
Me->Noodle shop 1.4 BTC



Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

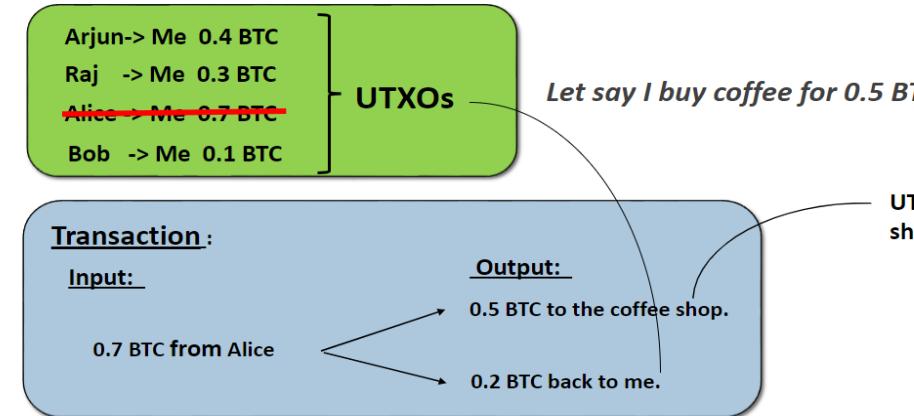


Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC

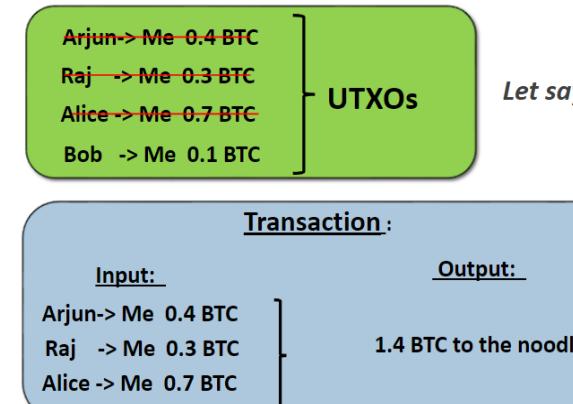


Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

Transaction and UTXOs



Transaction and UTXOs



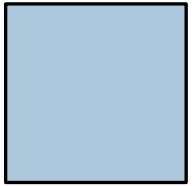
Cryptocurrency Wallets



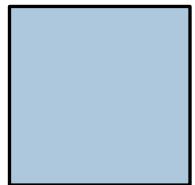


Private and Public Key

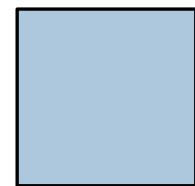
Cryptocurrency Wallets



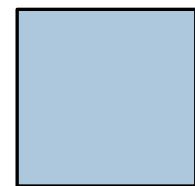
Me->Noodle shop 1.4 BTC



Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC



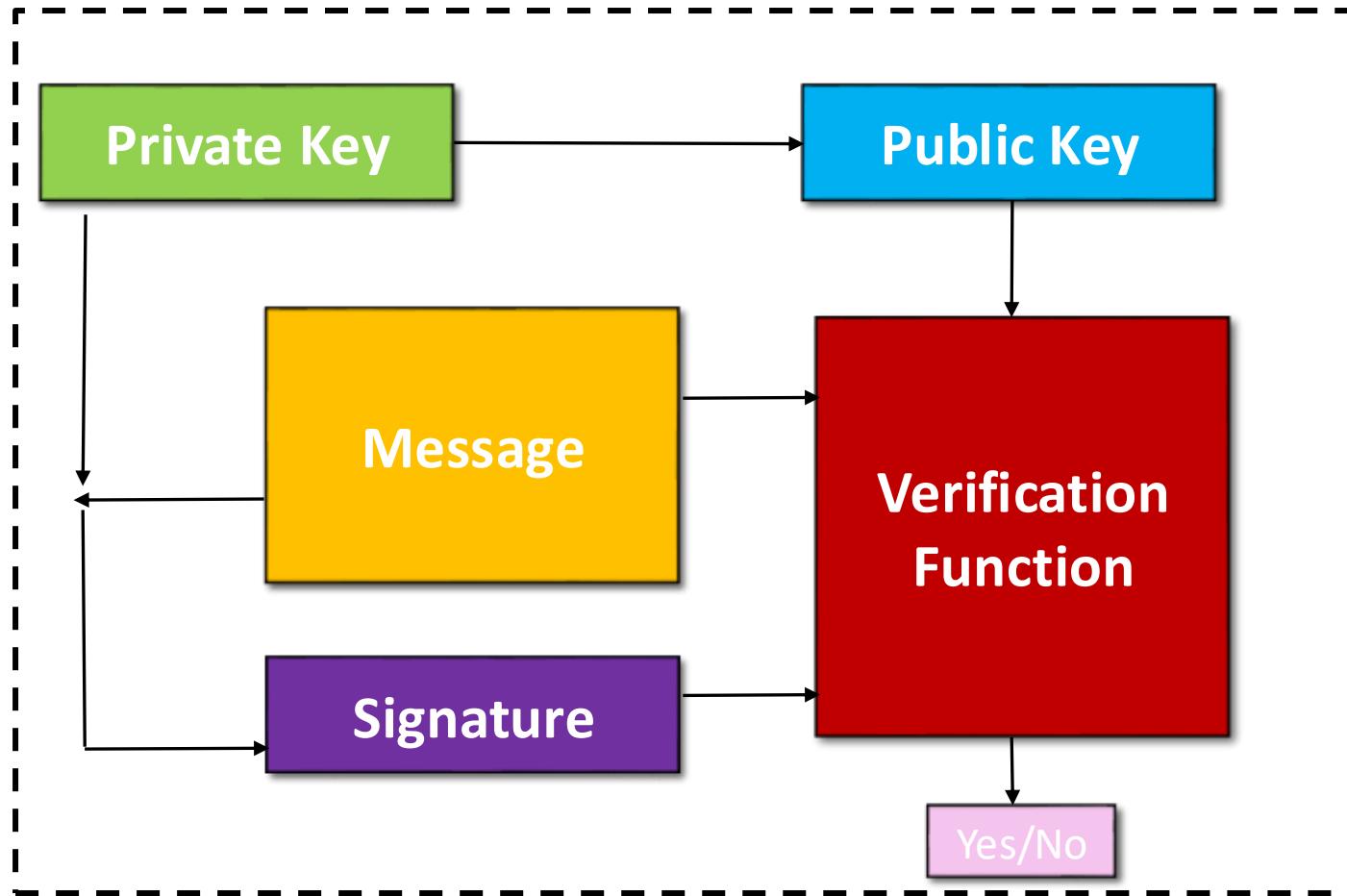
Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC



Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

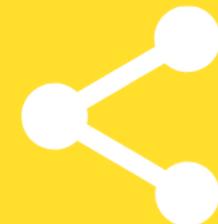
Private and Public Key

Private and Public Key



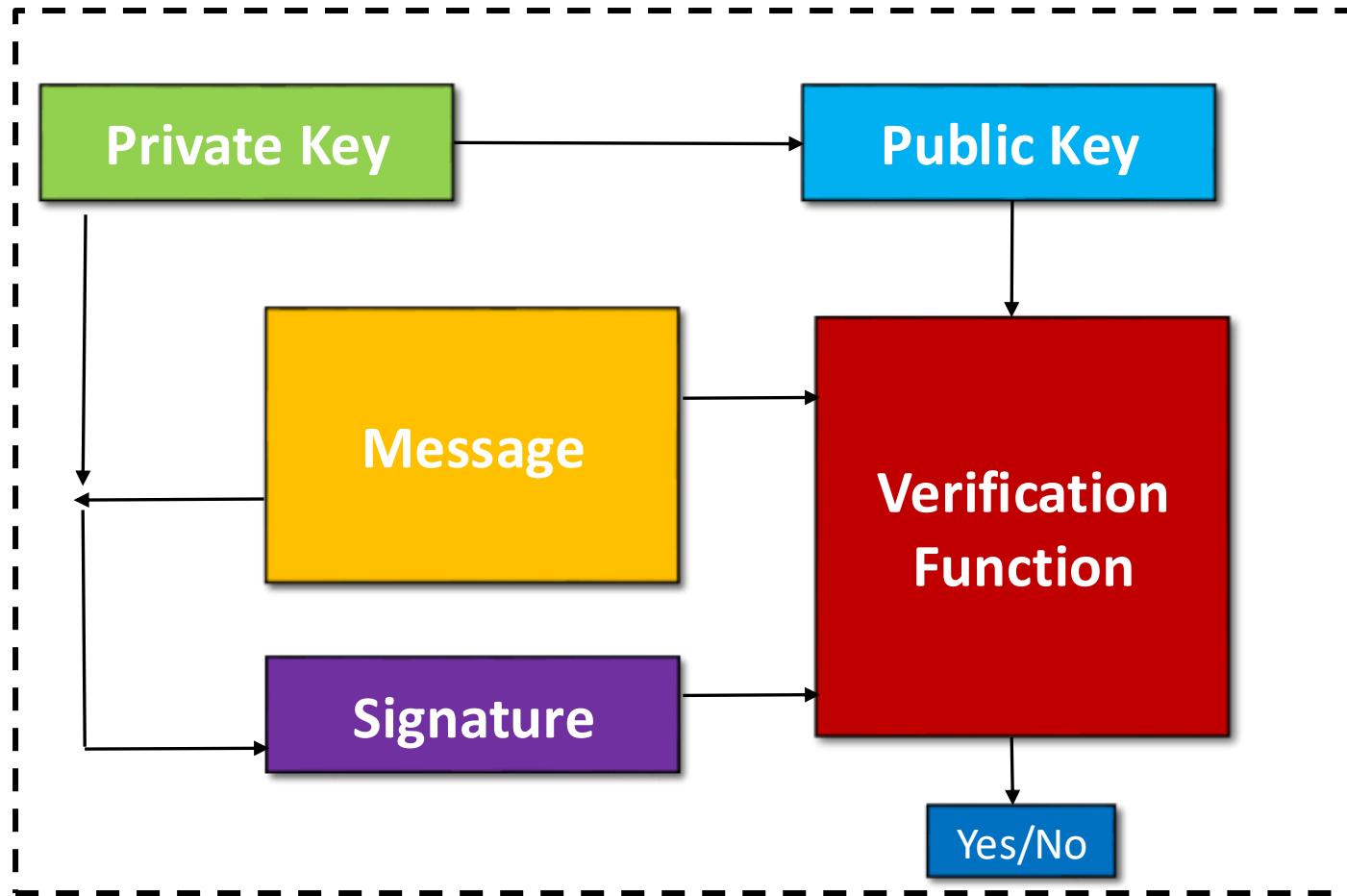
**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

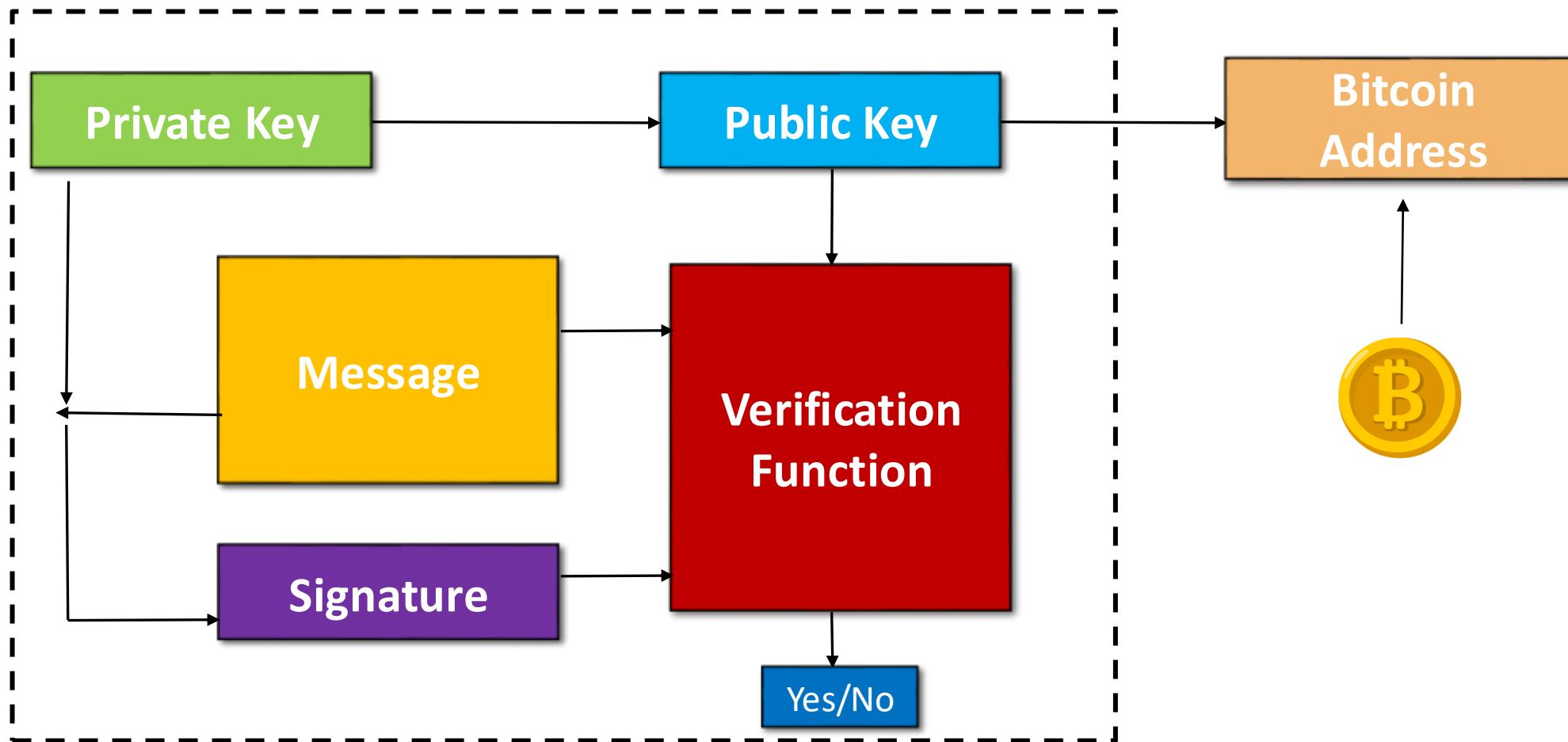


Public Key vs Bitcoin Address

Private and Public Key



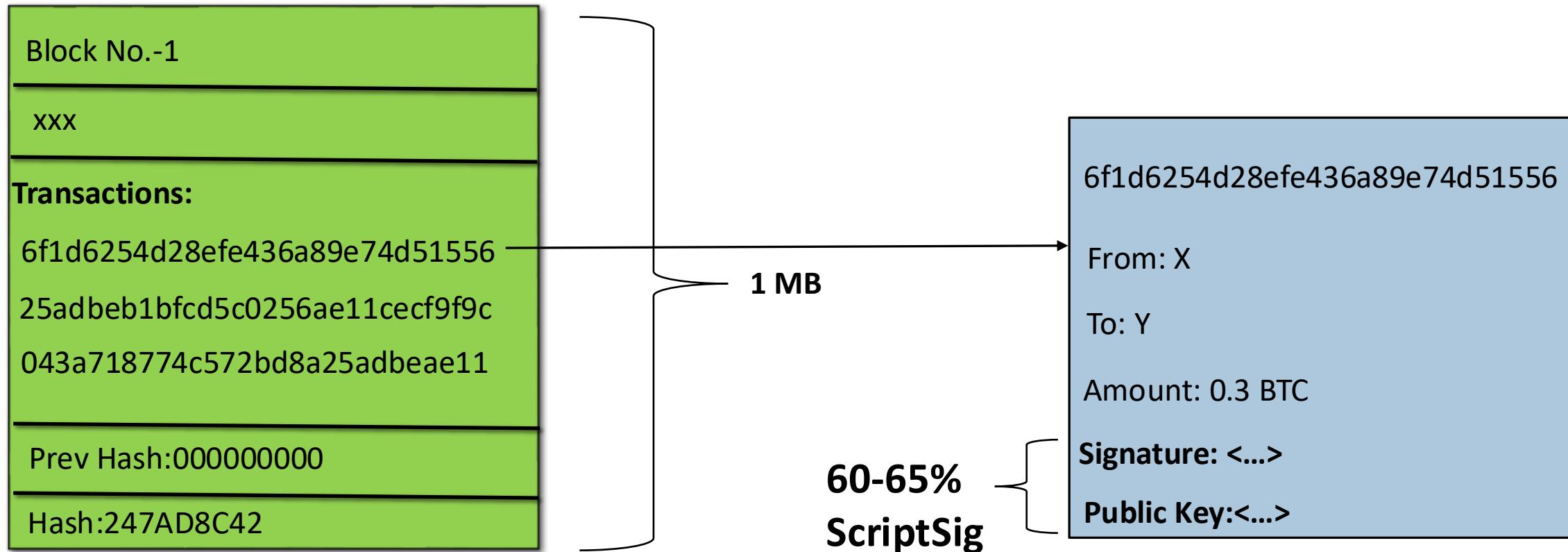
Private and Public Key





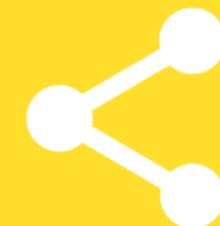
Segregated Witness

Segregated Witness



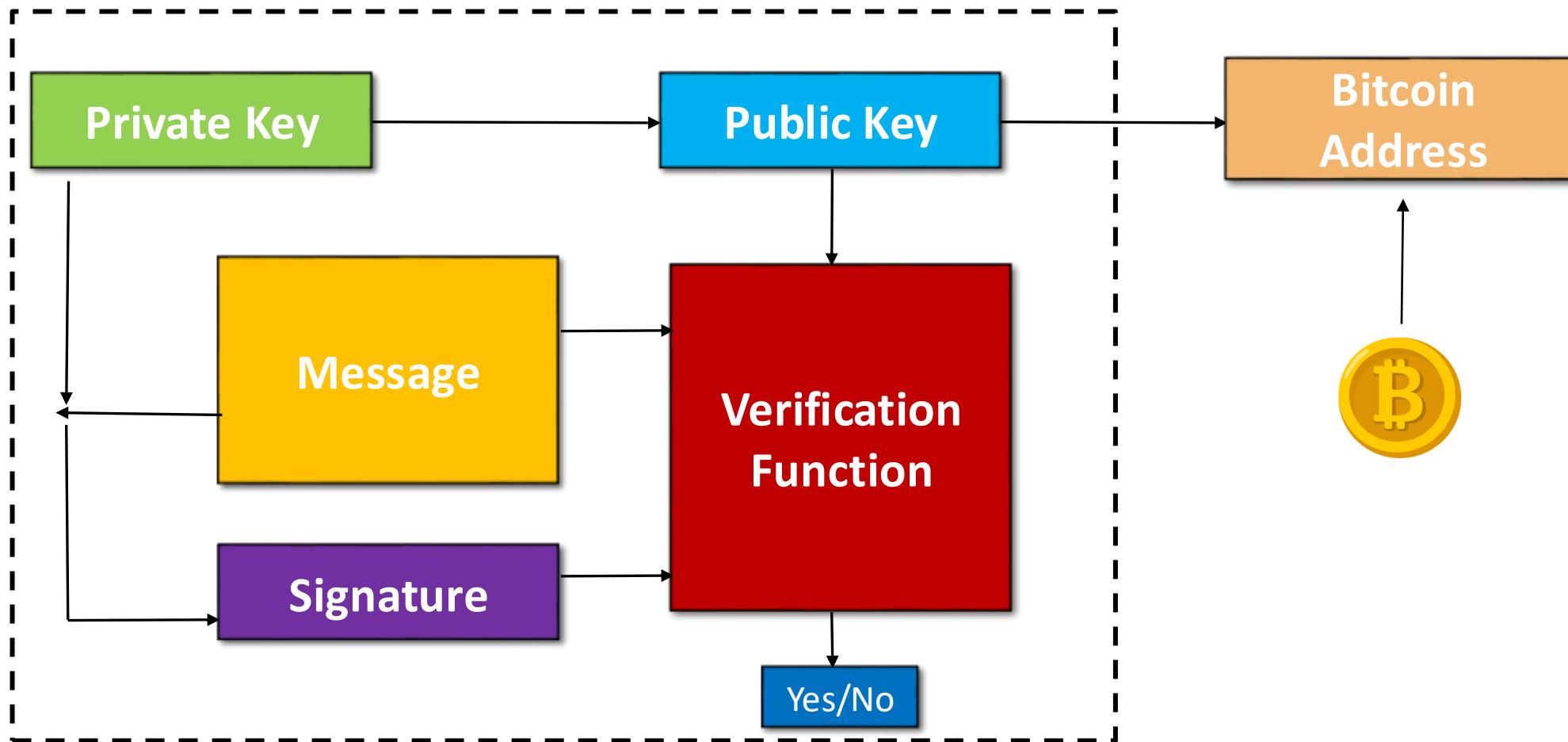
**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

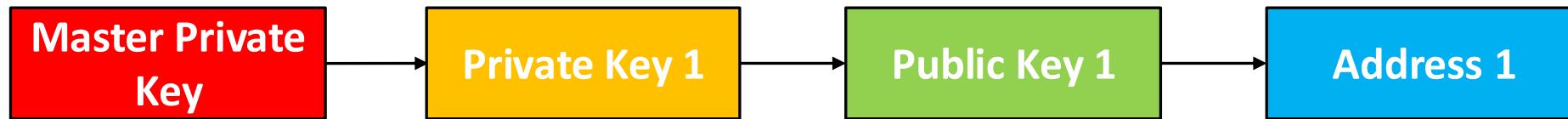


Hierarchically Deterministic Wallet

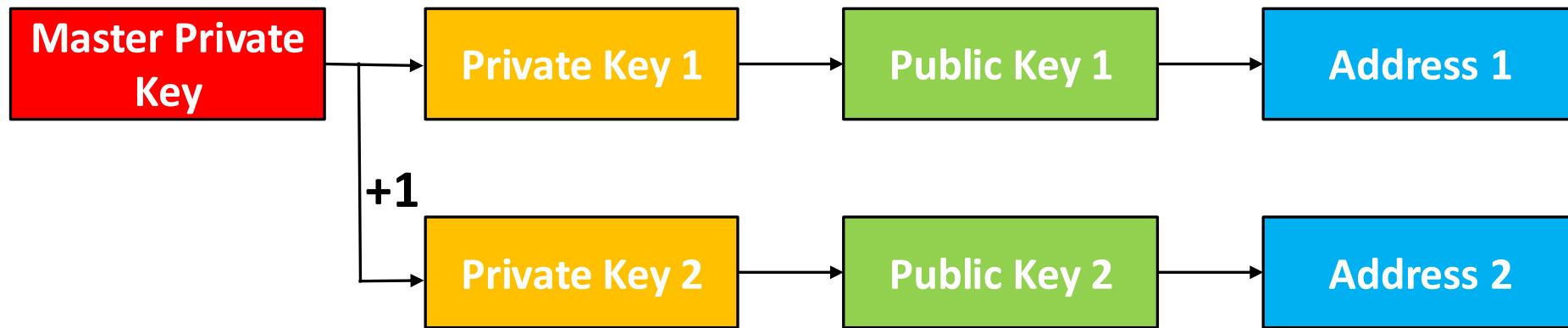
Private and Public Key



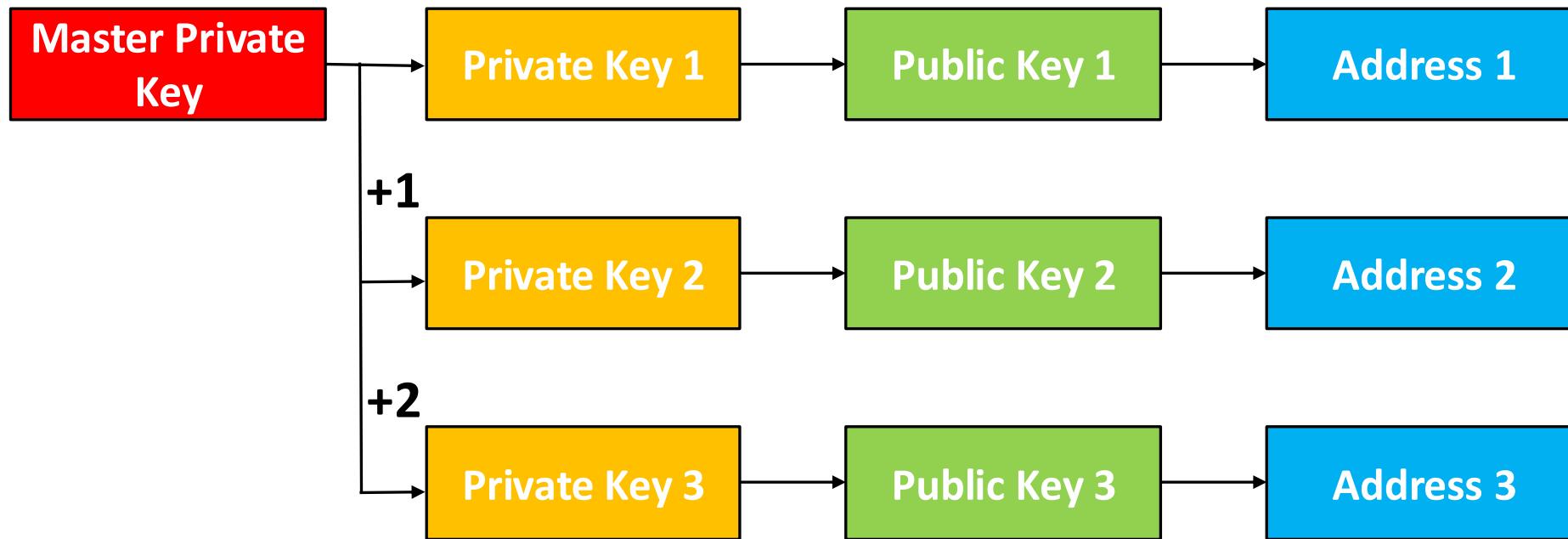
Hierarchically Deterministic (HD) Wallets



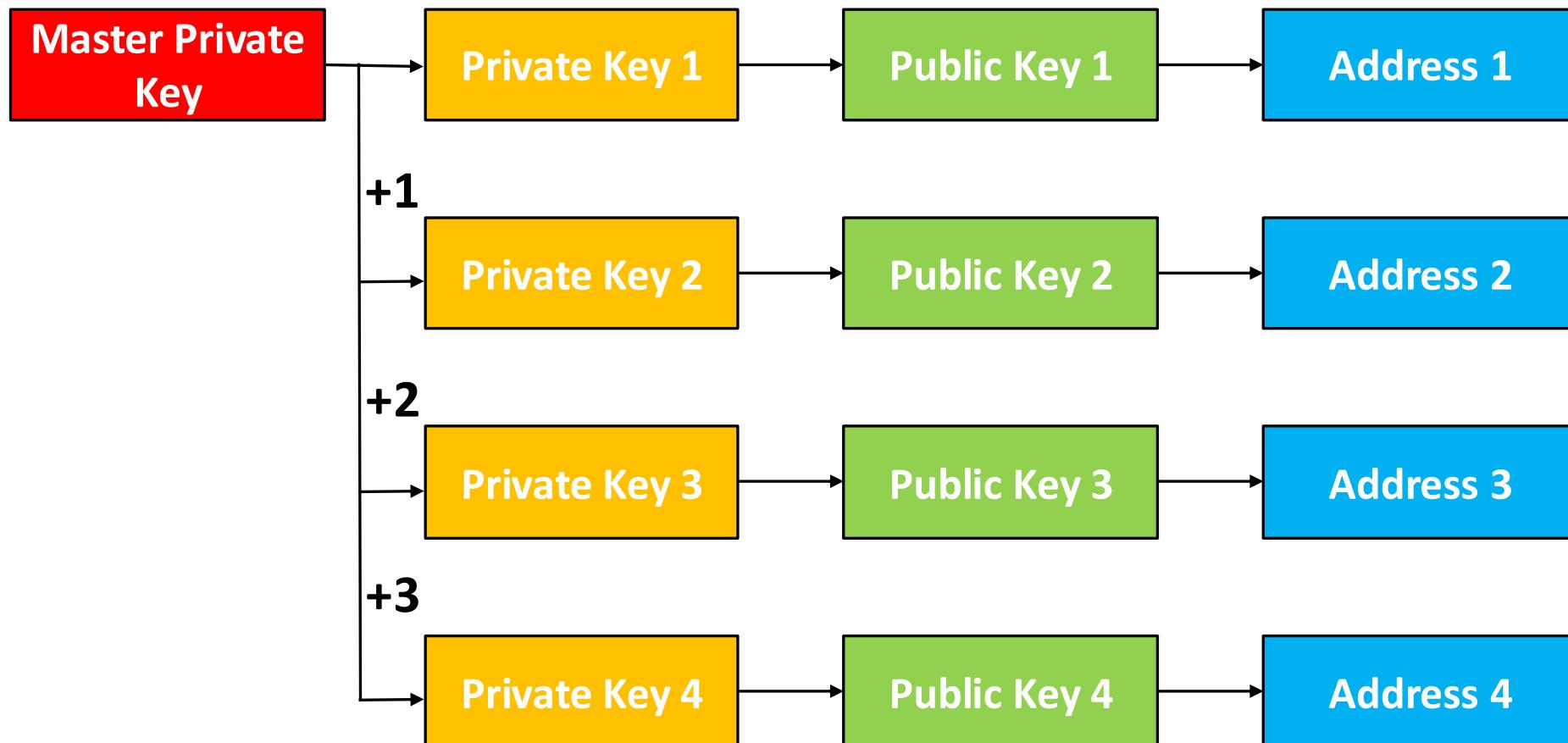
Hierarchically Deterministic (HD) Wallets



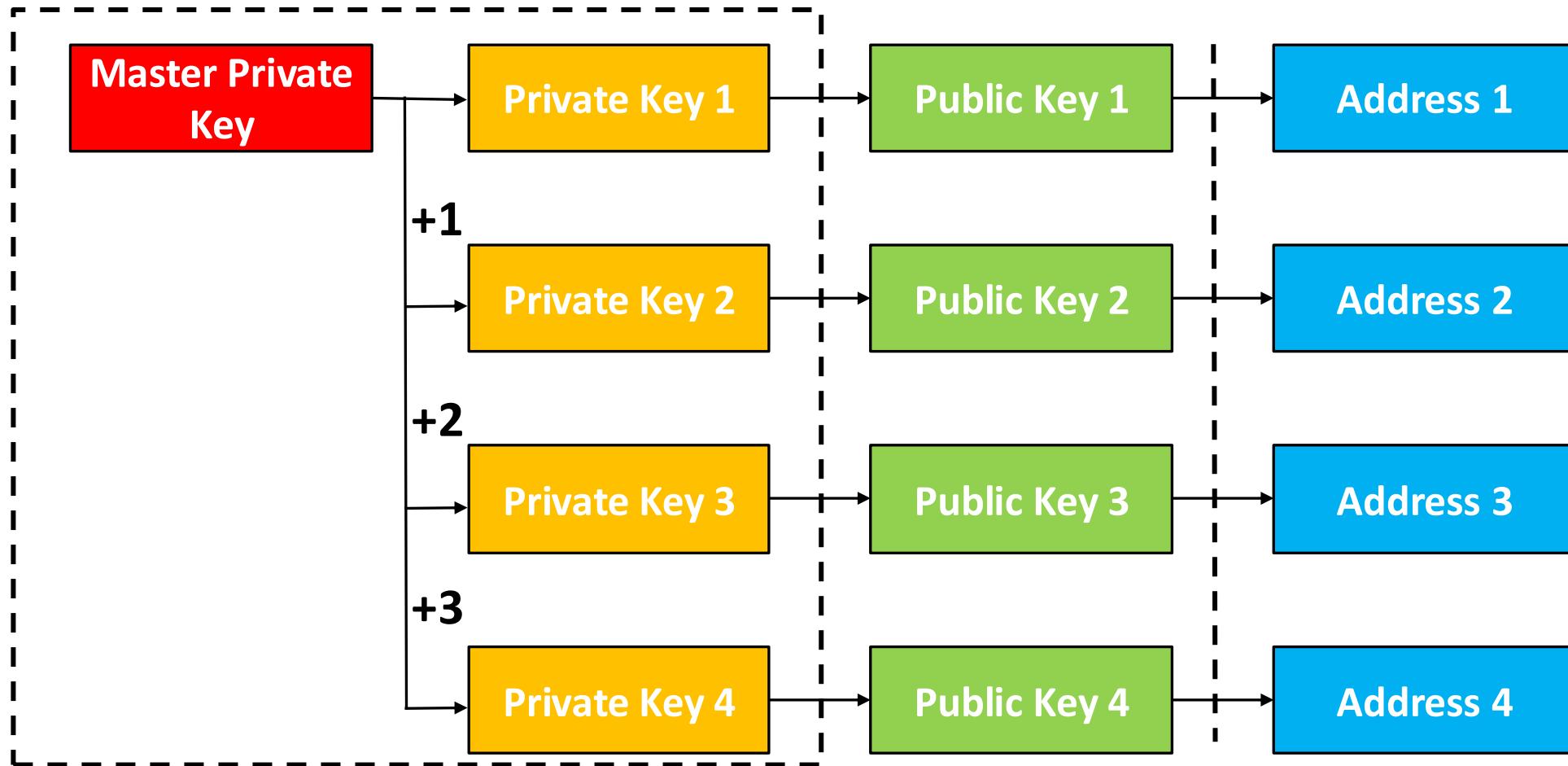
Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets

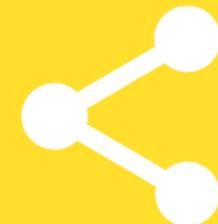


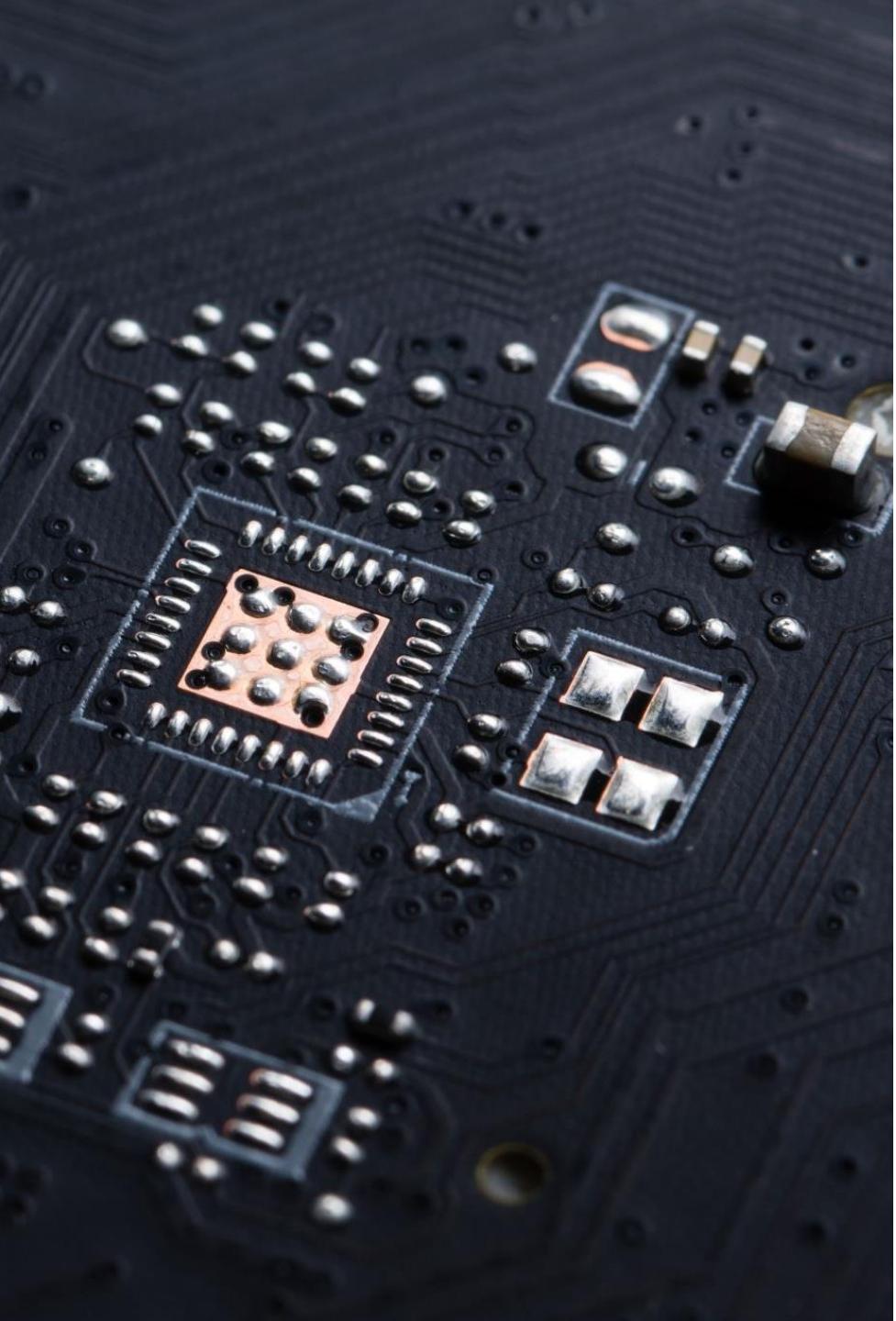
Hierarchically Deterministic (HD) Wallets



**GIVE THIS VIDEO
A THUMBS-UP !**

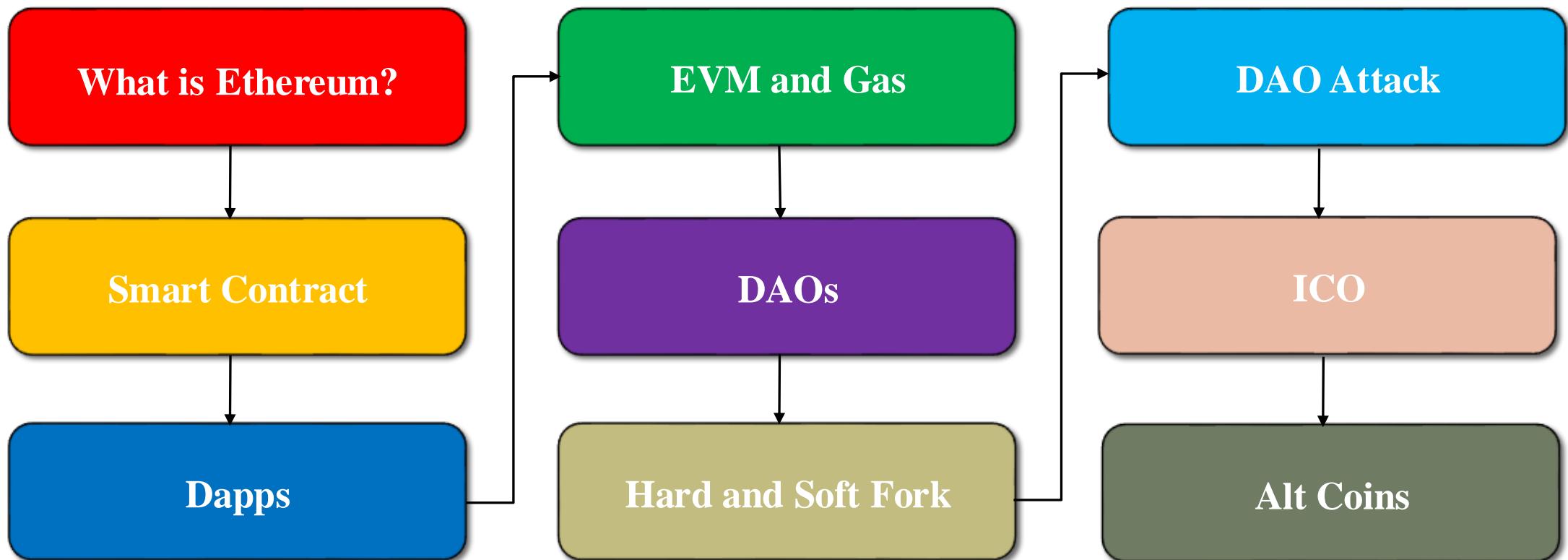
CODE EATER





Ethereum

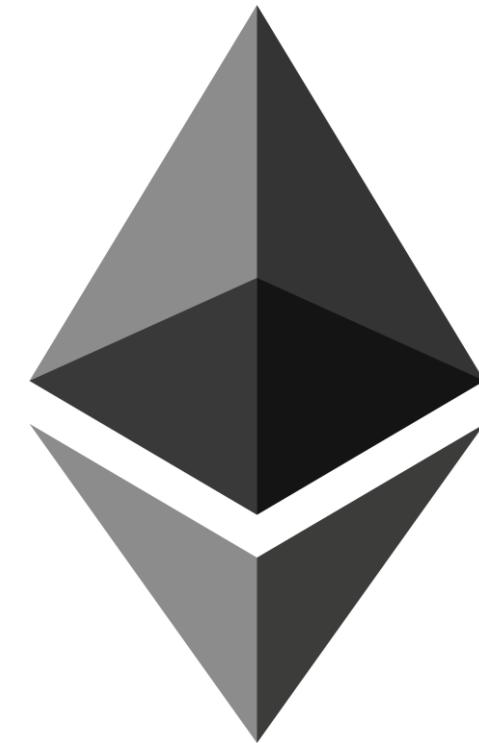
Contents – Module C



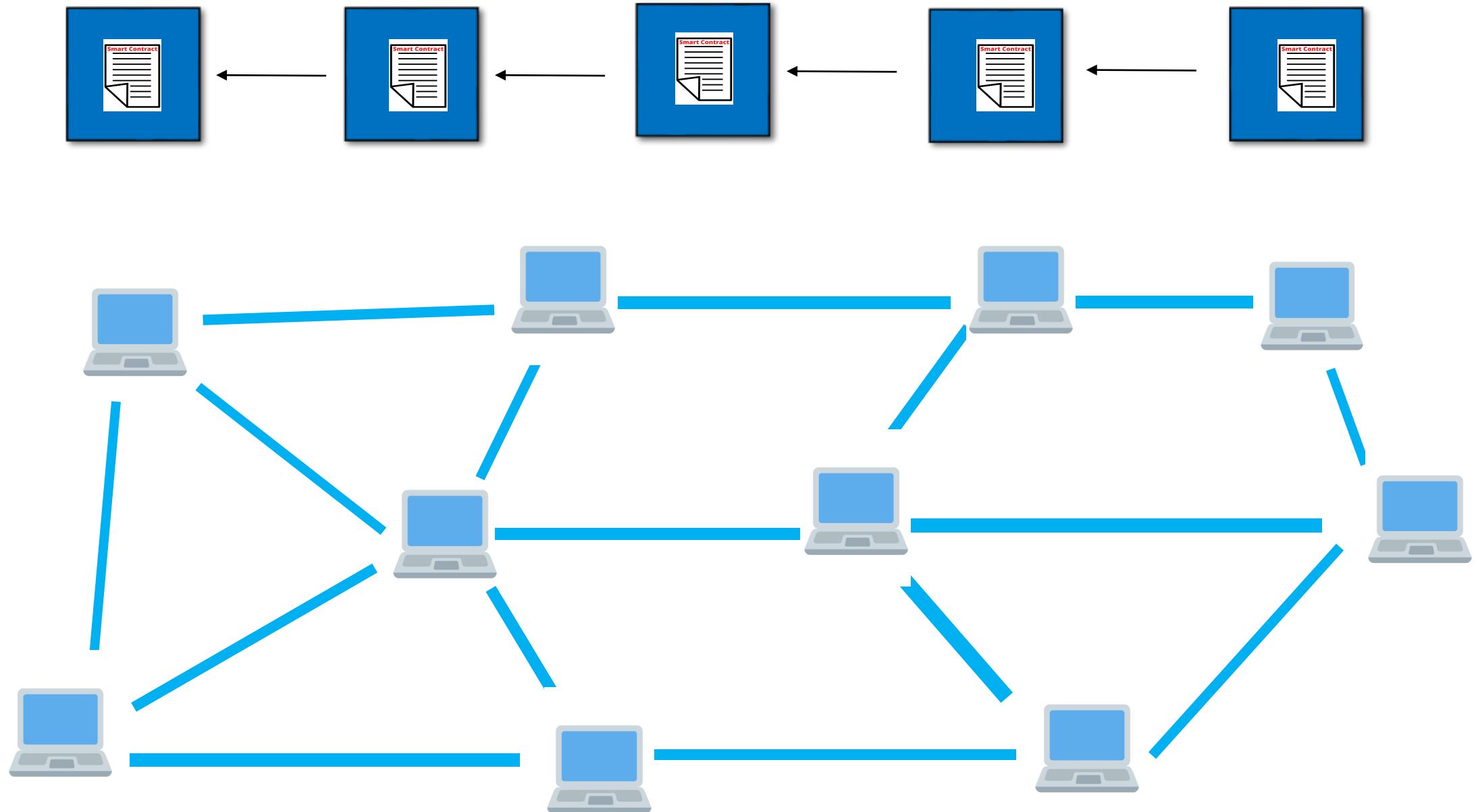
Ethereum



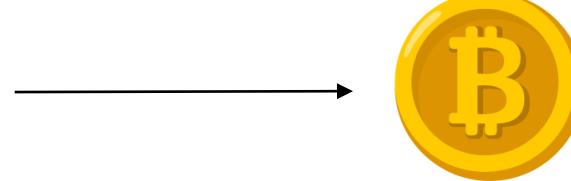
Vitalik Buterin



Ethereum



Bitcoin



Ethereum



What is Ethereum?

Technology

Blockchain

Protocol/Coin

Waves

Bitcoin

Ethereum

Token

WGB	BI
INTL	WGR

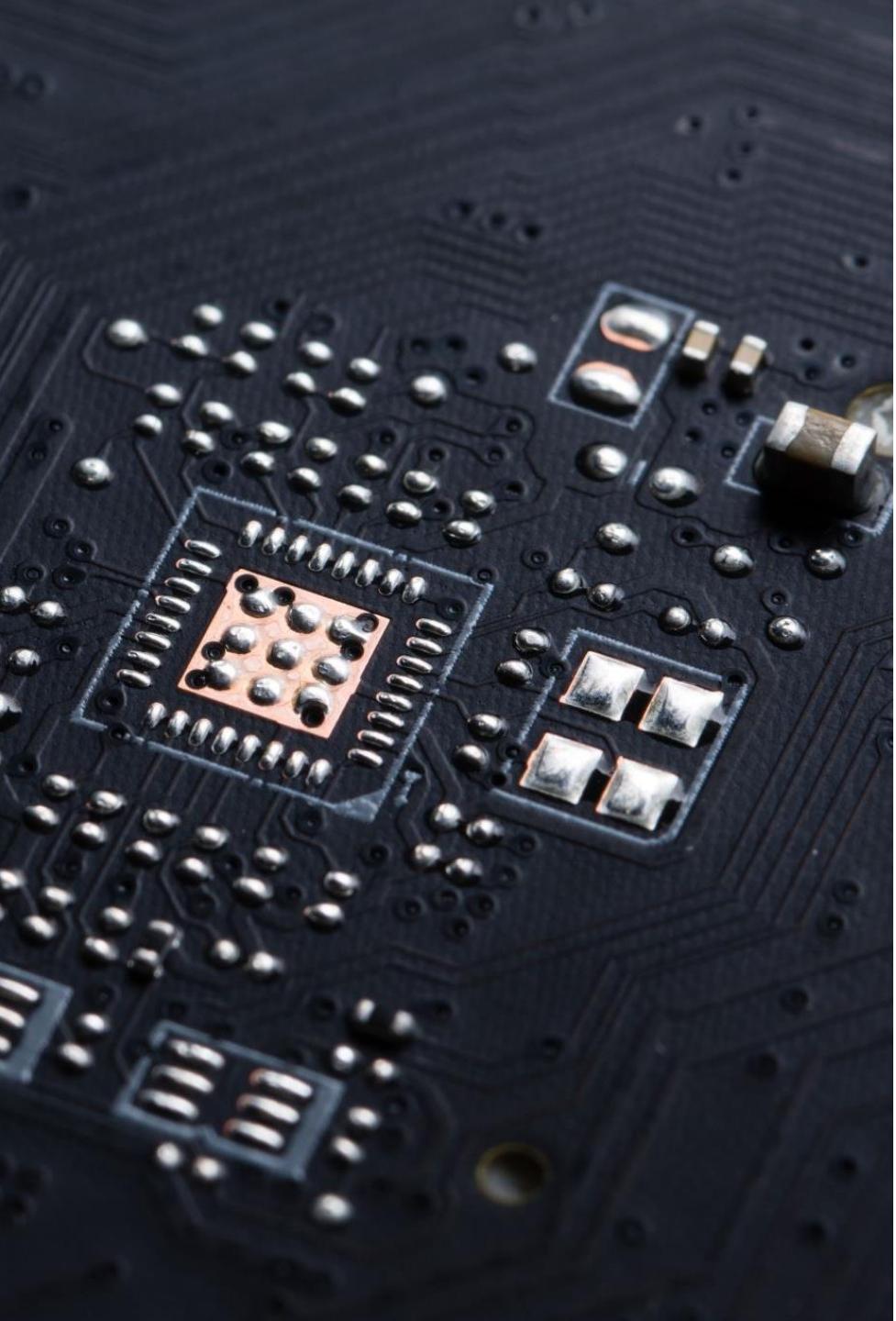


TRX	SNT
REP	AE

**GIVE THIS VIDEO
A THUMBS-UP !**

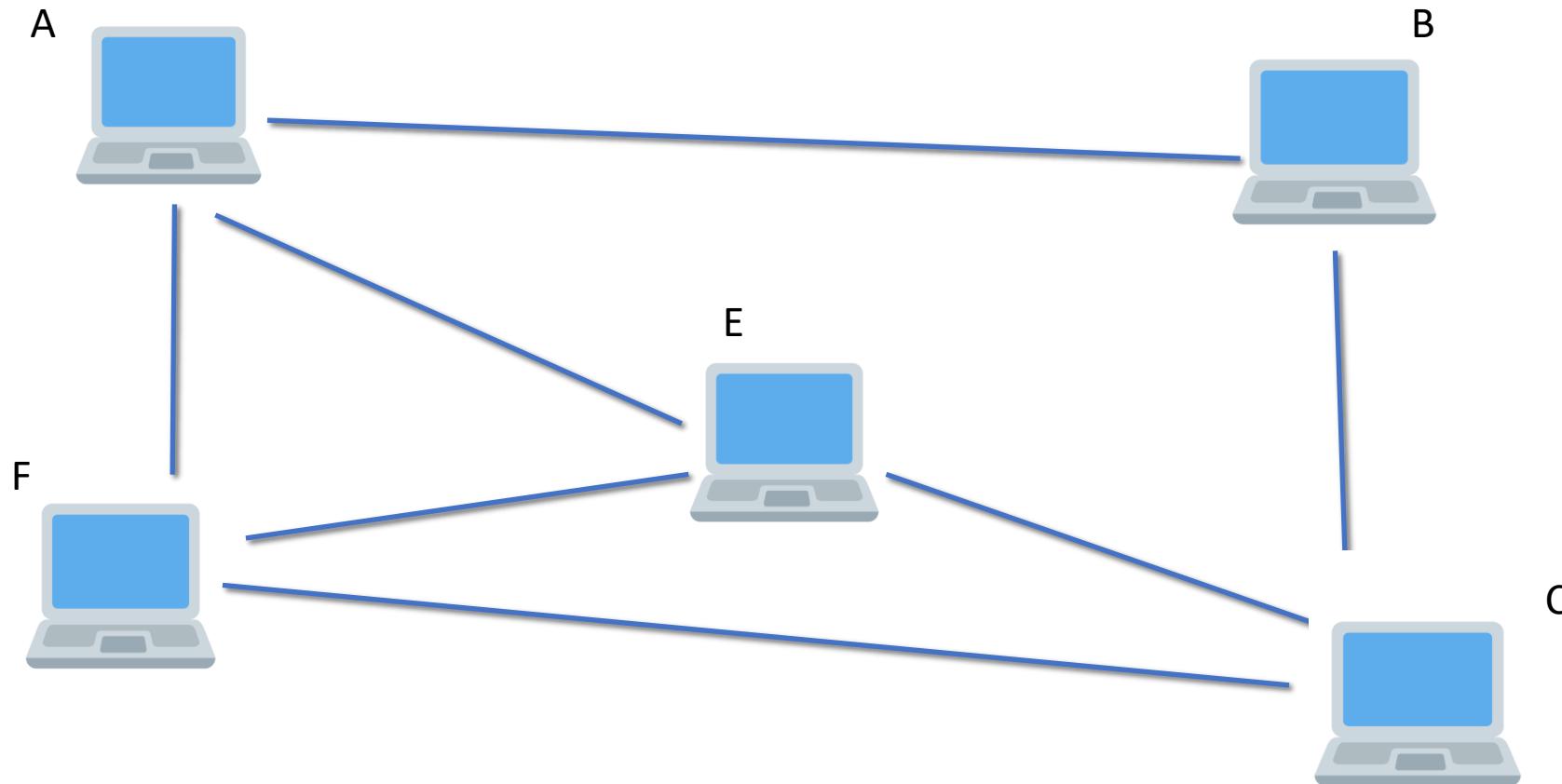
CODE EATER





Ethereum Nodes

Ethereum Nodes



Types of Nodes

Full Node

Light Node

Archive Node

Full Node

- Stores full blockchain data (although this is periodically pruned so a full node does not store all state data back to genesis)
- Participates in block validation, verifies all blocks and states.
- Serves the network and provides data on request.
- All states can be derived from a full node (although very old states are reconstructed from requests made to archive nodes)



Light Node

- Stores only the block header and depends on full node.
- For low capacity devices which cannot afford to store the gigabytes of data.
- The light nodes do not participate in consensus (i.e. they cannot be miners/validators), but they can access the Ethereum blockchain with the same functionality as a full node.



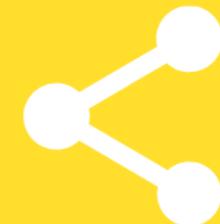
Archive Node

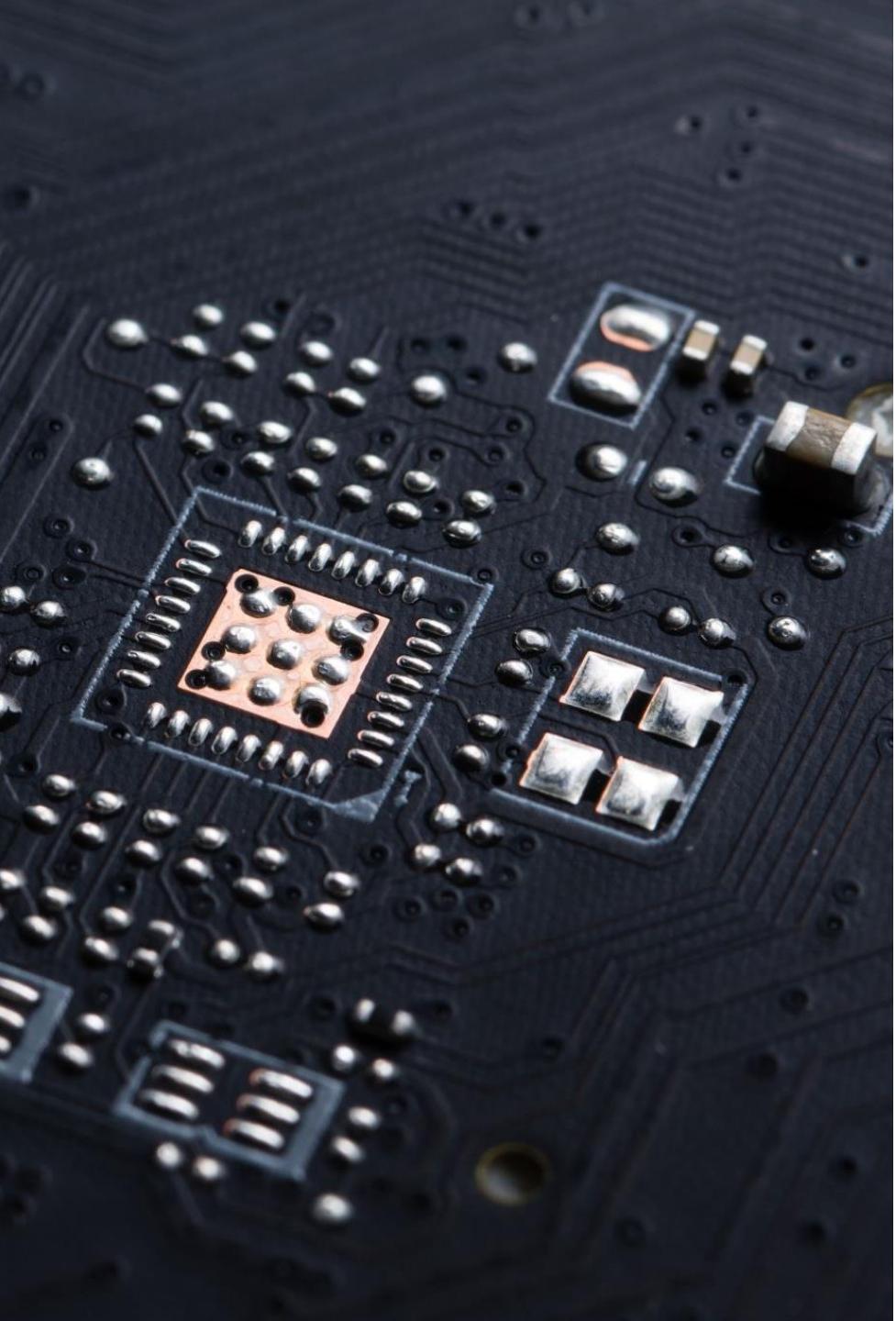
- Stores everything kept in the full node and built an archive of historical data.
- Requires terabytes of diskspace.



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





Ethereum Accounts

Ethereum Accounts

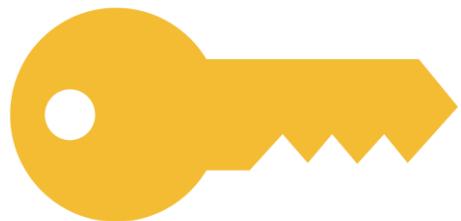
- An Ethereum account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.

Types of Ethereum Accounts

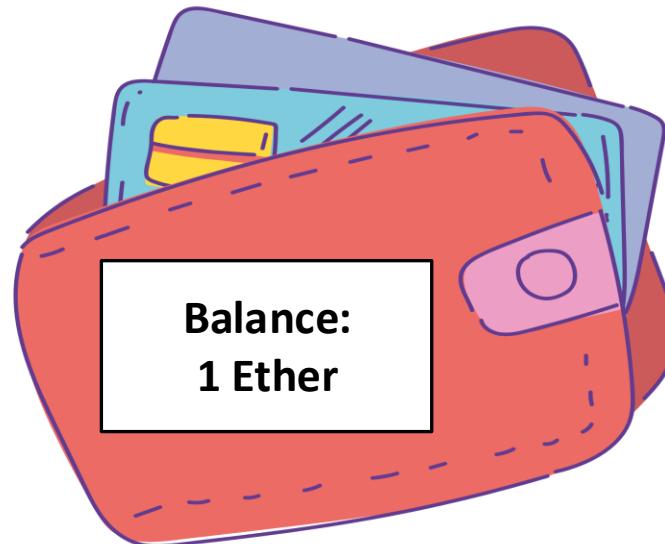
**Externally Owned
Account(EOA)**

Contract Account(CA)

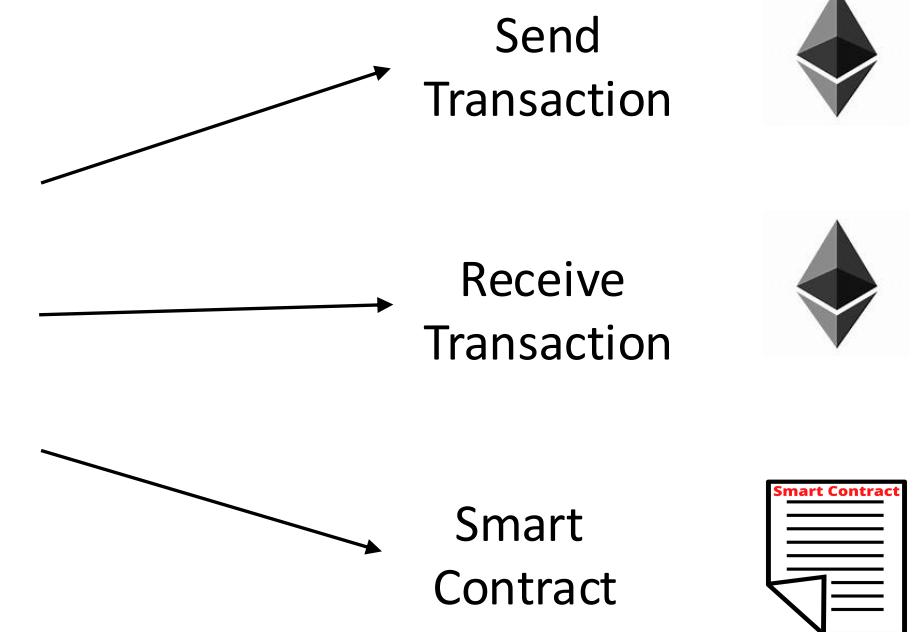
Externally Owned Account(EOA)



Private Key



Wallet



Contract Account (CA)

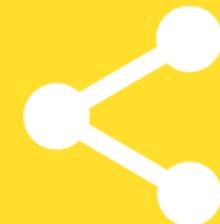
- Controlled by contract code.

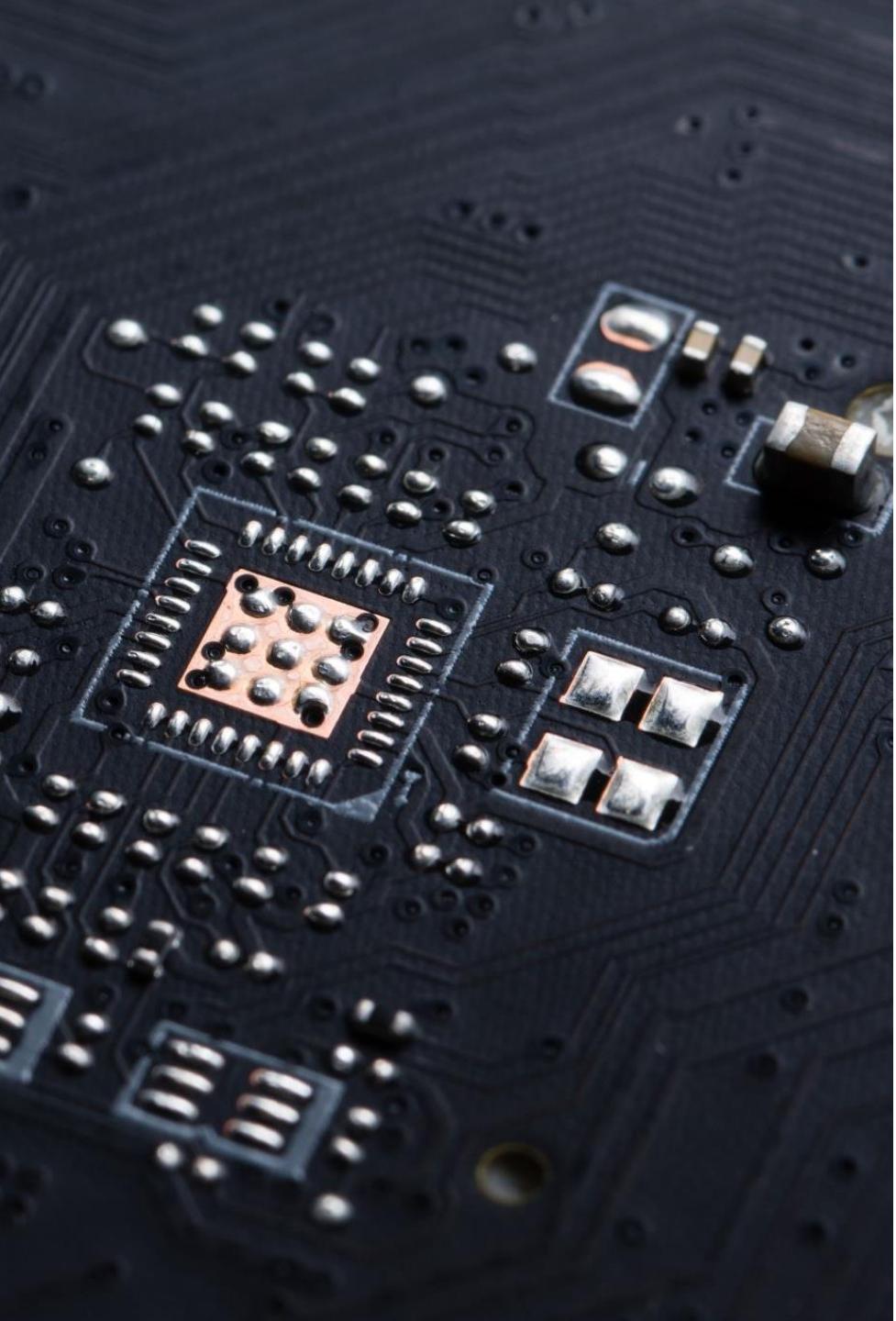
EOA VS CA

EOA	CA
Private Key is needed	No private or public key is needed.
Controlled by Human	Controlled by Contract code
Has a unique address	Has a unique address
Holds ETH balance	Holds ETH balance

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





Smart Contract

Smart Contract





Smart Contract



Smart Contract

Bitcoin Script

Not Turing Complete

Solidity

Turing Complete

Smart Contract

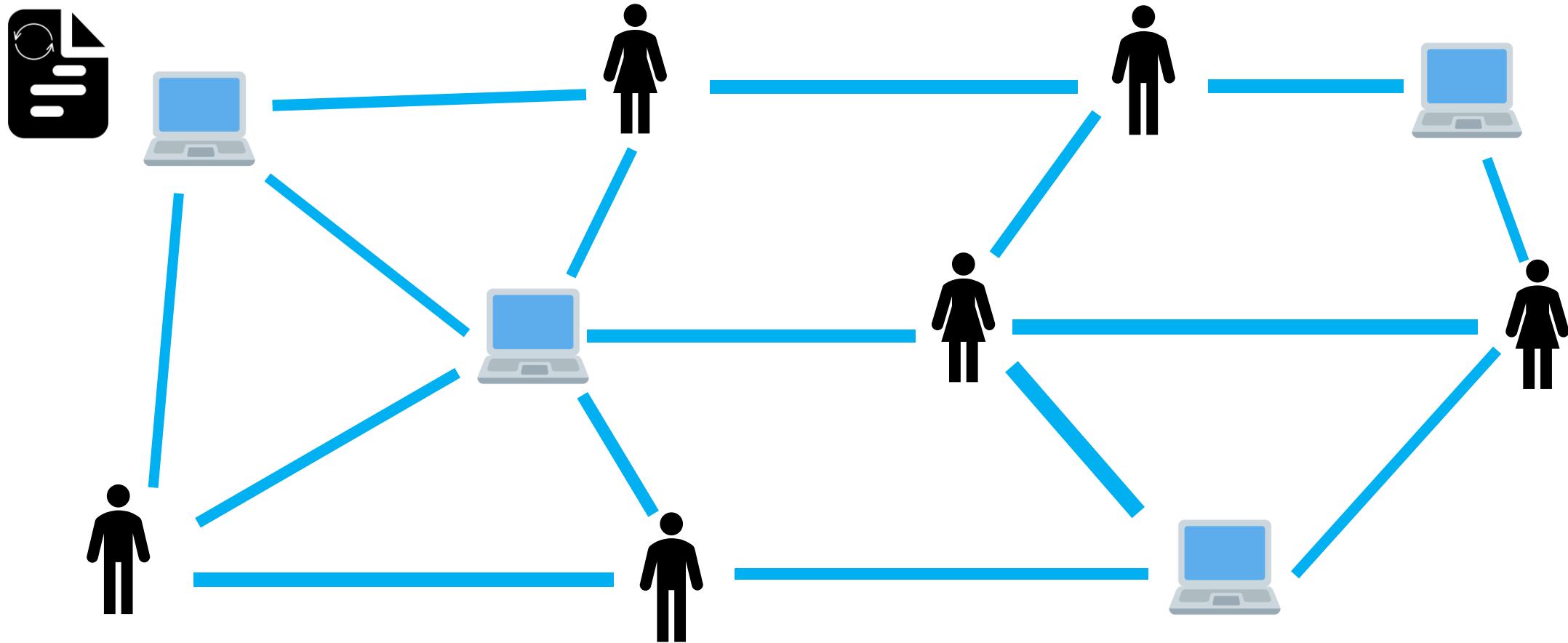
Bitcoin Script

Not Turing Complete

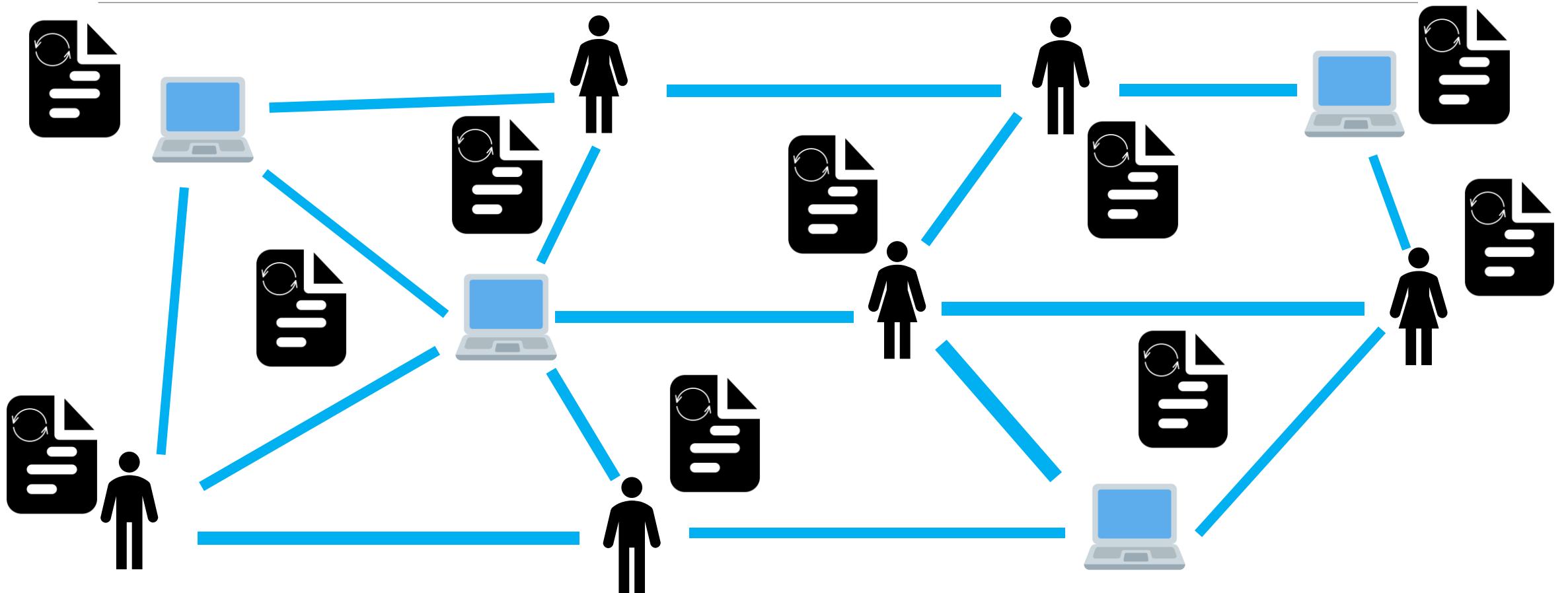
Solidity

Turing Complete

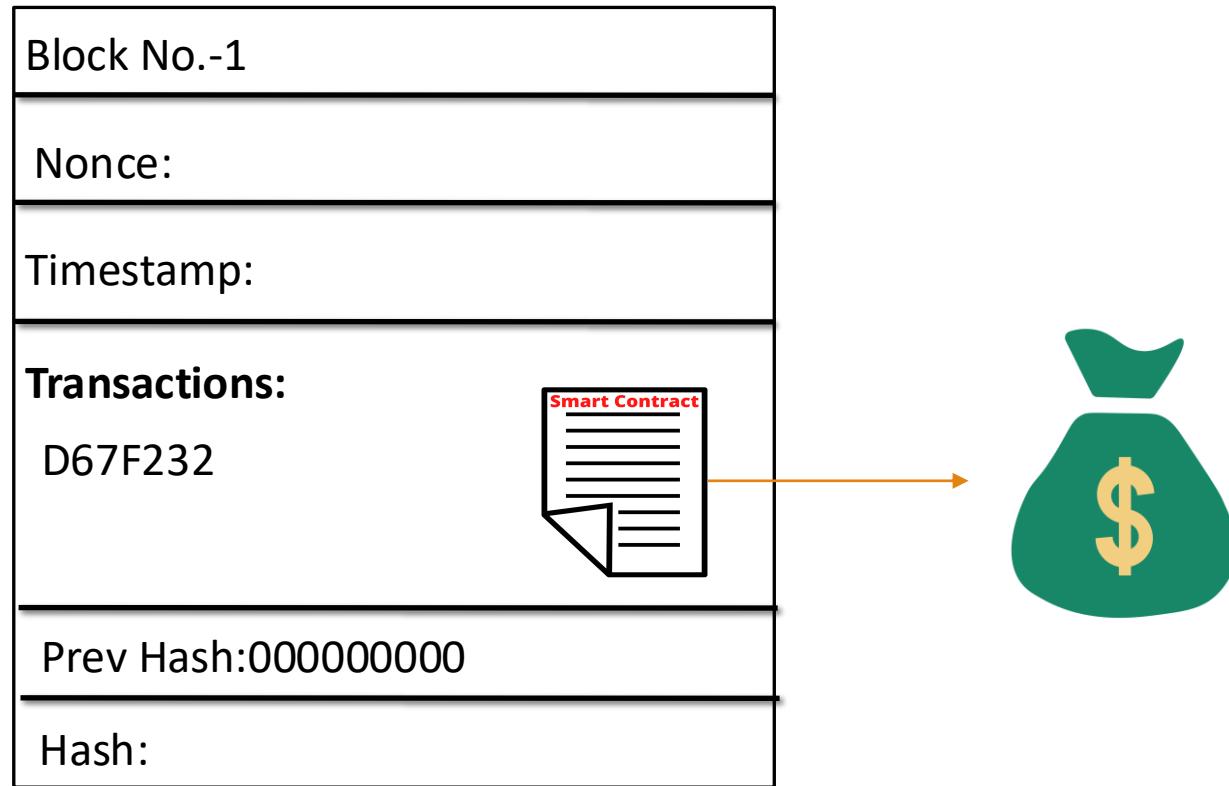
Smart Contract



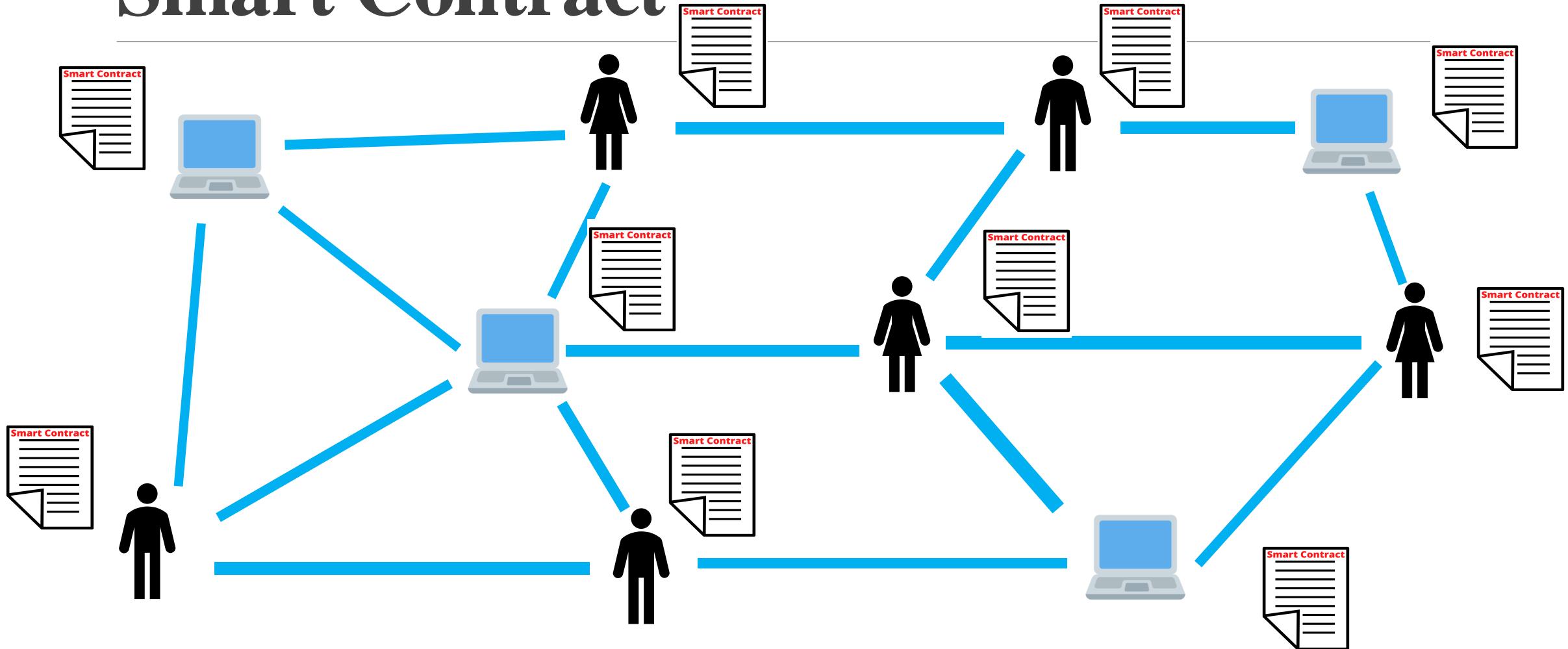
Smart Contract



Smart Contract



Smart Contract



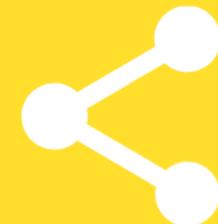
Smart Contract

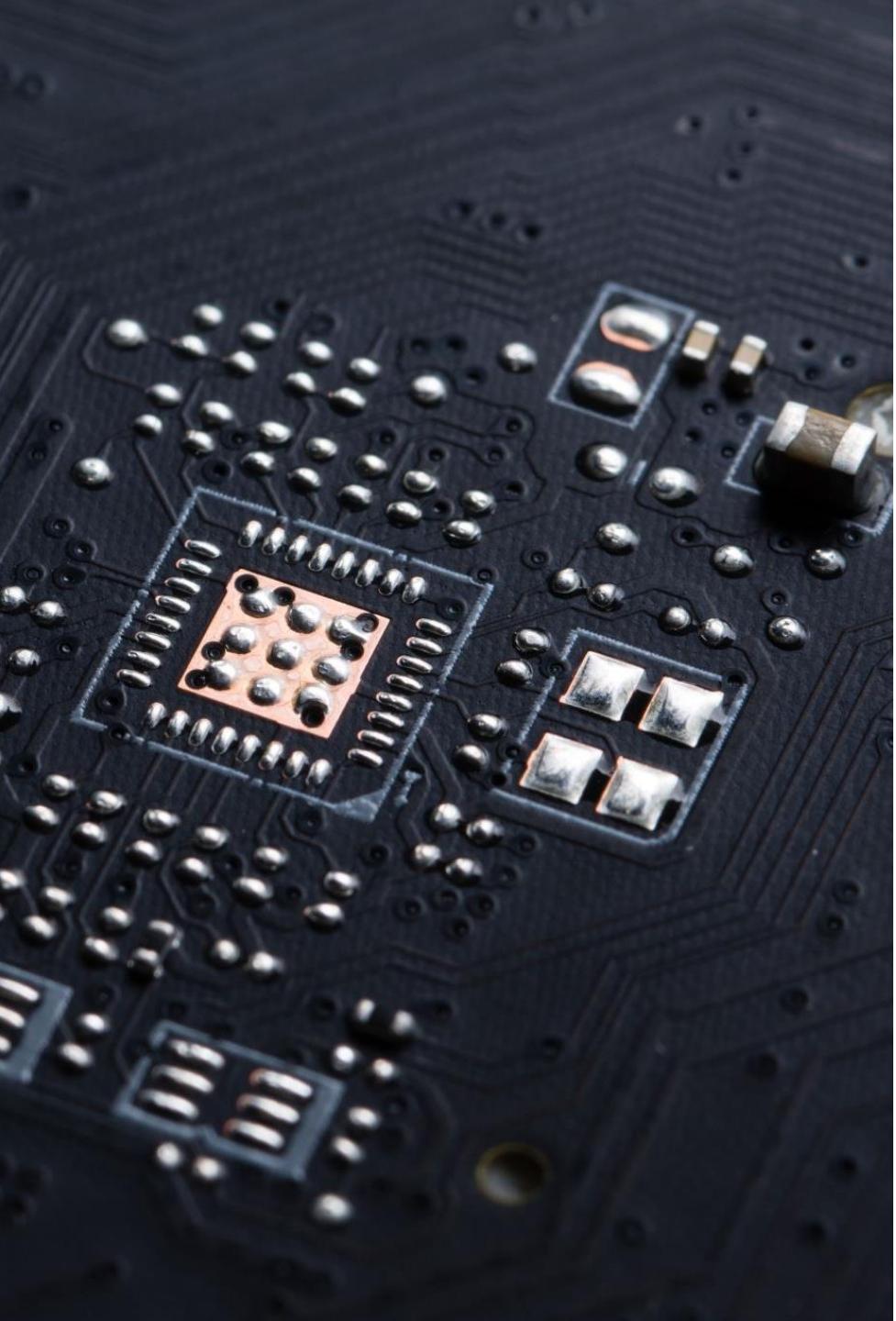
Each node has the following:-

- Current state of all smart contracts.
- History of both transaction and smart contract.

**GIVE THIS VIDEO
A THUMBS-UP !**

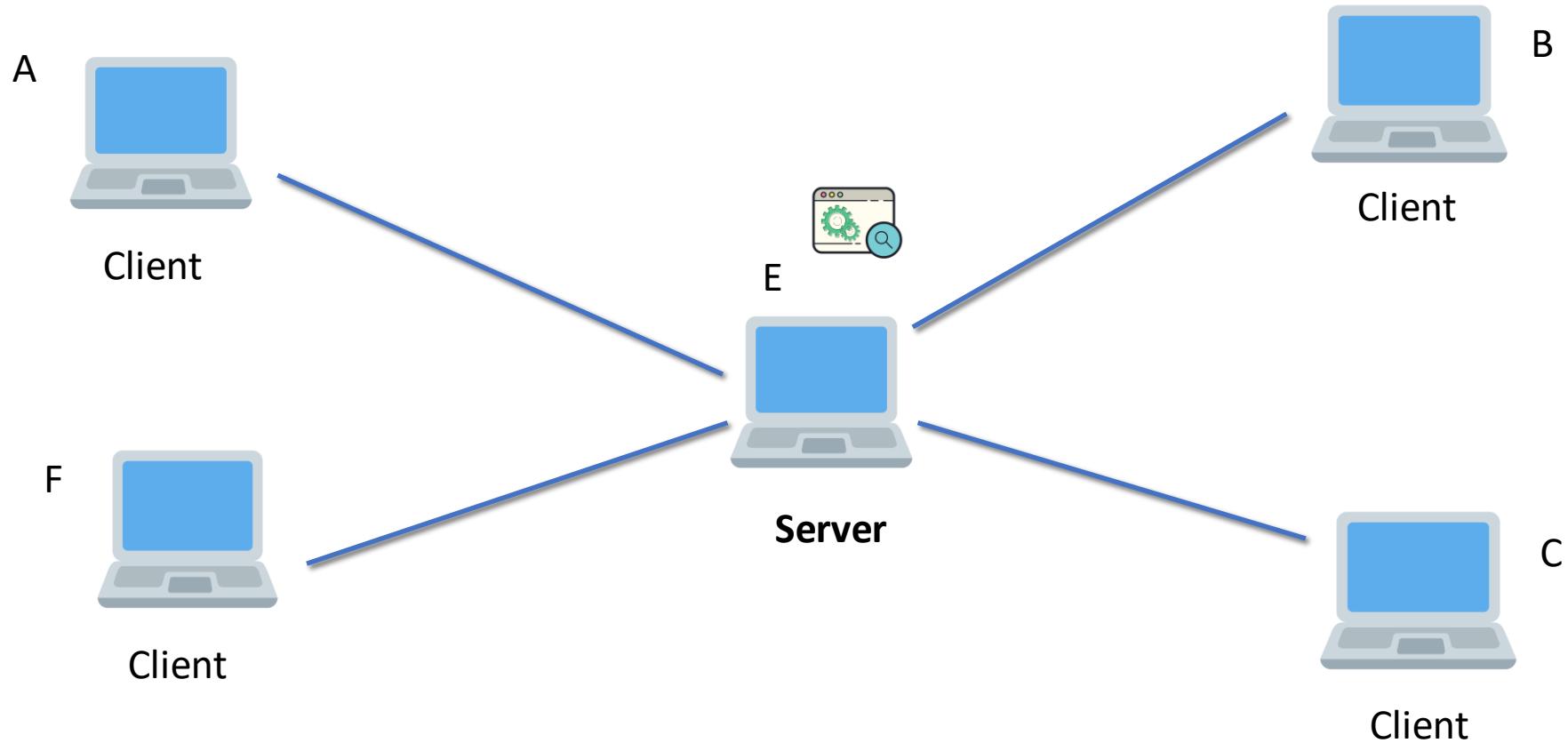
CODE EATER



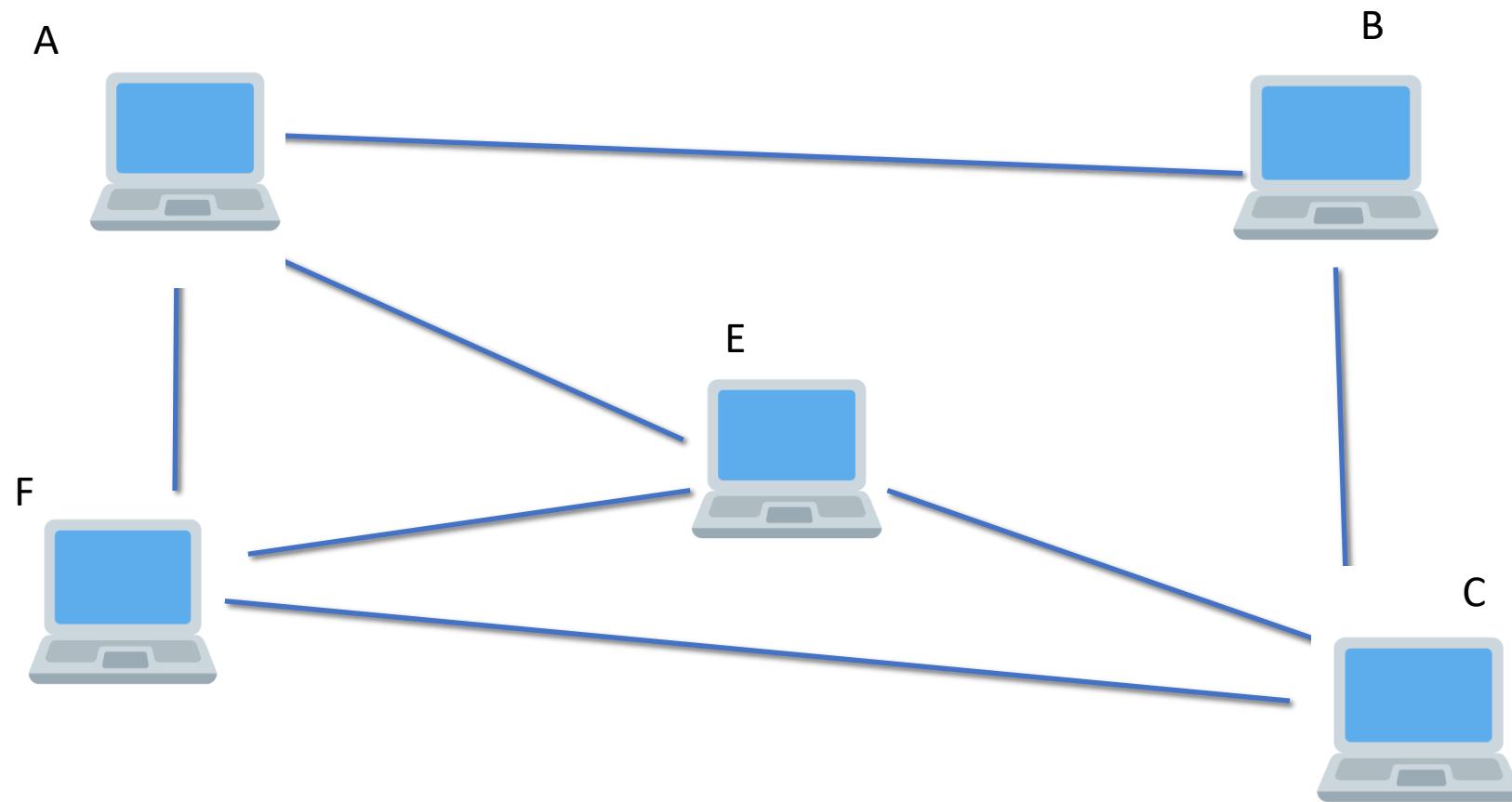


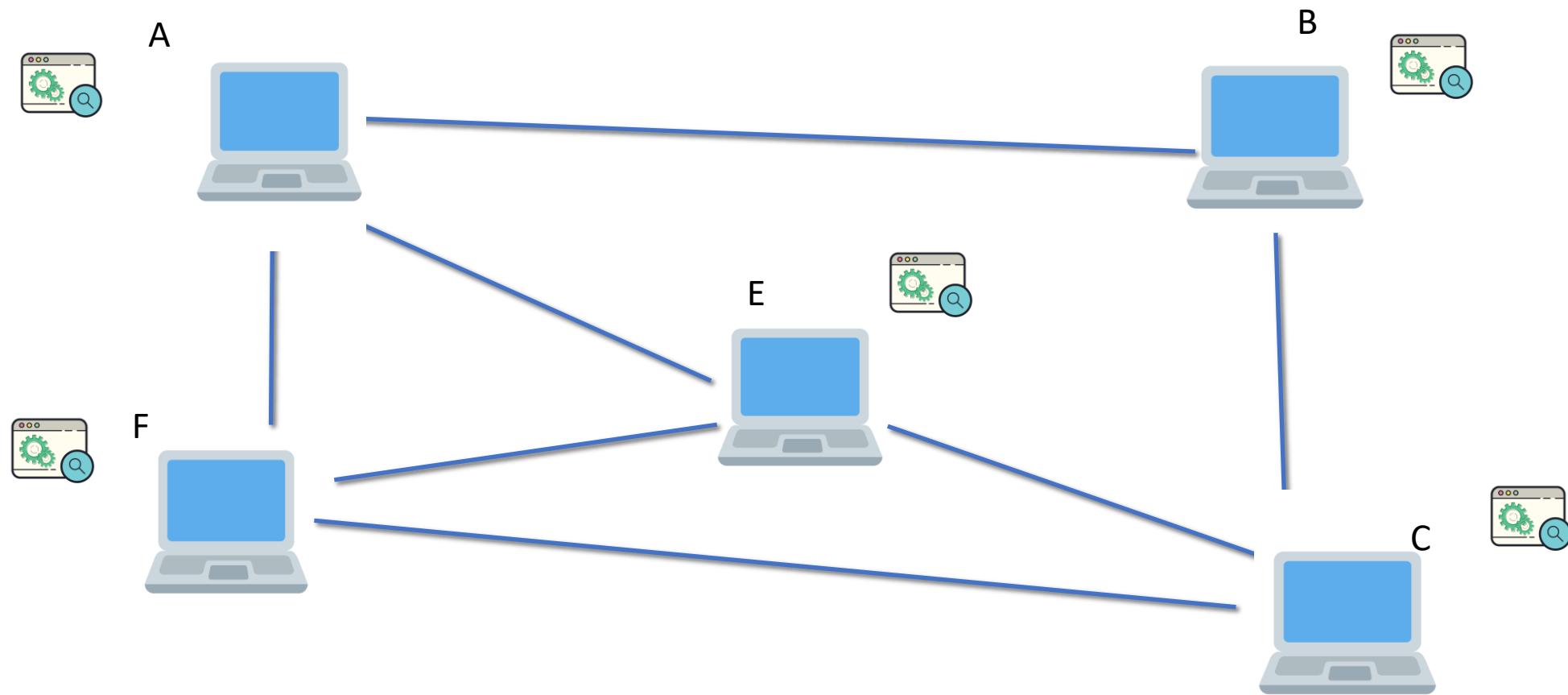
Decentralized Apps(Dapps)

Decentralized Apps(Dapps)



Decentralized Apps(Dapps)



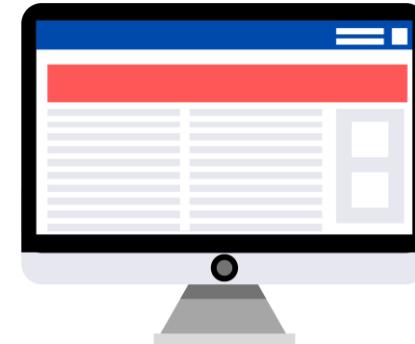
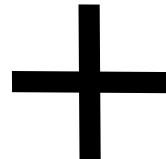


Decentralized Apps(Dapps)

Decentralized Network



Smart Contract

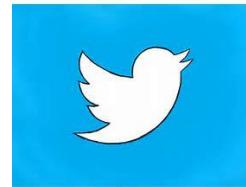


Front End

Search Engine



Social Media



Video Platform



Presearch



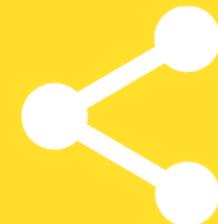
D.tube

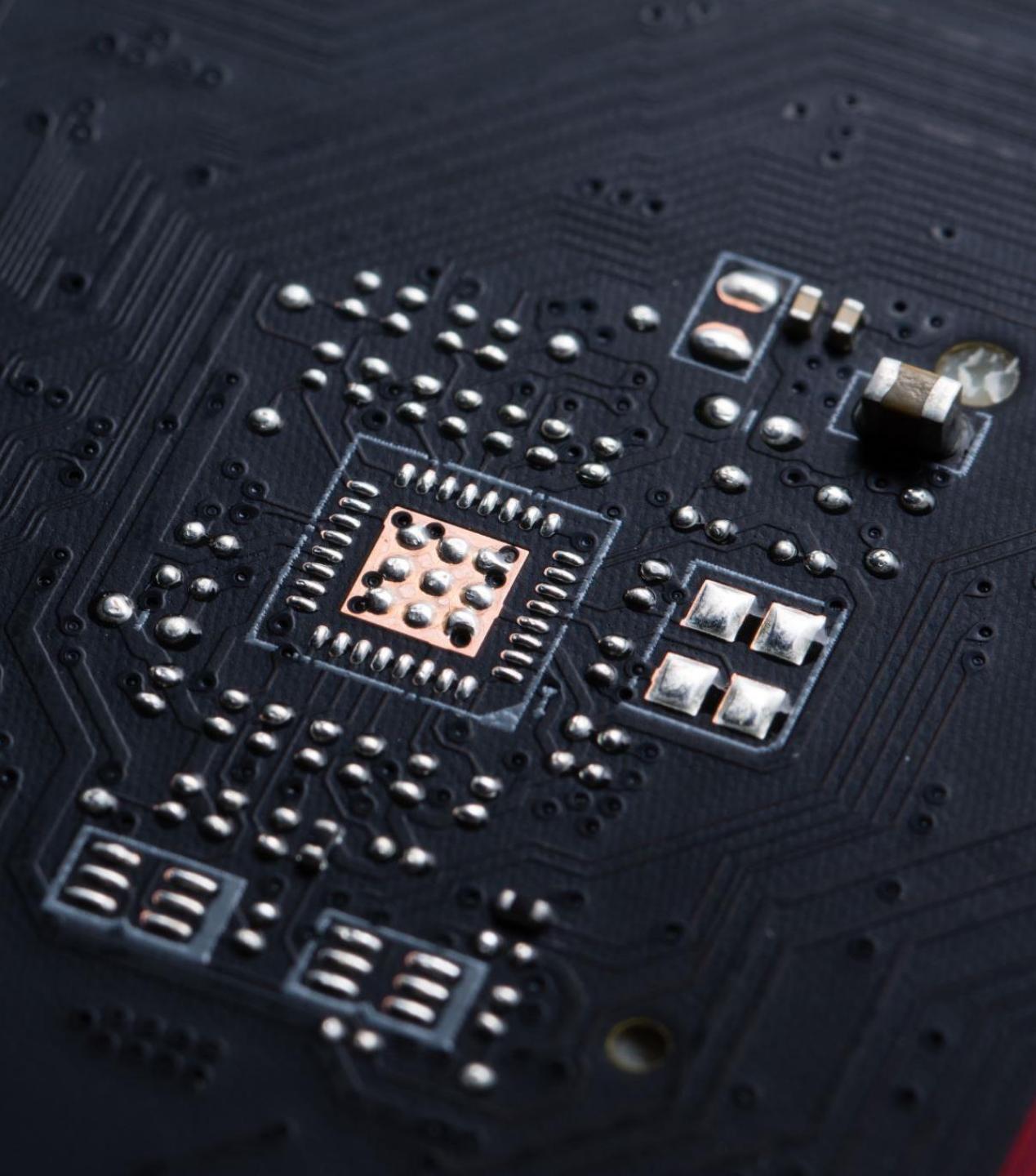
Decentralized Apps(Dapps)

Centralized Apps	Decentralized Apps
Not Trustworthy	Trustworthy
Censorship	No censorship
You pay	They pay
Go down	Can never go down

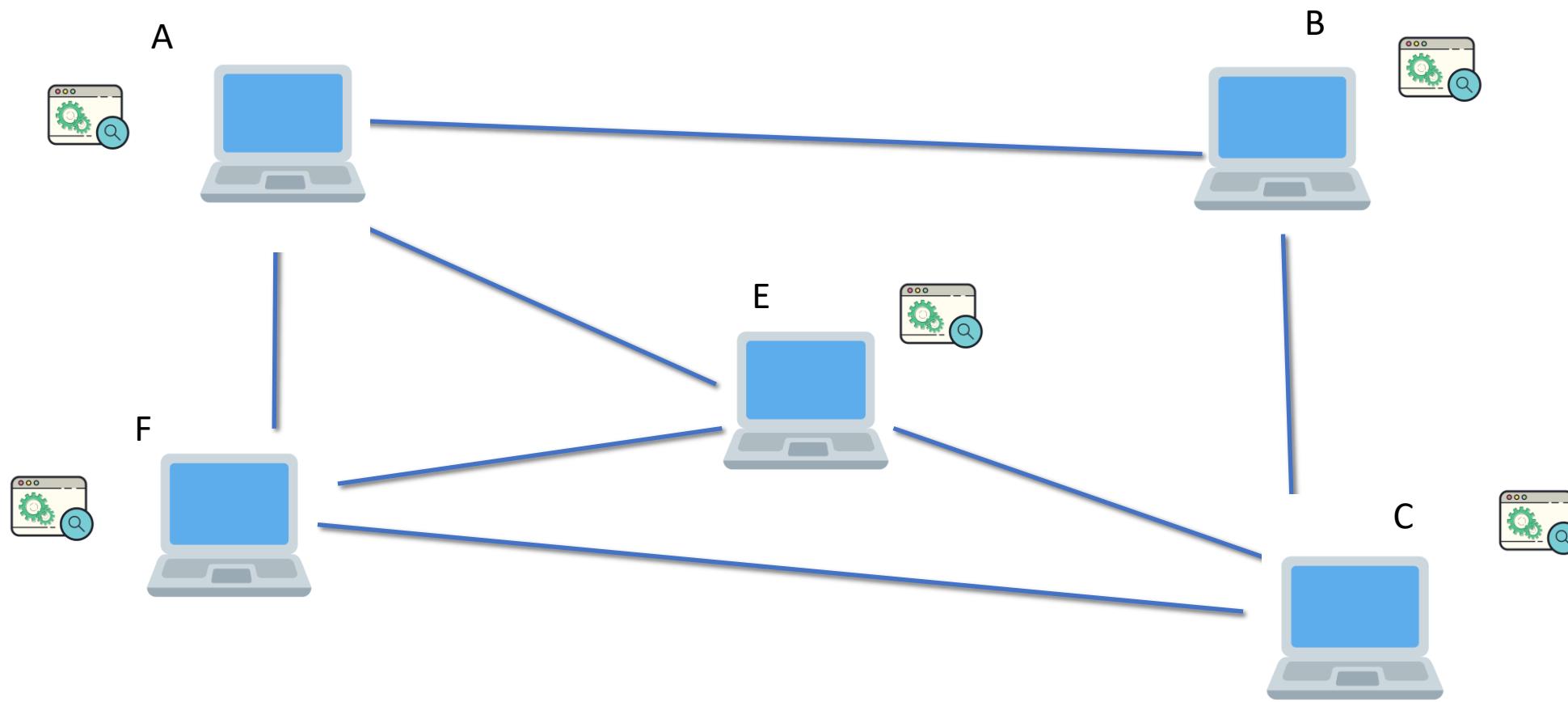
**GIVE THIS VIDEO
A THUMBS-UP !**

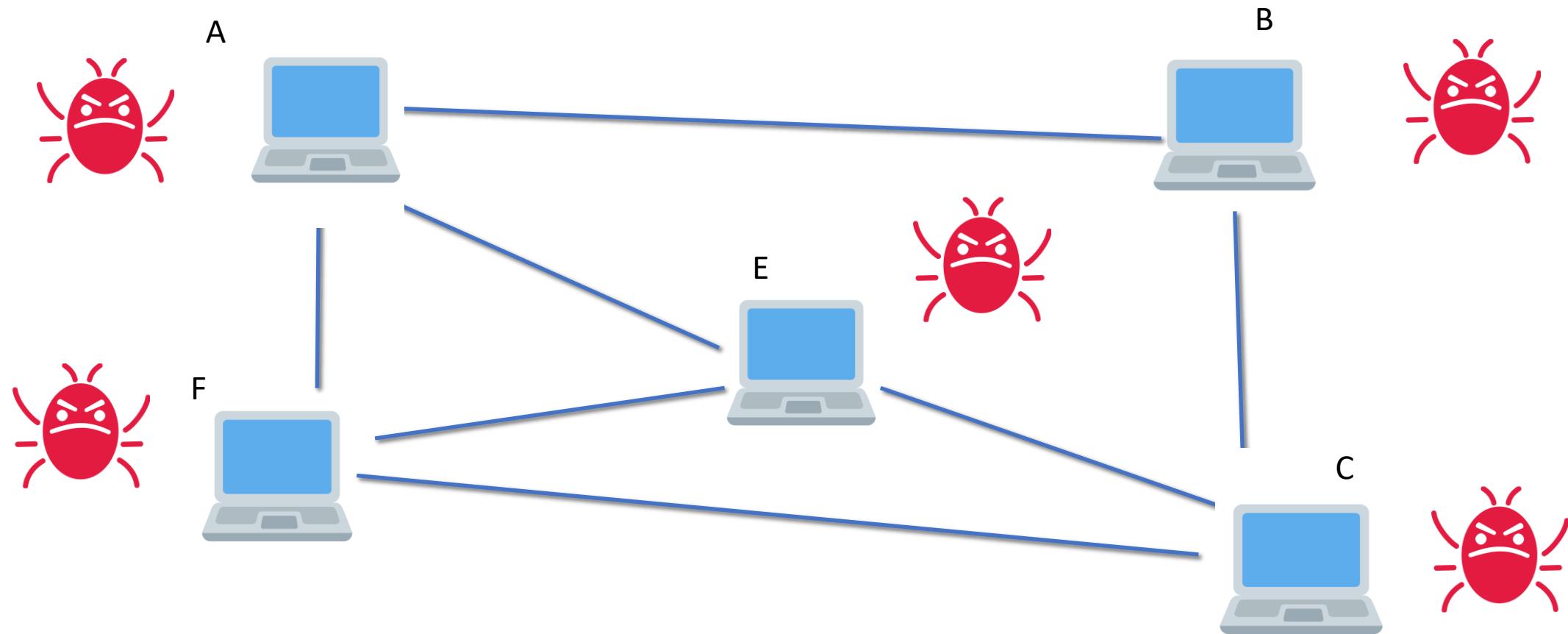
CODE EATER





Ethereum Virtual Machine(EVM)





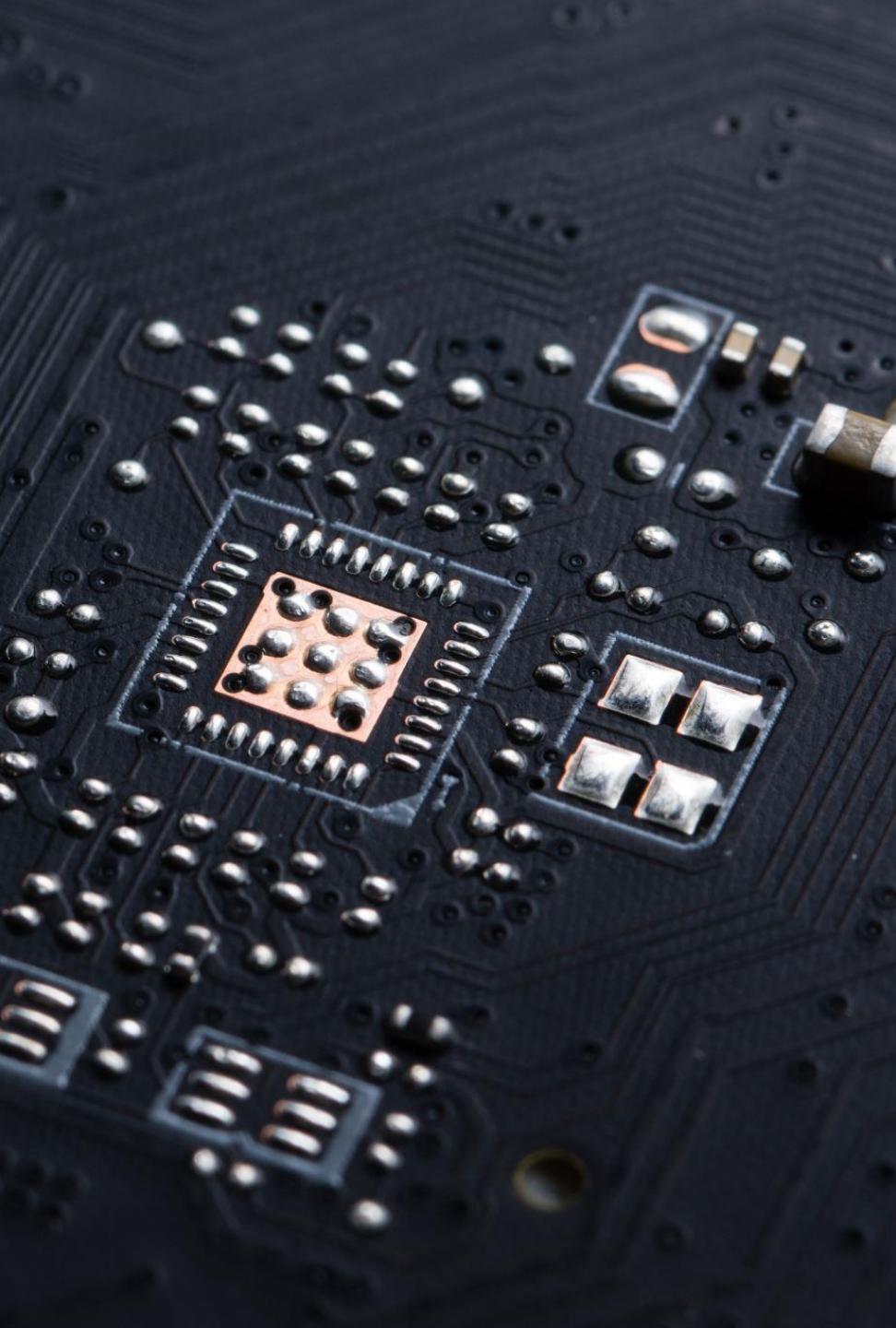
Ethereum Virtual Machine



**GIVE THIS VIDEO
A THUMBS-UP !**

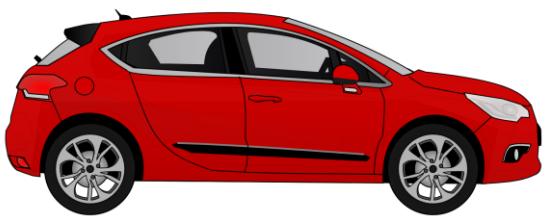
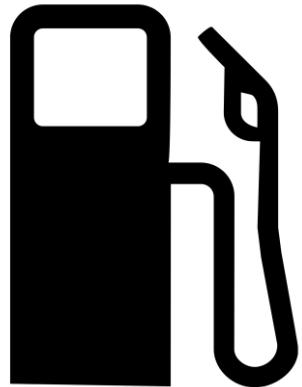
CODE EATER





Ethereum Gas

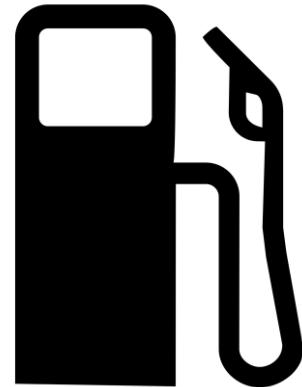
Ethereum Gas



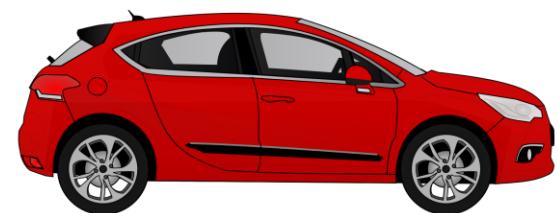
A

B

Ethereum Gas

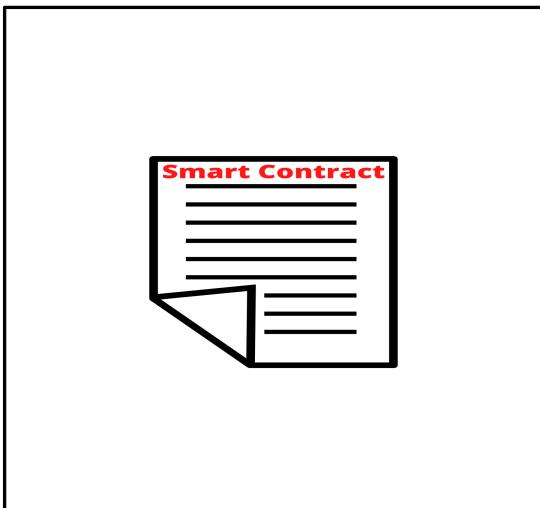


A



B

Ethereum Gas



Ethereum Gas

$$10 * 3 - 6 = ?$$

Multiplication – 5 gas

Subtraction – 3 gas

Equal to – 3 gas

Total gas → 5 + 3 +3 = 11 Gas

Ethereum Gas

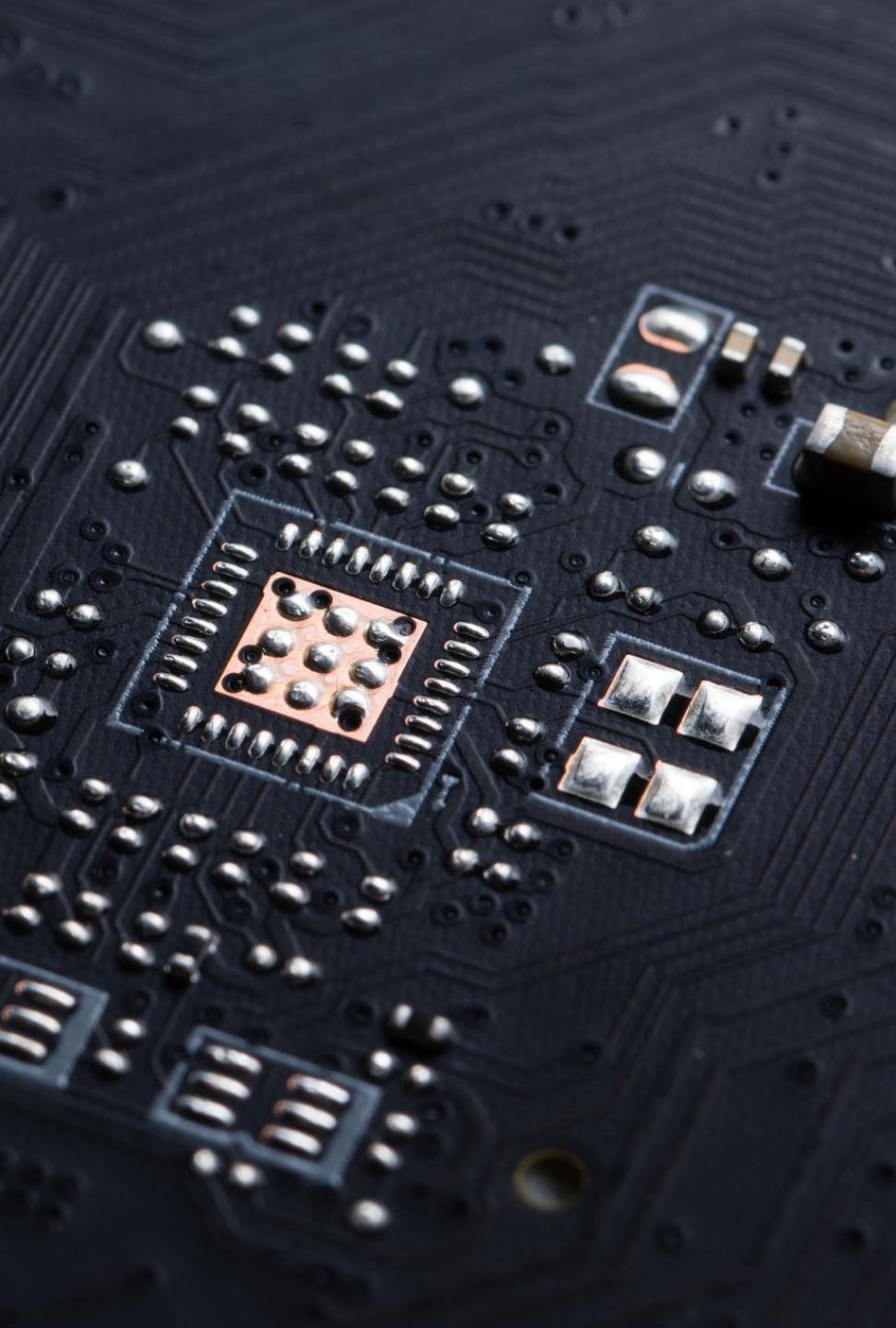
Some important points to note -

- Any transaction that modifies the blockchain costs gas.
- The user that generated the transaction pays for the gas.

**GIVE THIS VIDEO
A THUMBS-UP !**

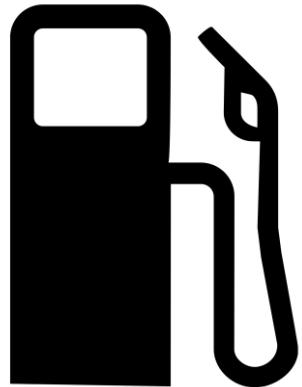
CODE EATER



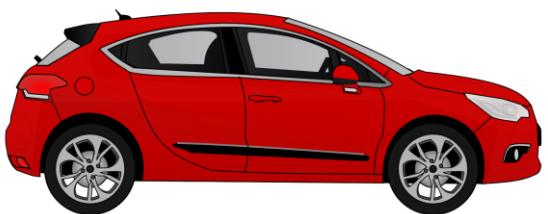


Ethereum Gas Price

Gas Price



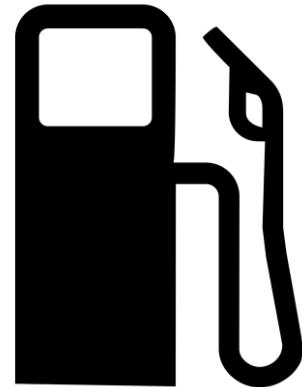
Petrol – 10 liters



A

B

Gas Price

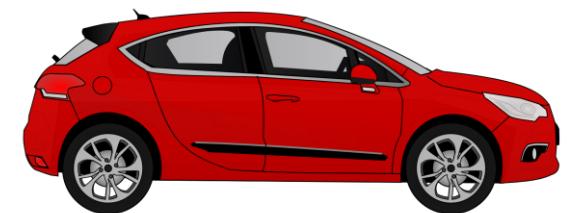


Petrol – 10 liters

Total price= ?

1 liter – Rs.5

Total price= $10 \times 5 =$
Rs. 50



A

B

Gas Price

$$10 * 3 - 6 = ?$$

Multiplication – 5 gas

Subtraction – 3 gas

Equal to – 3 gas

Total gas → $5 + 3 + 3 = 11$ Gas

Gas Price

- It is the amount the sender wants to pay per unit of gas to get the transaction mined. `gasPrice` is set by the sender.
- Gas prices are denoted in gwei. ($1 \text{ gwei} = 10^{-9} \text{ ETH}$)

1 Gas price = 10 gwei

Gas Price

- It is the amount the sender wants to pay per unit of gas to get the transaction mined. `gasPrice` is set by the sender.
- Gas prices are denoted in gwei. ($1 \text{ gwei} = 10^{-9} \text{ ETH}$)

1 Gas price = 100 gwei

Gas Price

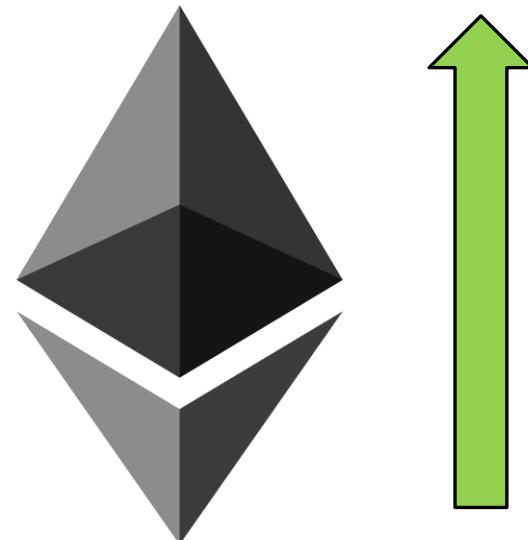
- It is the amount the sender wants to pay per unit of gas to get the transaction mined. `gasPrice` is set by the sender.
- Gas prices are denoted in gwei. ($1 \text{ gwei} = 10^{-9} \text{ ETH}$)

1 Gas price = 1000 gwei



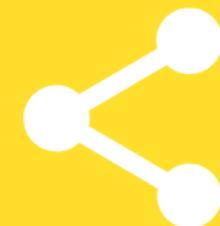
Gas Price

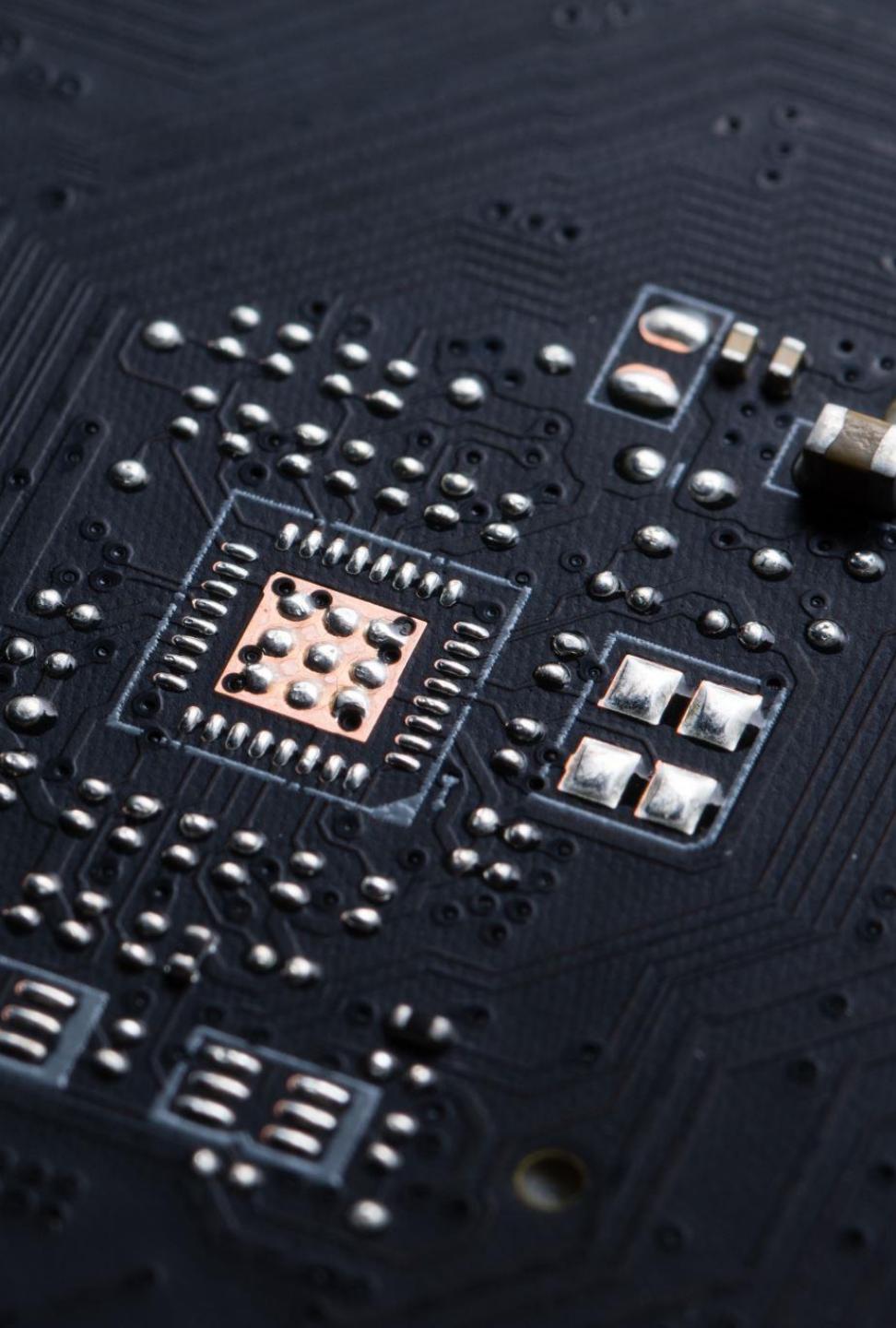
- The higher the gas price the faster the transaction will be mined. It just like the transaction in Bitcoin.



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

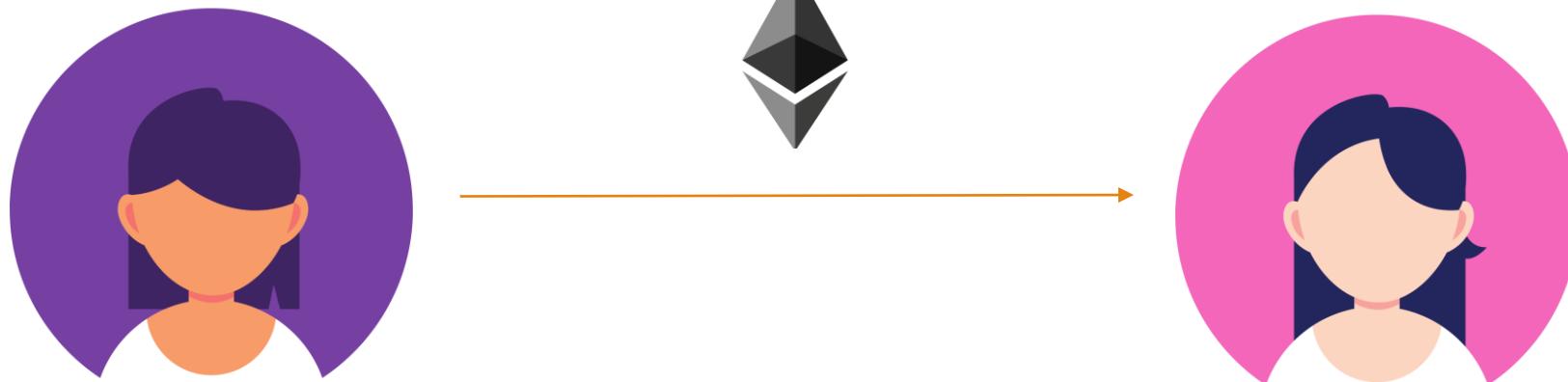




Ethereum Gas Limit

Gas Limit

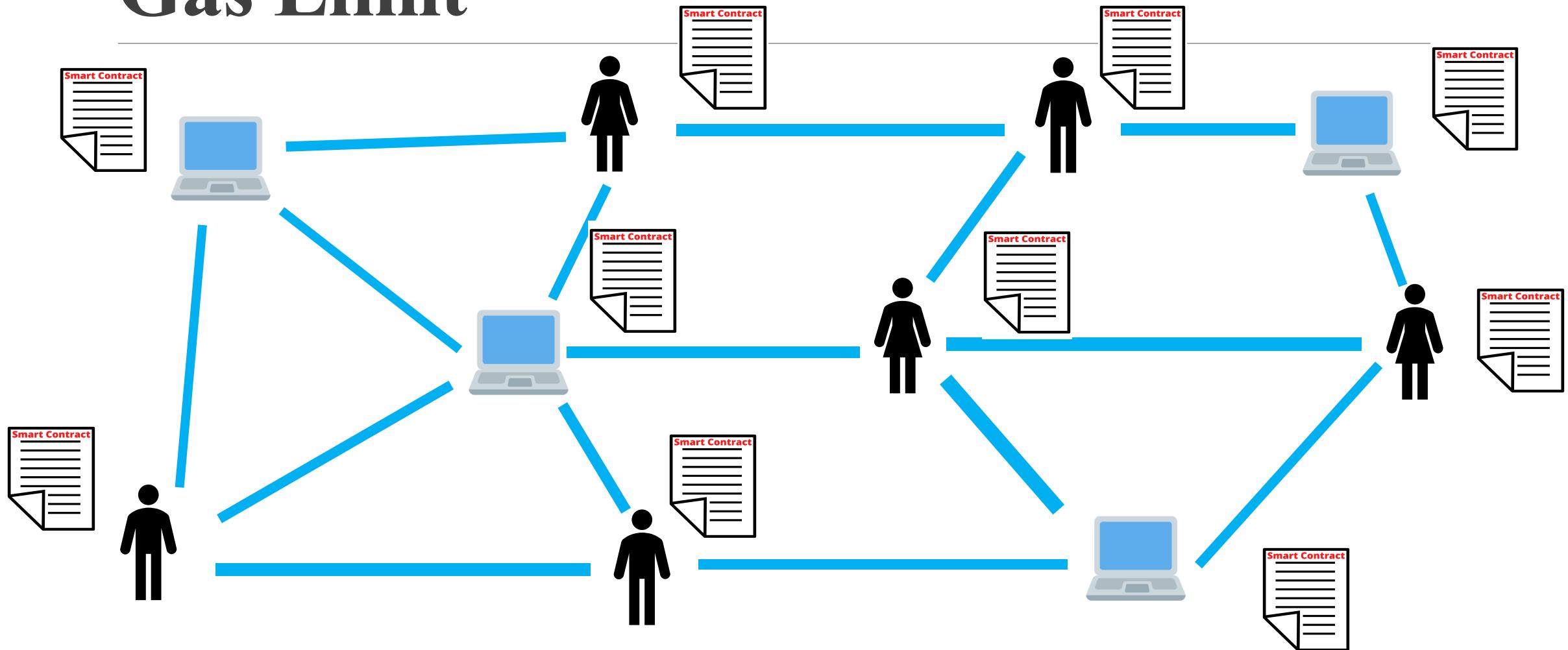
- It is the maximum gas the transaction can consume.
- Set by the sender.



Gas Limit



Gas Limit



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

Case 1: When transaction gas limit is 21,000 units.

A sets the gas price per unit = 100 gwei.

Transaction gas limit = 21,000 units.

Total fee will be: Gas units(limit) * Gas price per unit

Total fee will be: $21,000 * 100 = 210,0000$ gwei or 0.0021 ETH

Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

Case 2: When gas transaction limit < 21000 units.

Transaction gas limit = 20,000 units.

Transaction Fail

Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

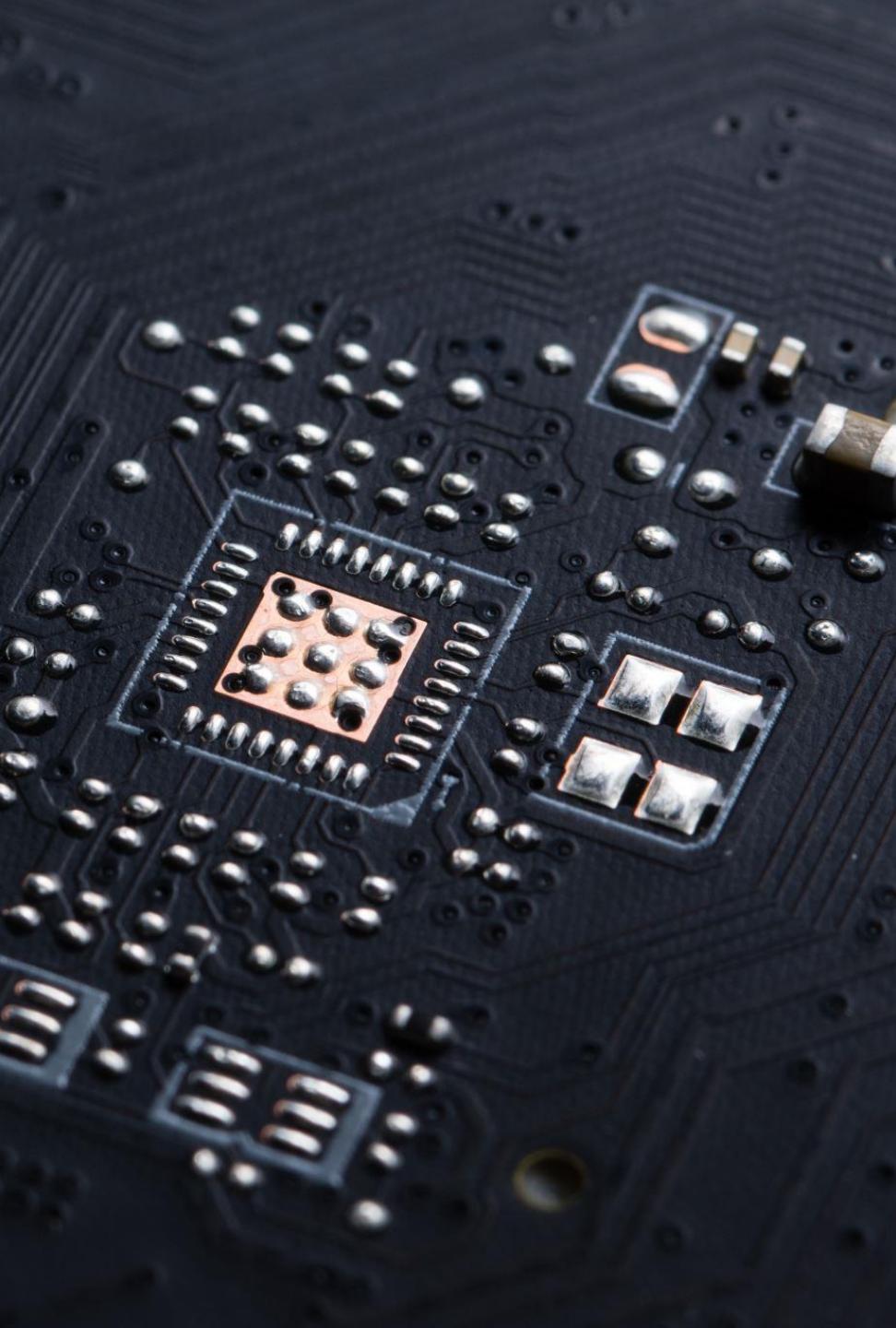
Case 3: When gas transaction limit > 21000 units.

Transaction gas limit = 22,000 units.

22,000 – 21000 = 1000 will be returned

Gas Limit

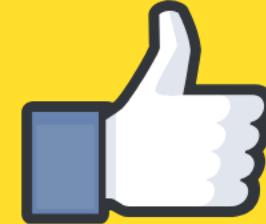
Q) What is the use of Gas Limit ?

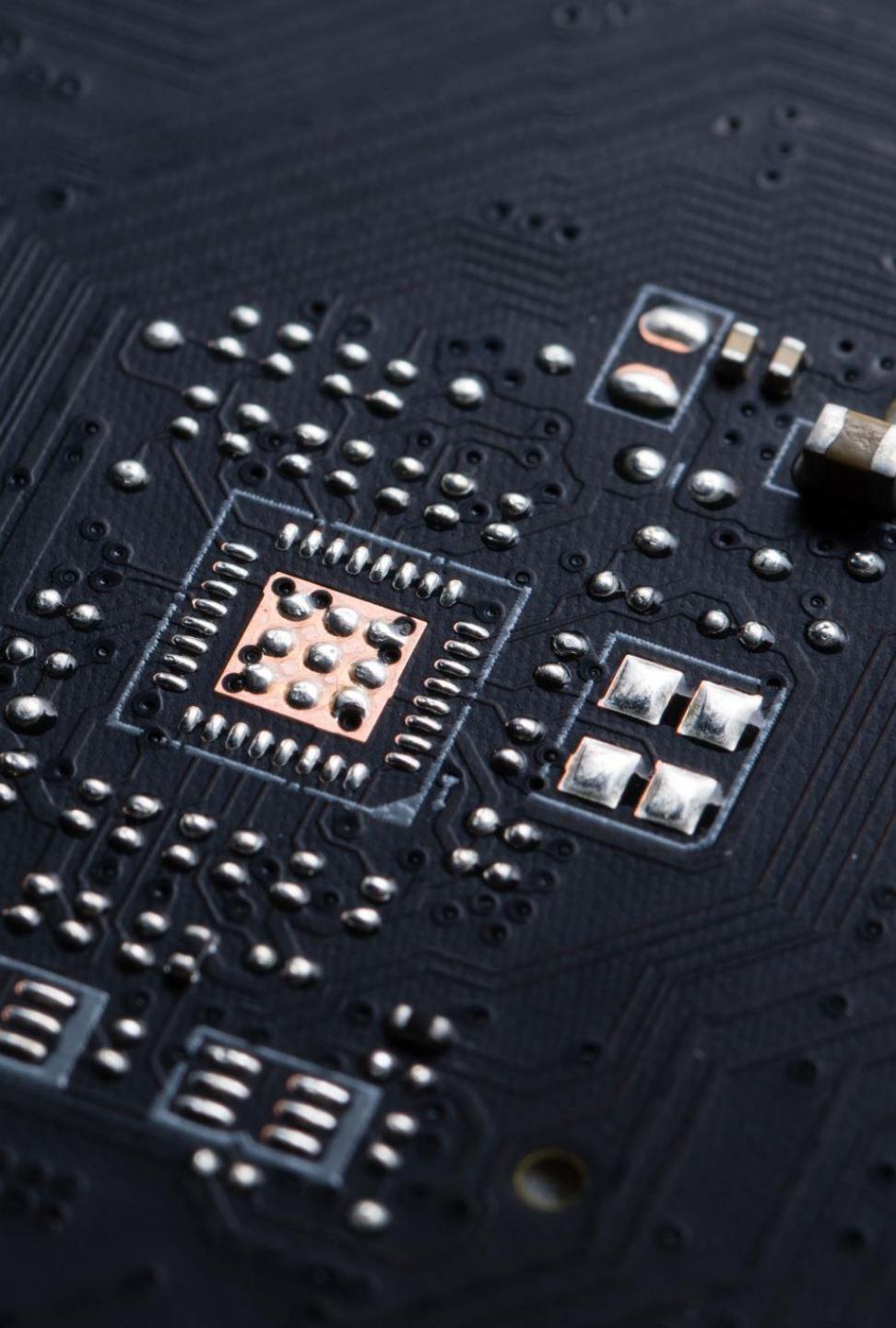


Ethereum Demo

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



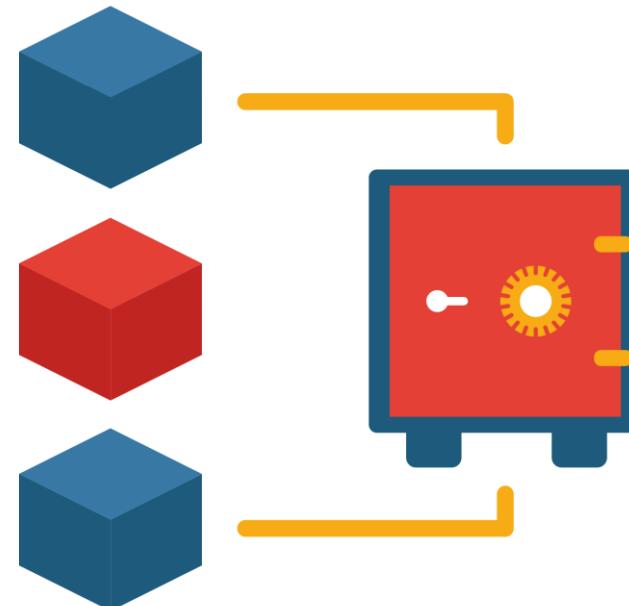


Ethereum 2.0

ETH 2.0

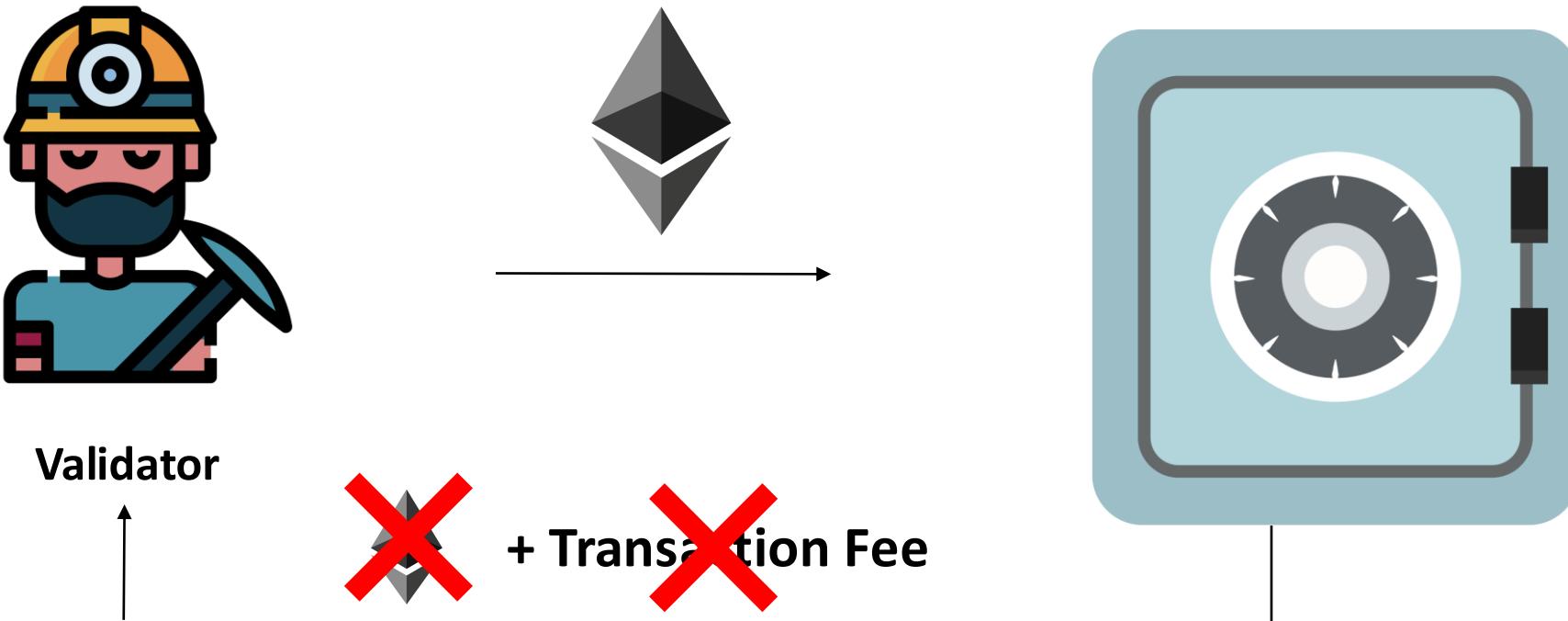


POW

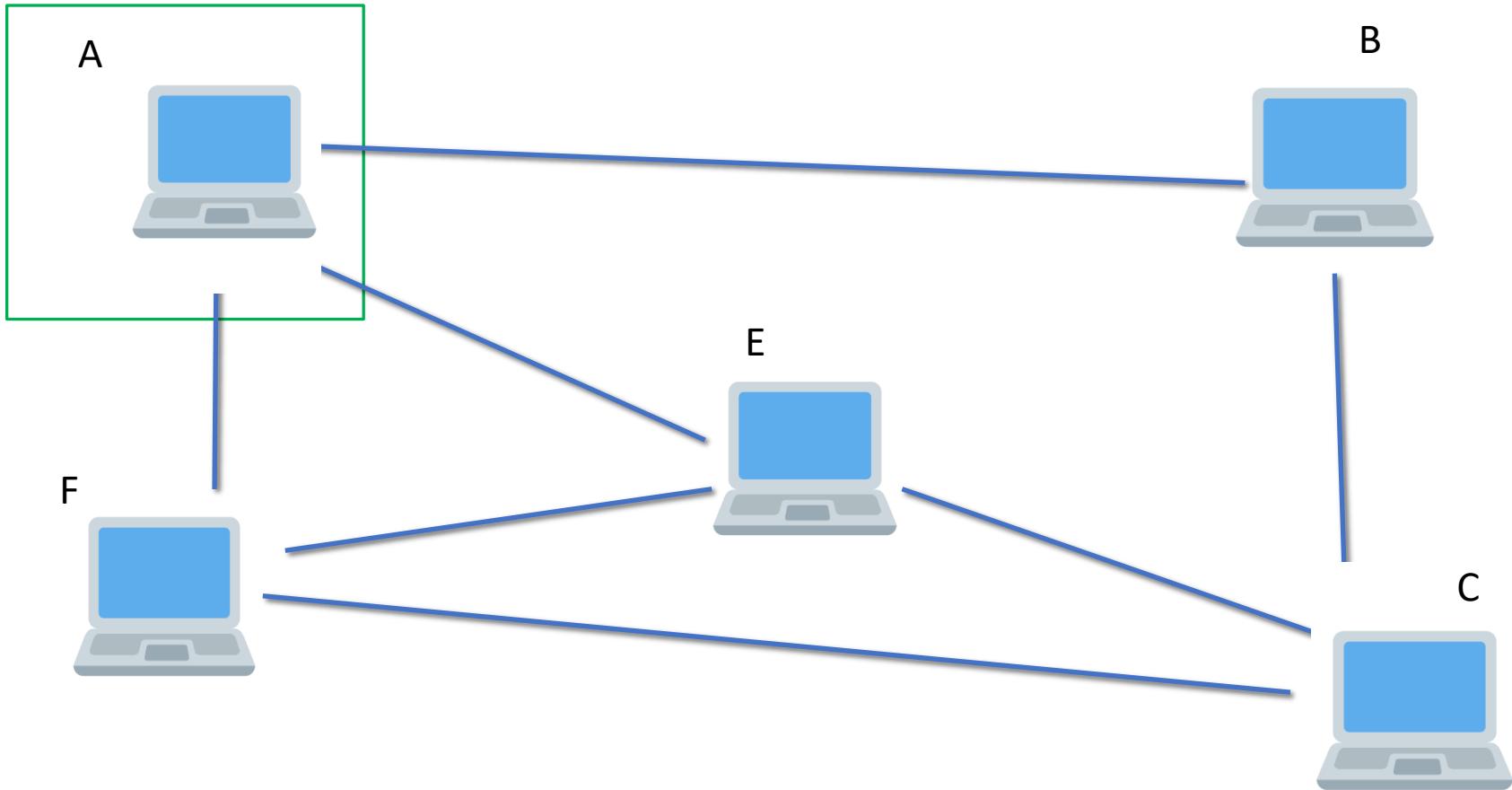


POS

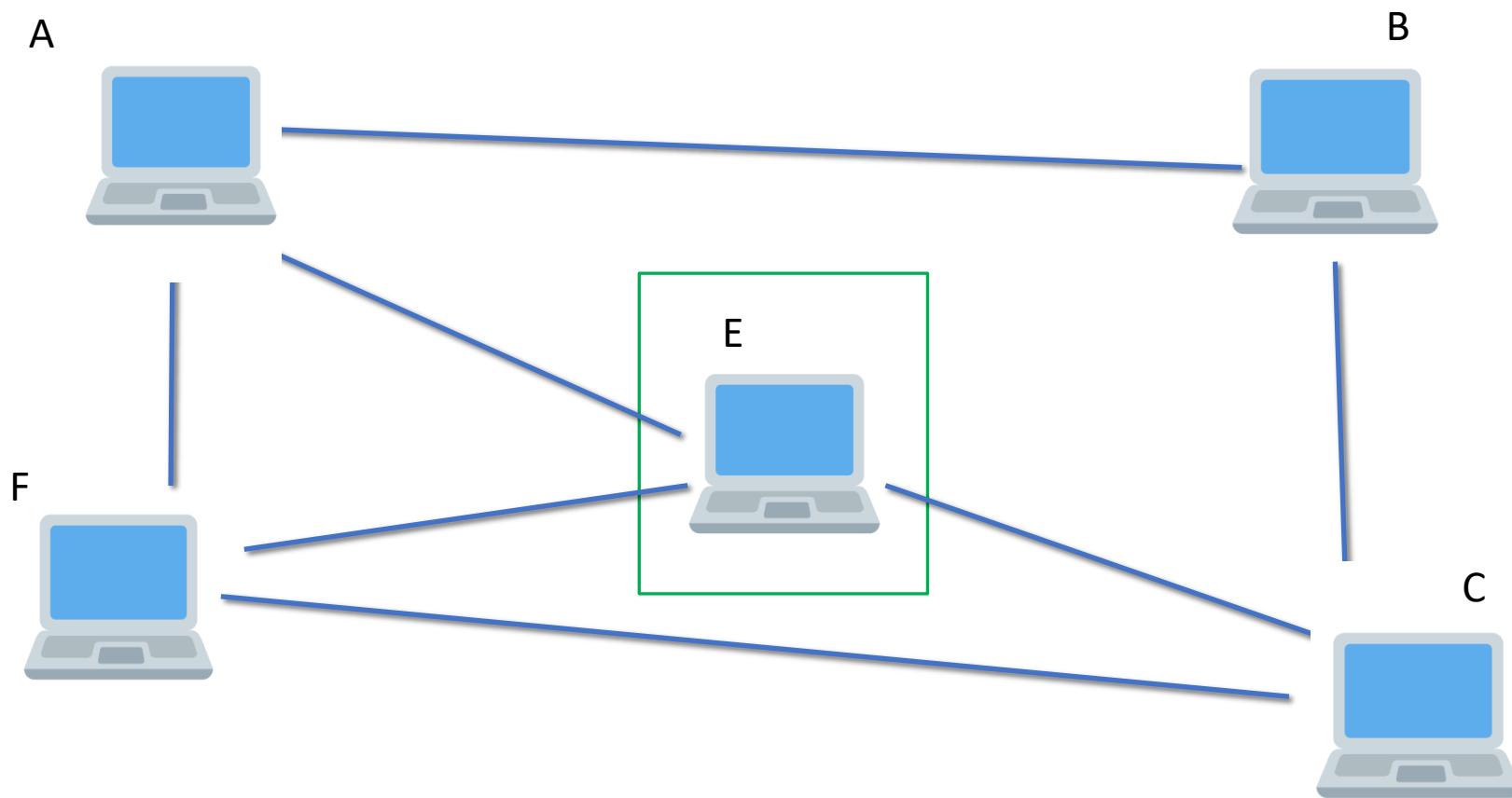
Proof of Stake



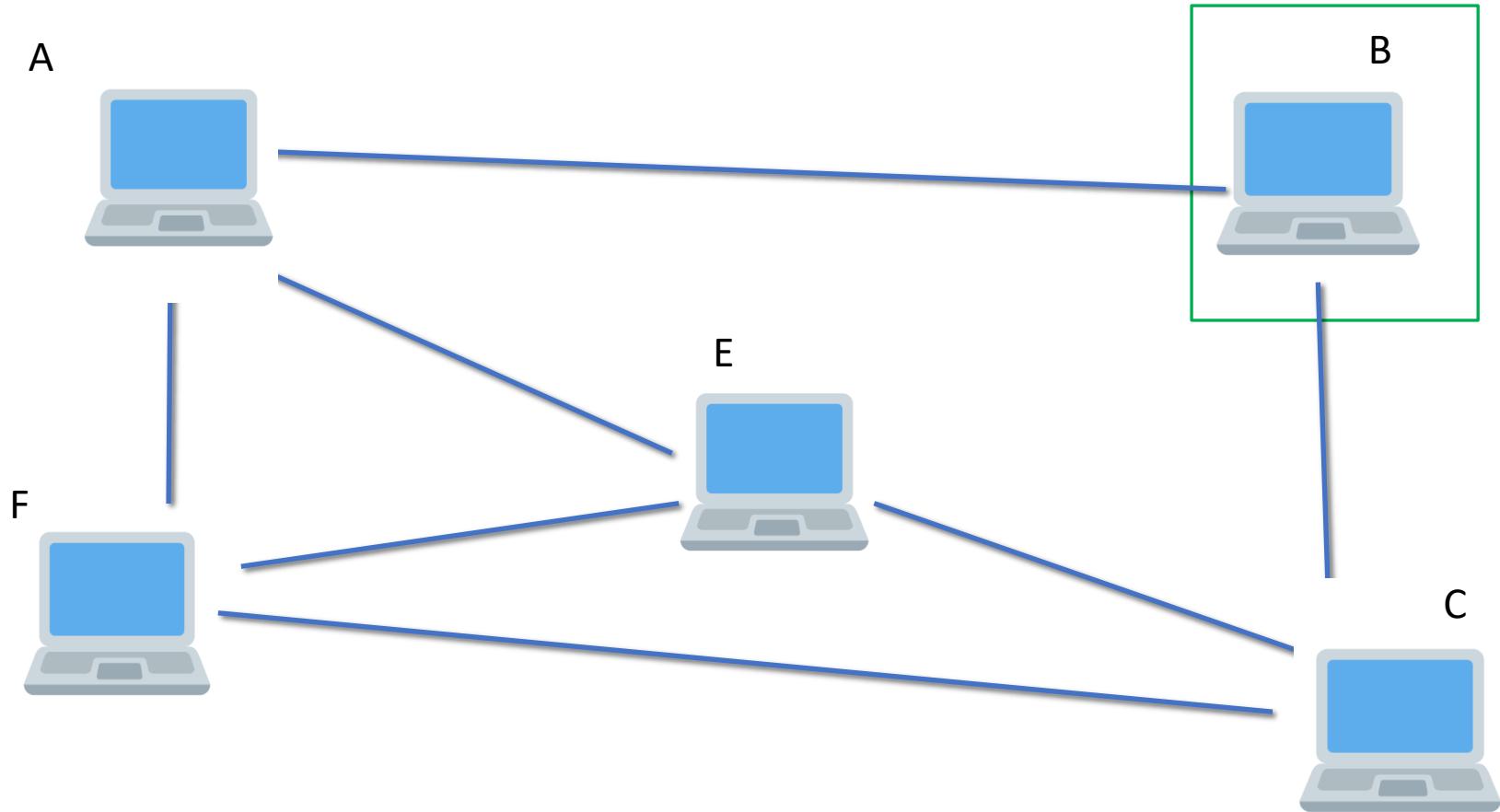
Proof of Stake



Proof of Stake



Proof of Stake



Proof of Stake

- The more ether you pay the more chances of getting randomly selected you have.

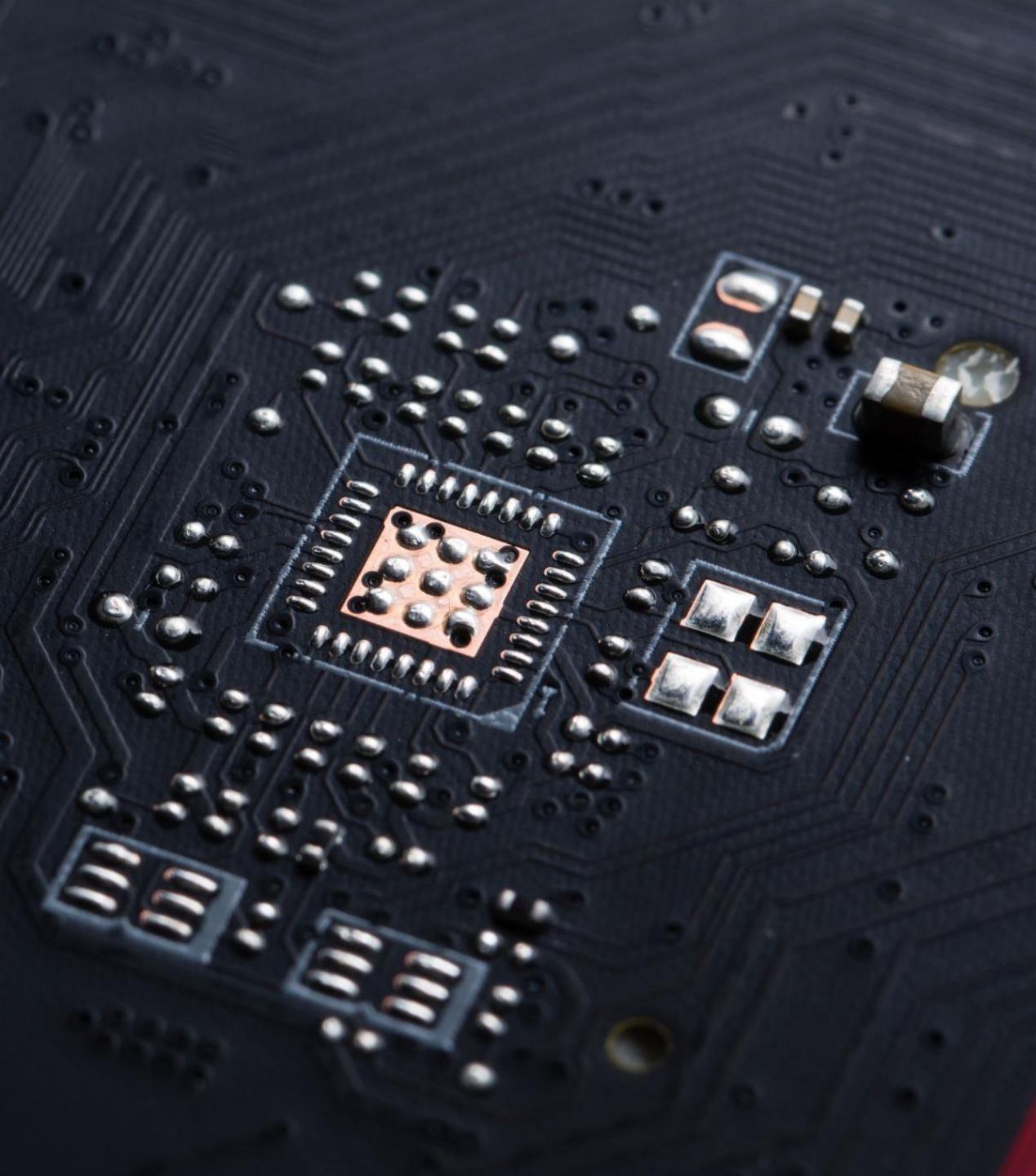
POW vs POS

Proof Of Work(PoW)	Proof Of Stake(PoS)
Miners	Validators
High performance hardware required.	Mobile or Laptop are enough.
Lots of electricity required.	Not much electricity is required.
The more hashing power you have the more blocks you can validate.	The more ETH you stake the more blocks you can validate.
Attack to happen 51% hashing power is required.	Attack to happen 51% of stake is required.
Competition is there.	Random selection is there.

**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

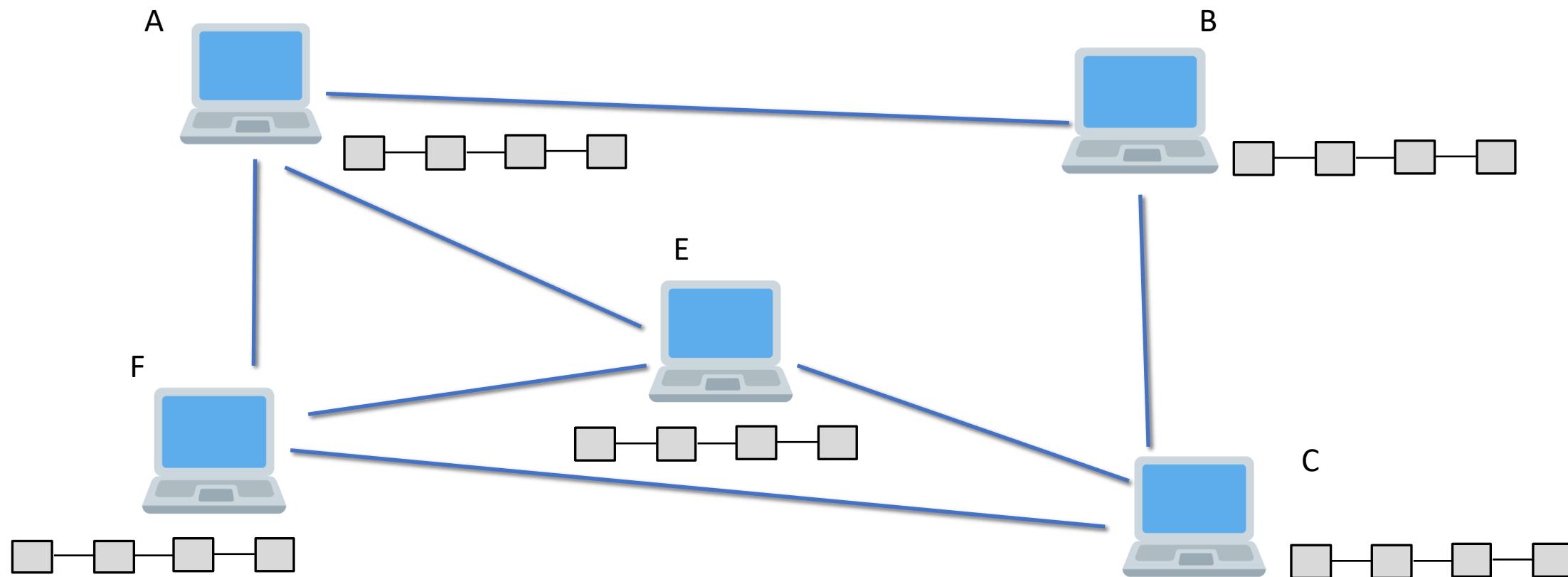




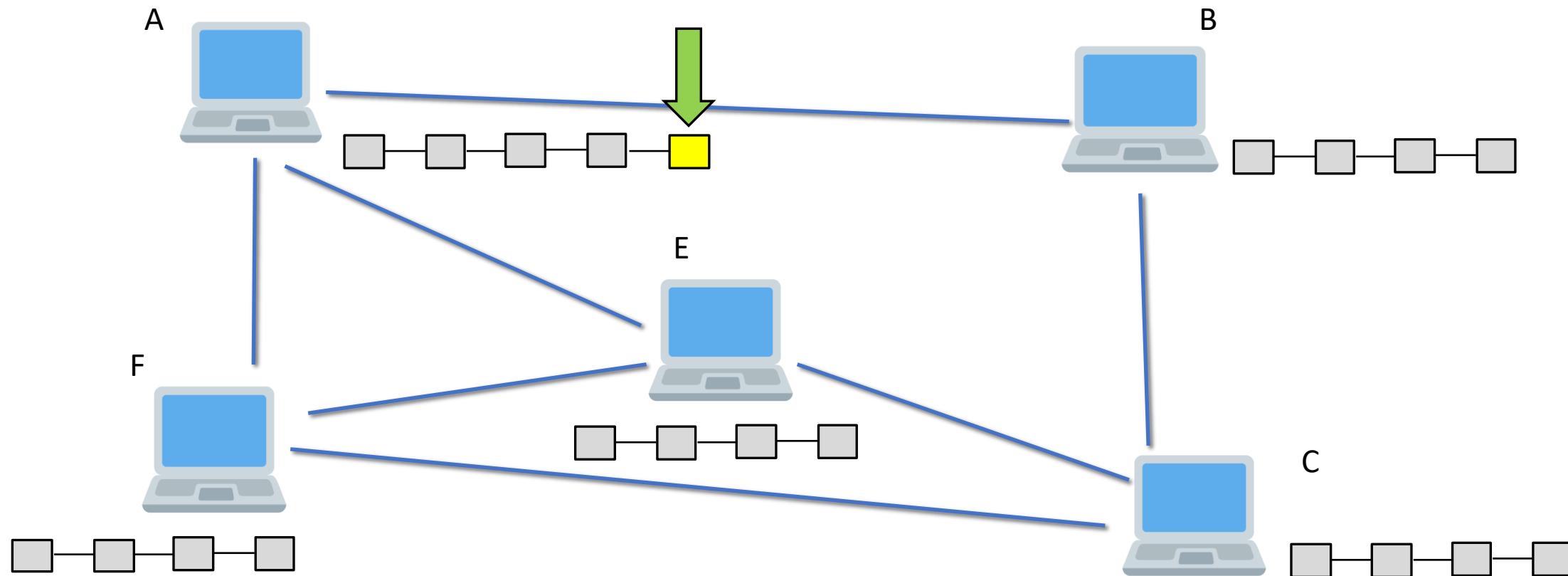
Sharding

Sharding

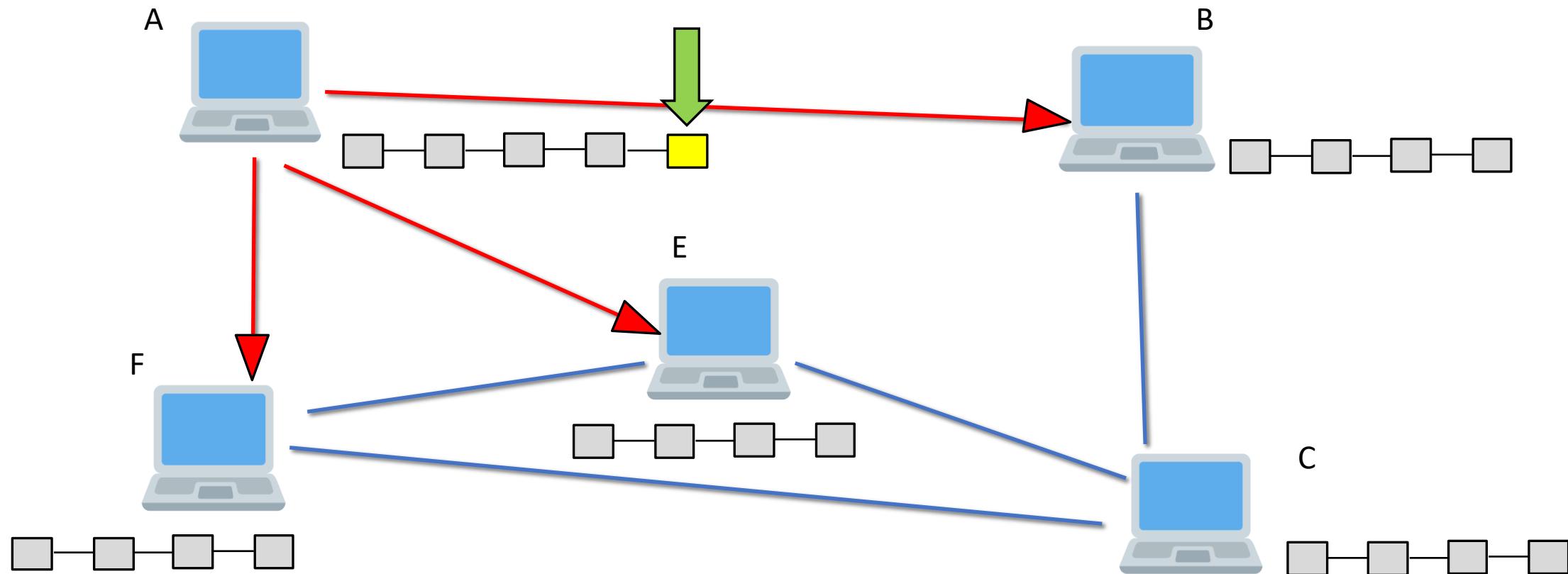
Consensus Protocol



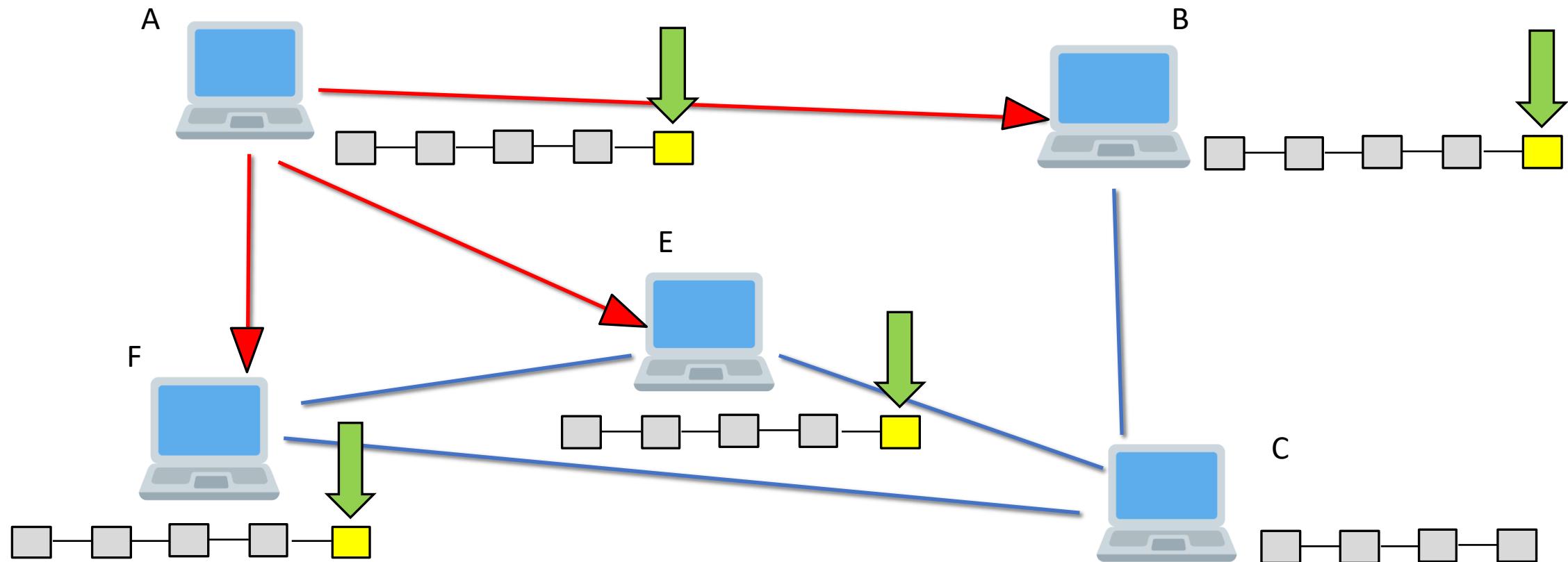
Consensus Protocol



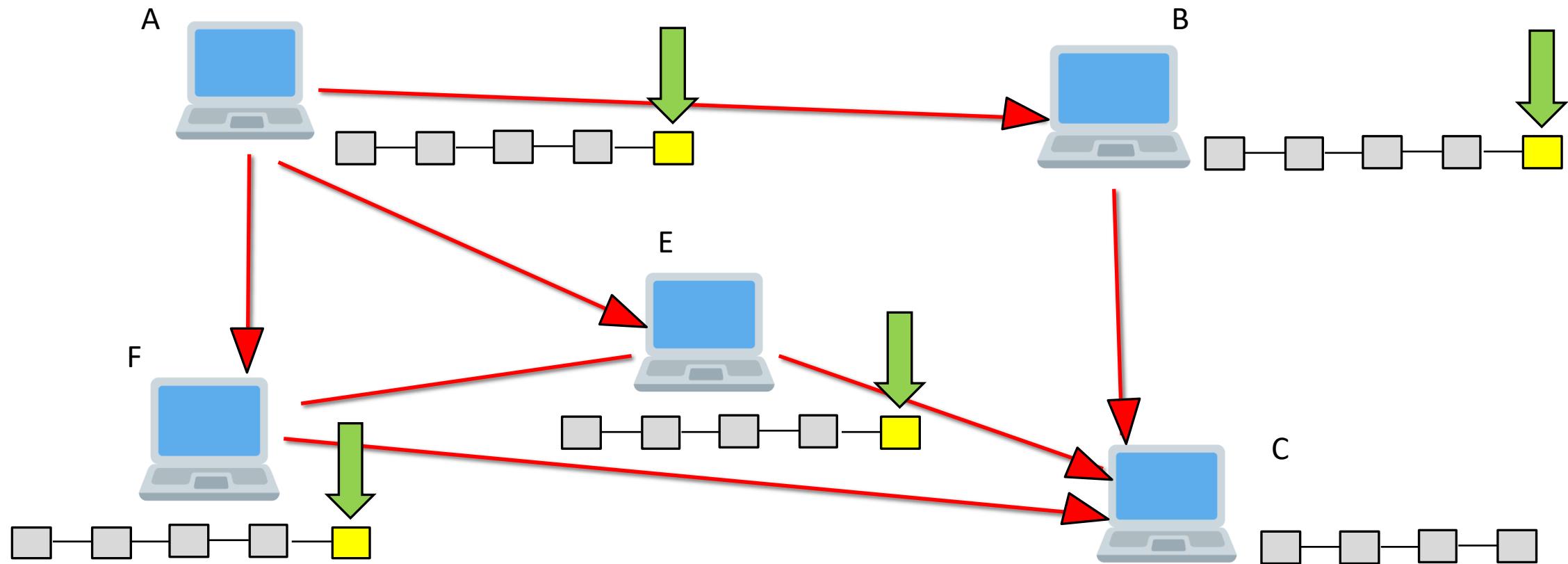
Consensus Protocol



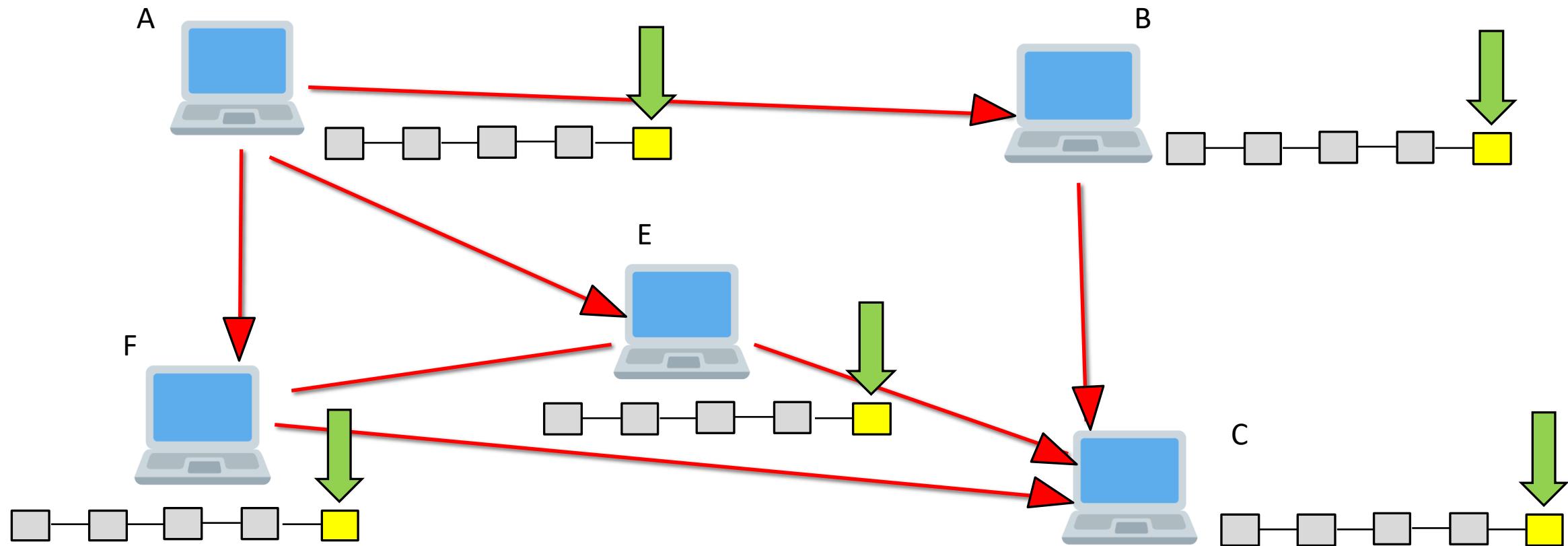
Consensus Protocol



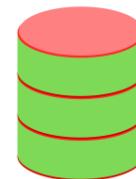
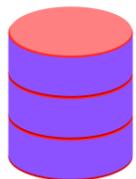
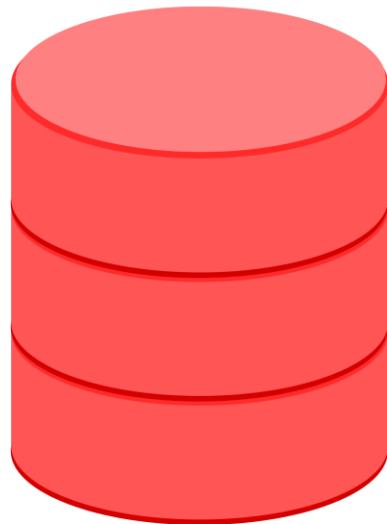
Consensus Protocol



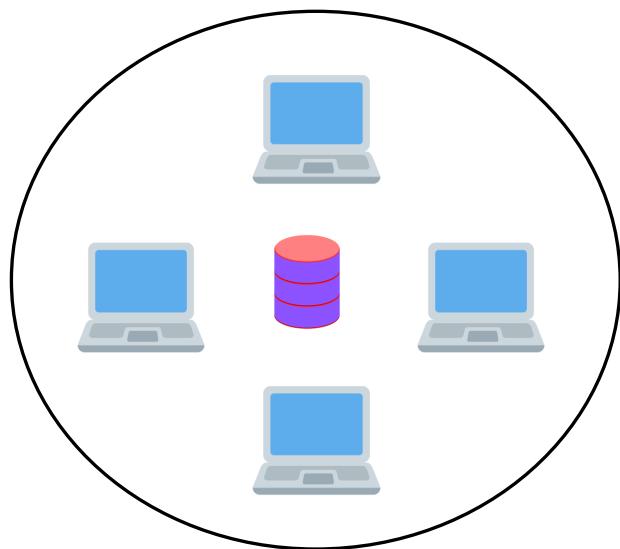
Consensus Protocol



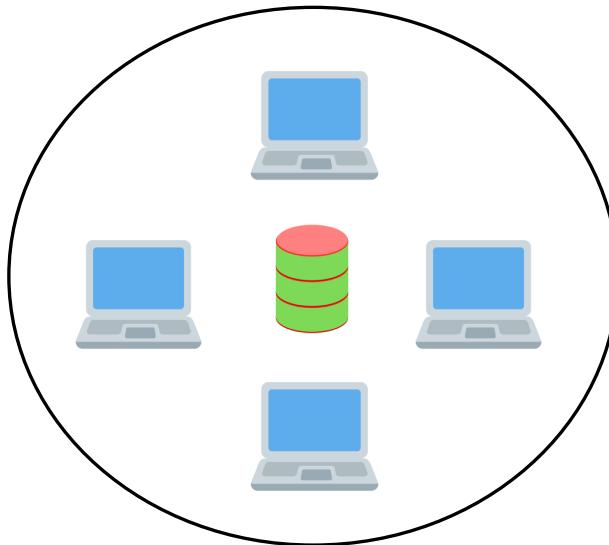
Sharding



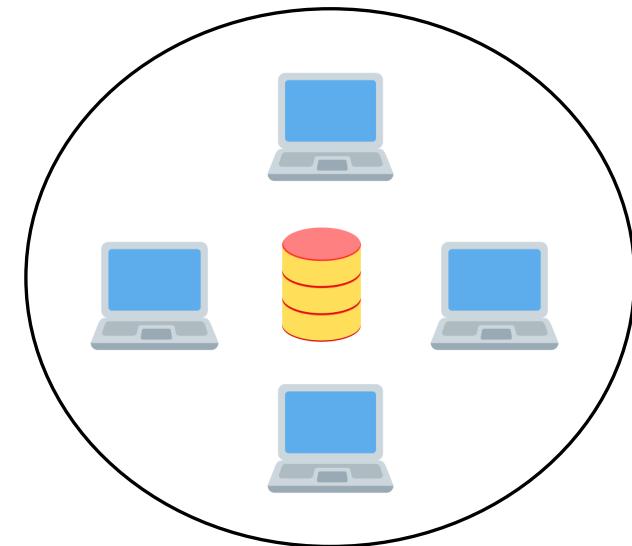
Sharding



Network A



Network B

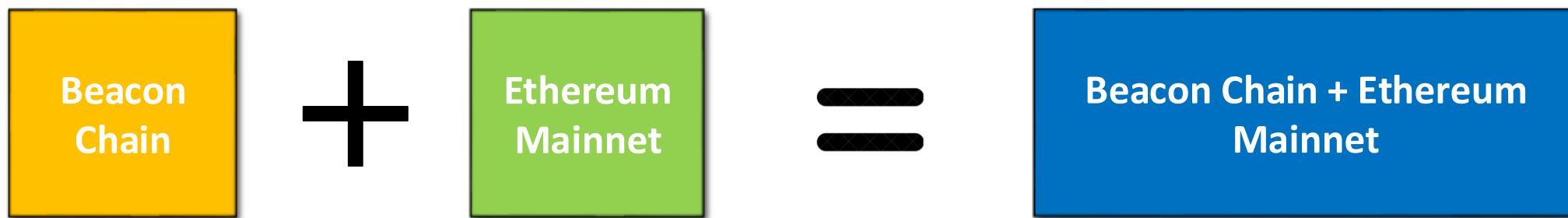


Network C

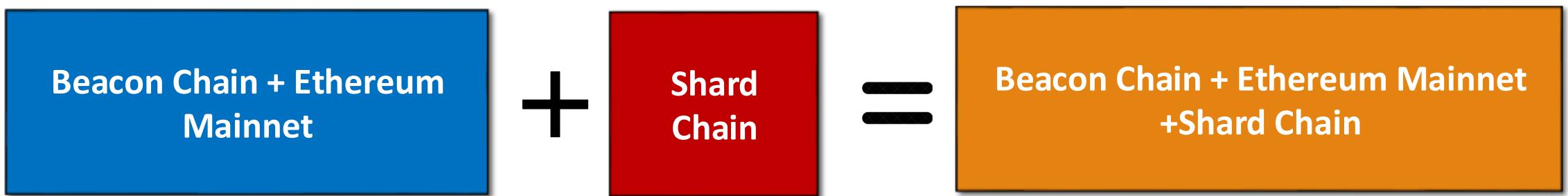
Major benefits

- Transactions per second increase.
- Powerful and expensive computers will not be needed.
- More validators will join.
- Energy consumption will reduce.

Sharding



Sharding



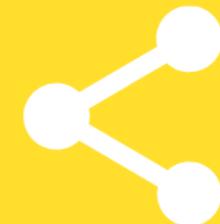
**GIVE THIS VIDEO
A THUMBS-UP !**

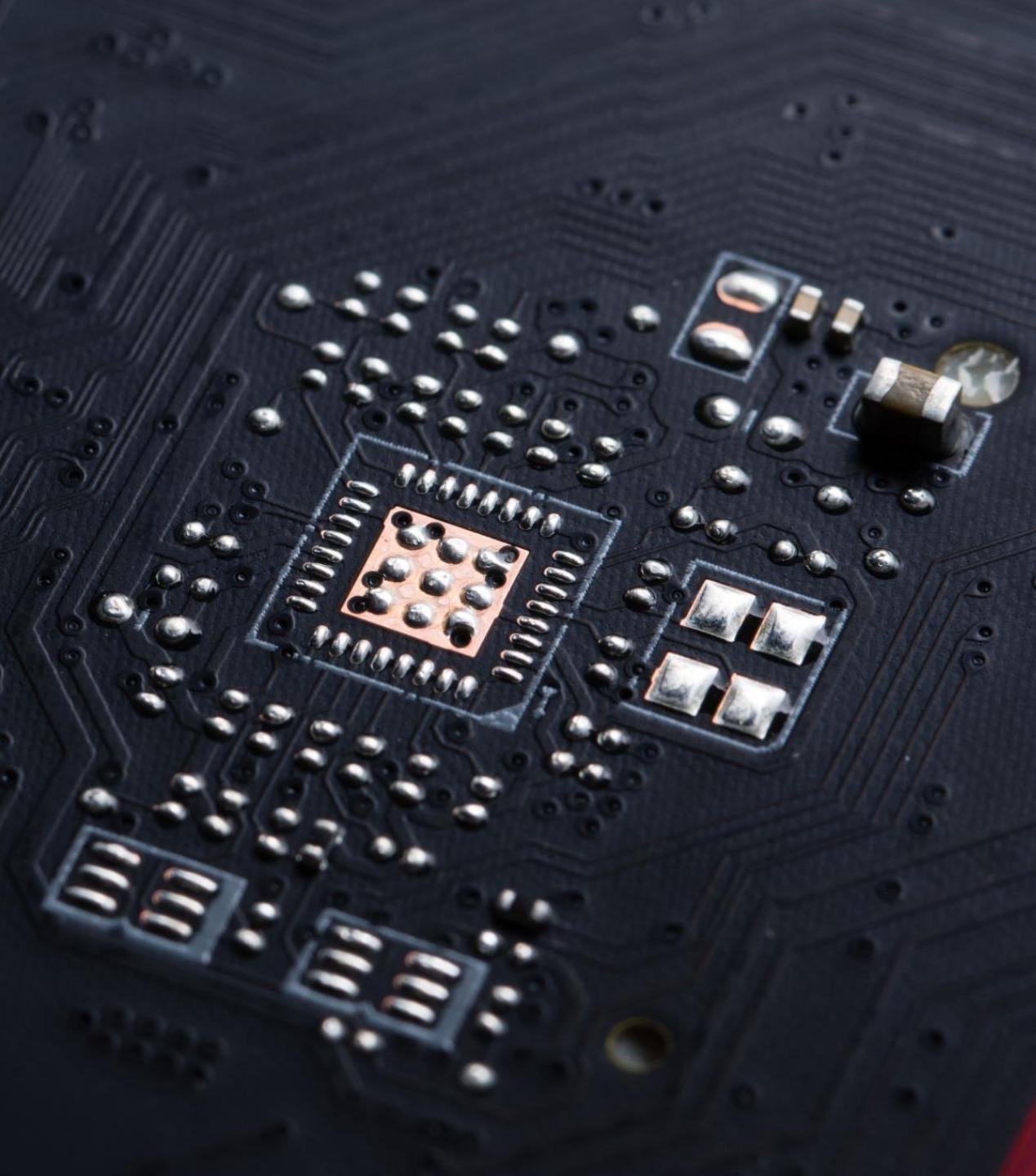
CODE EATER



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER

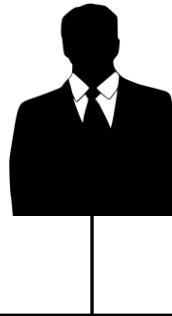




Decentralized Autonomous Organization (DAOs)

Decentralized Autonomous Organization (DAOs)

Director



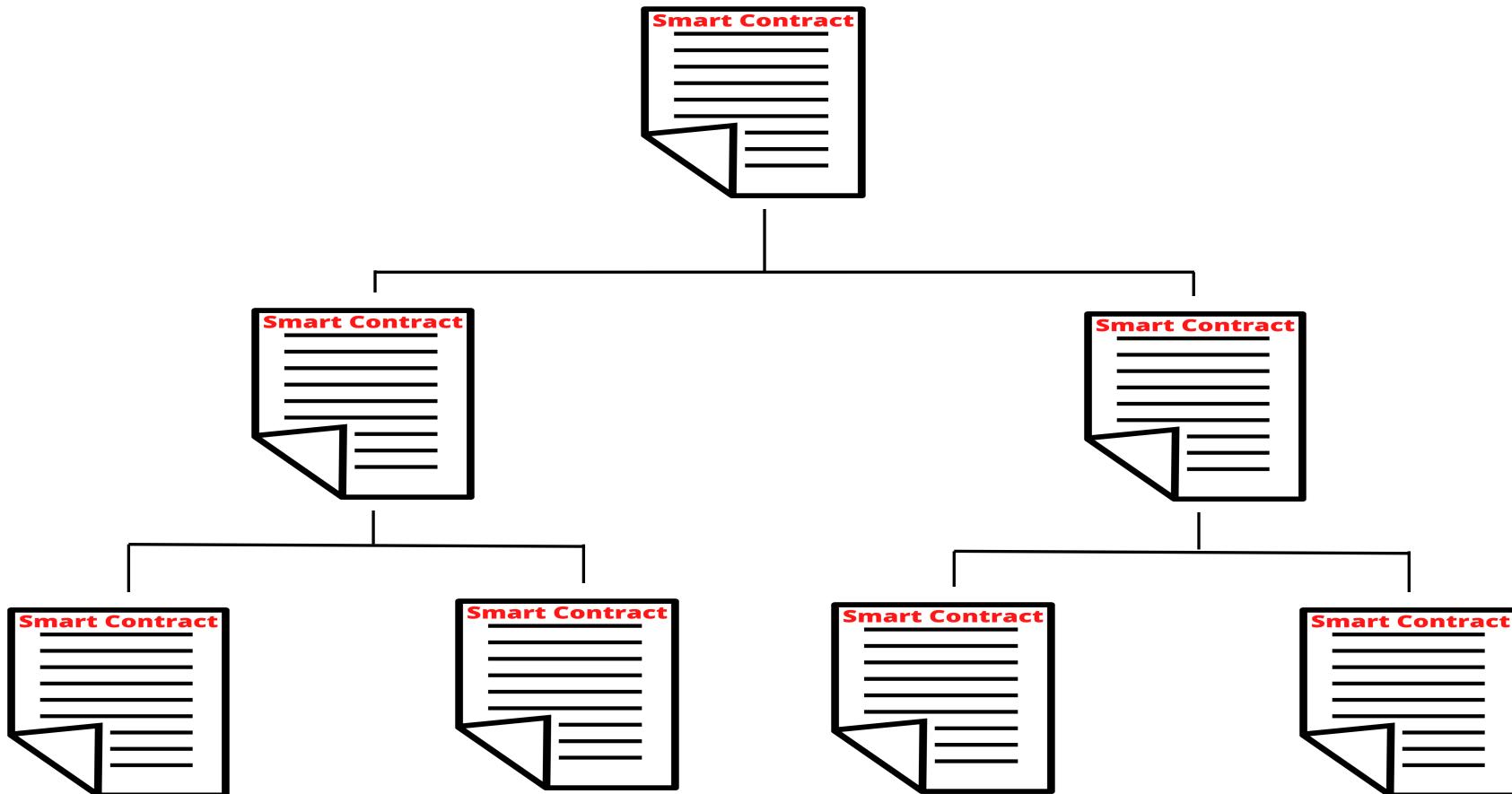
Manager



Employee



Decentralized Autonomous Organization (DAOs)



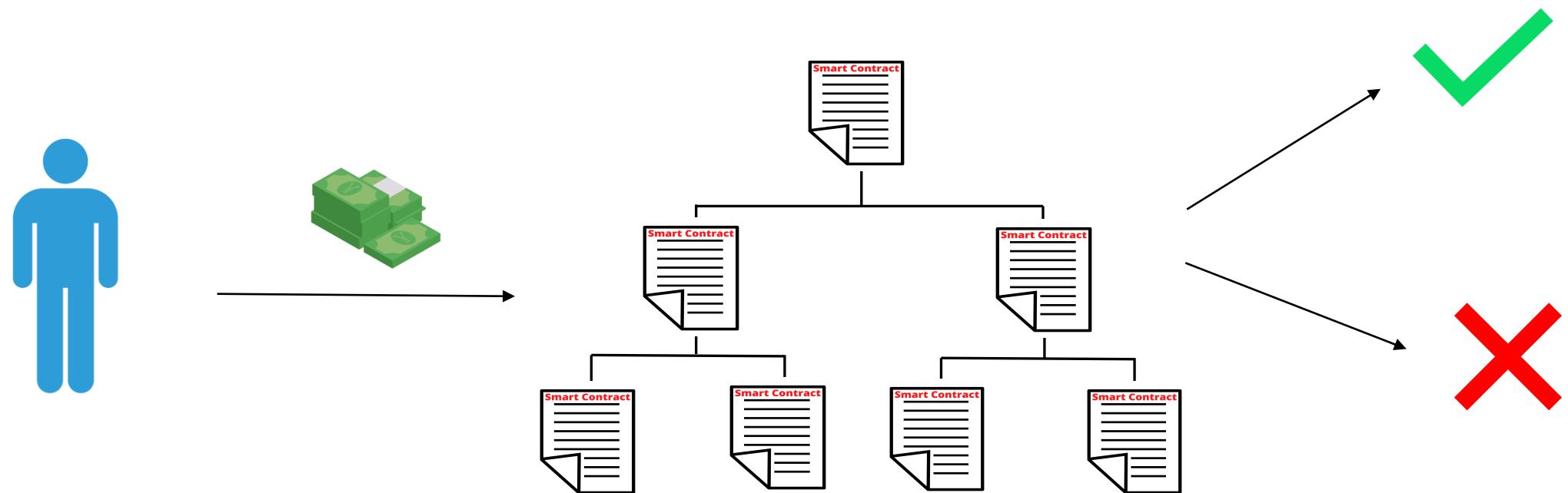
DAO vs Organization

DAO	A traditional organization
Fully democratized.	Usually hierarchical.
Voting required .	Voting may or may not require.
No trusted intermediary to count vote.	Outcome of voting must be handled manually.
Services offered are handled automatically.	Requires human handling, or centrally controlled automation.
All activity is transparent and fully public.	Activity is typically private, and limited to the public.

Decentralized Autonomous Organization (DAOs)



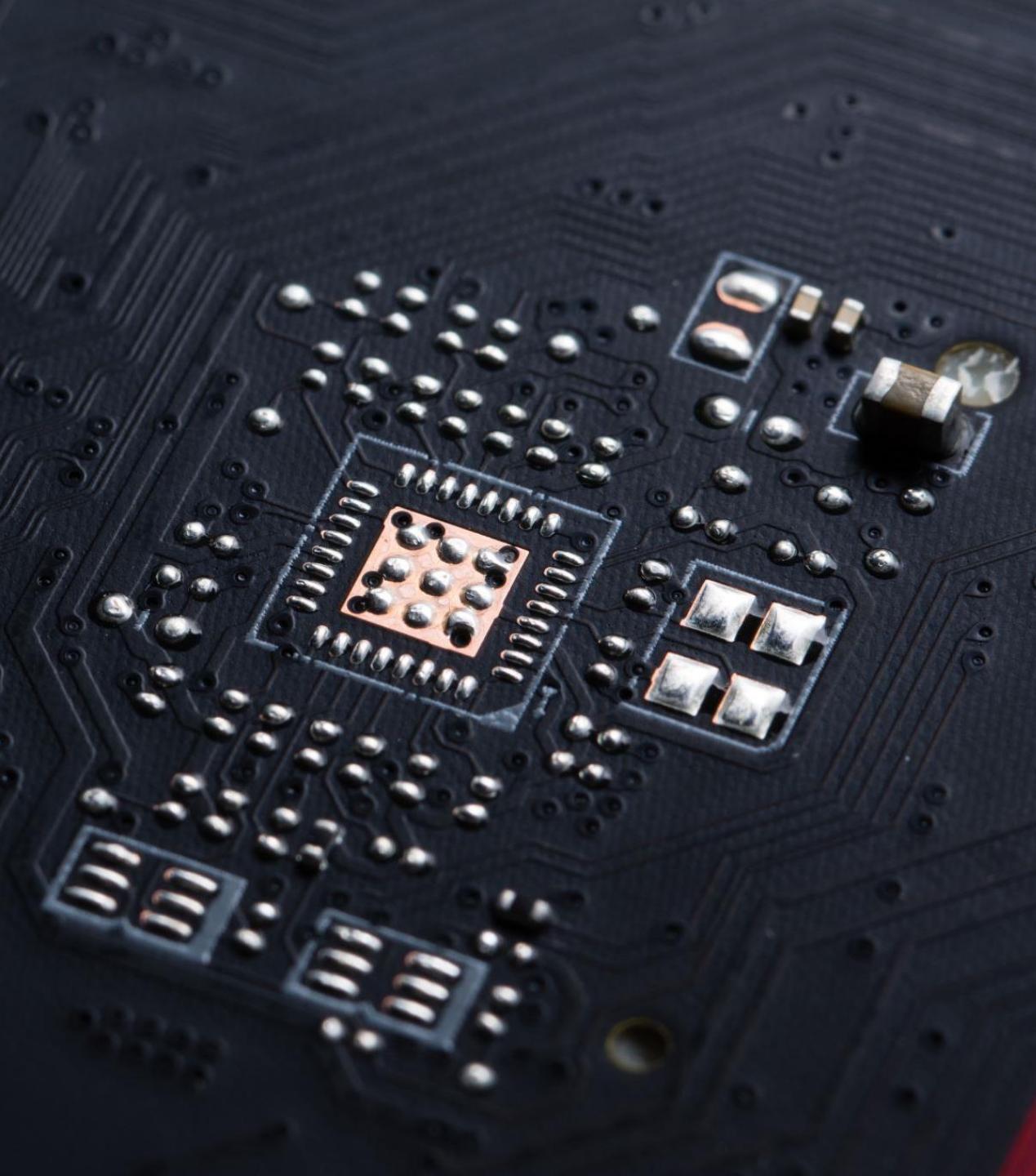
Decentralized Autonomous Organization (DAOs)



**GIVE THIS VIDEO
A THUMBS-UP !**

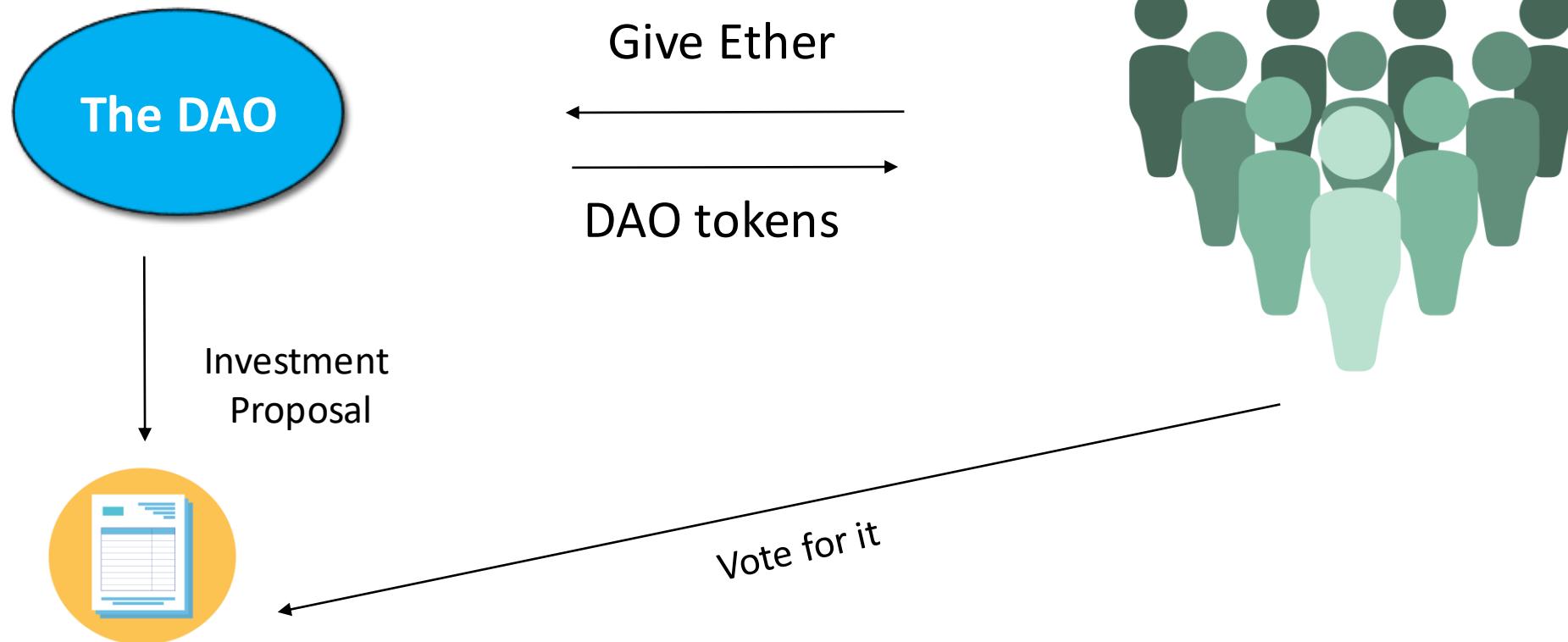
CODE EATER



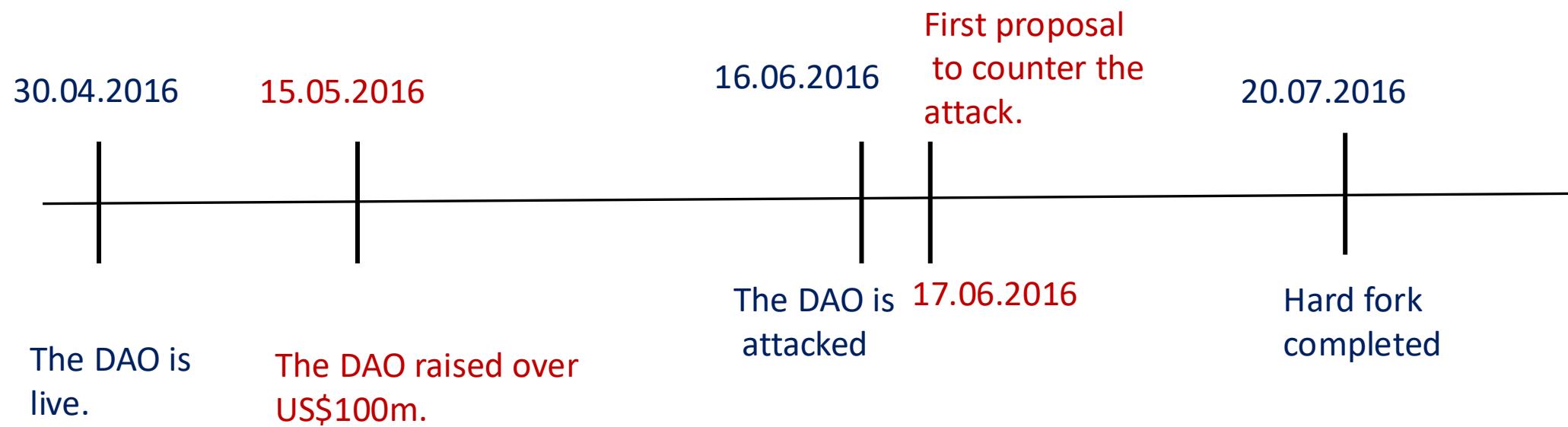


The DAO attack

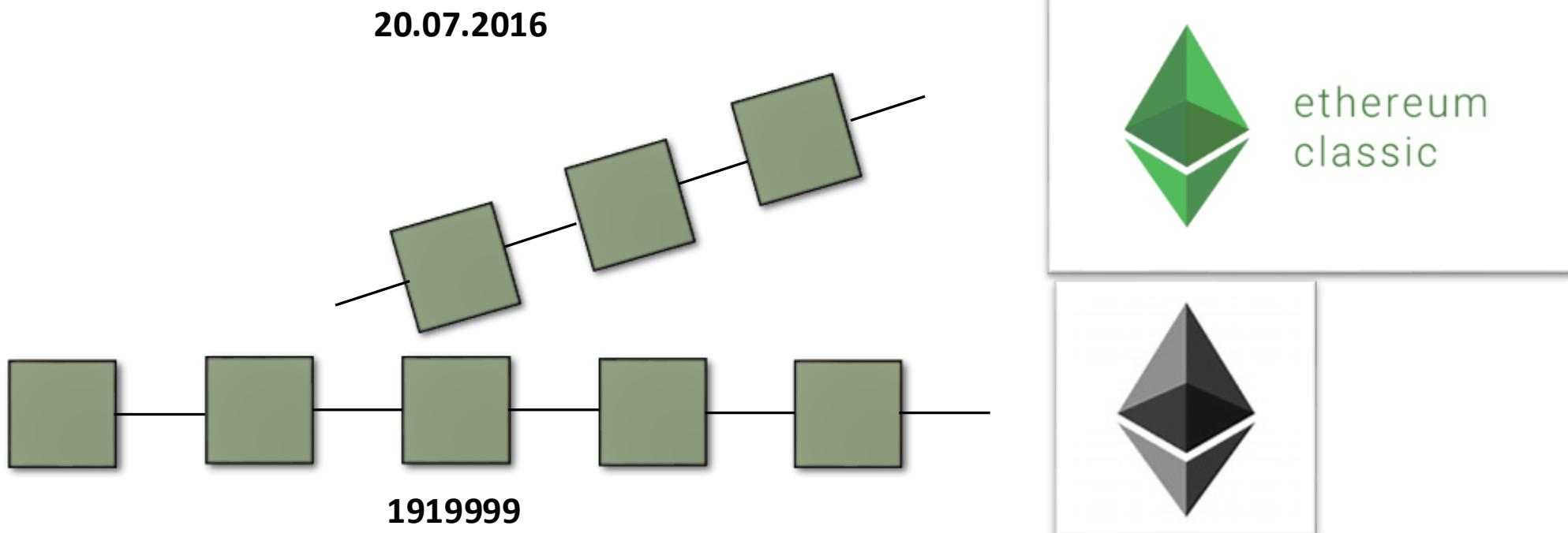
The DAO Attack



The DAO Attack



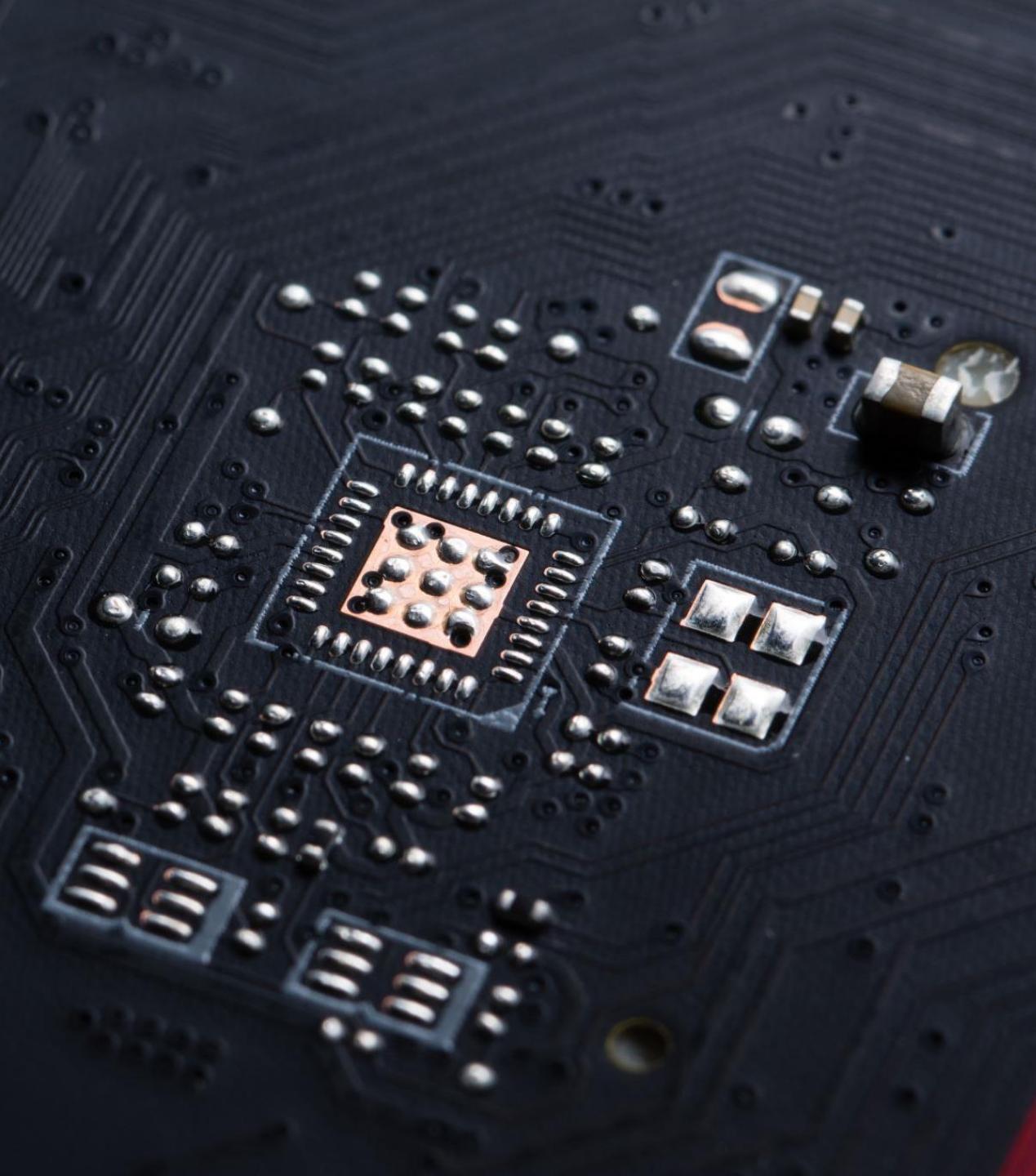
The DAO Attack



**GIVE THIS VIDEO
A THUMBS-UP !**

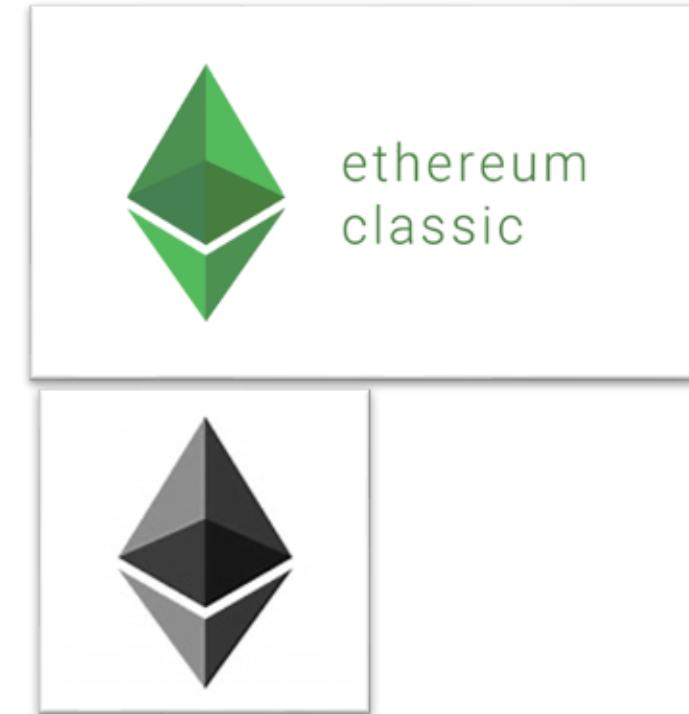
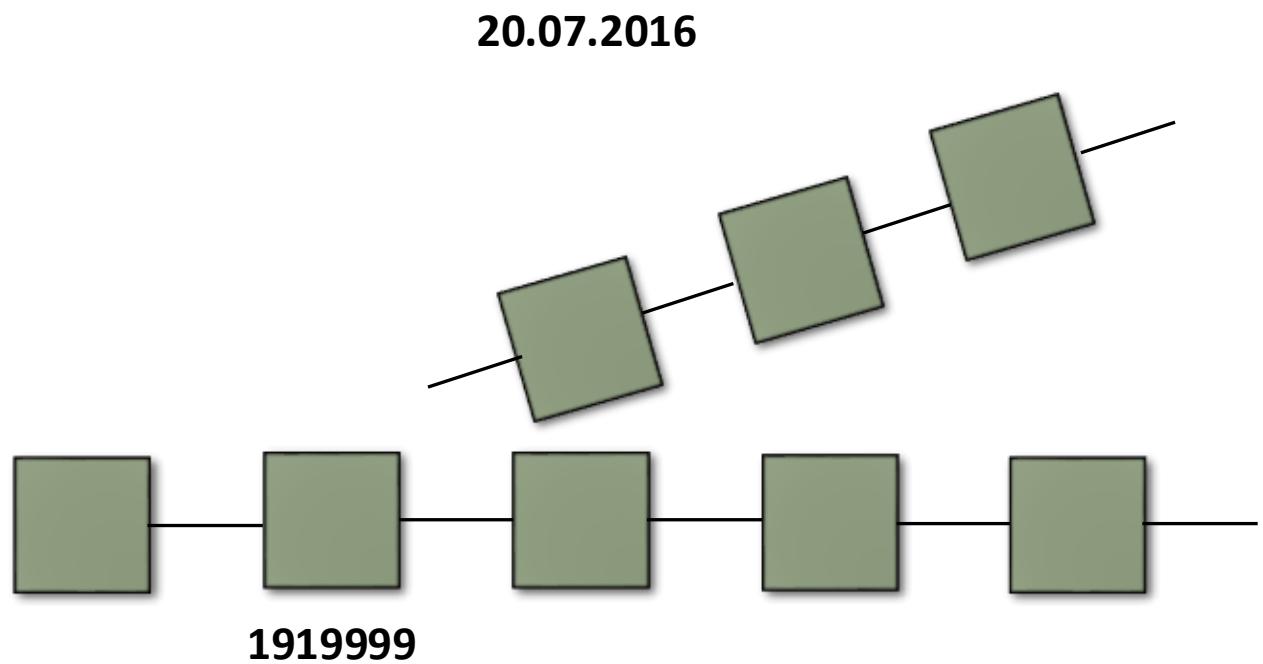
CODE EATER





Hard Fork

Hard Fork

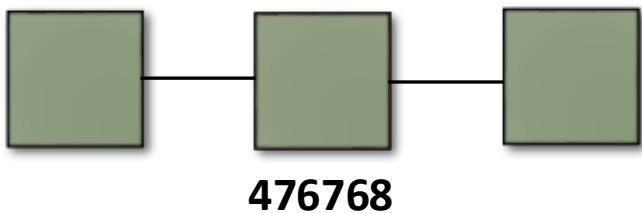


Hard Fork

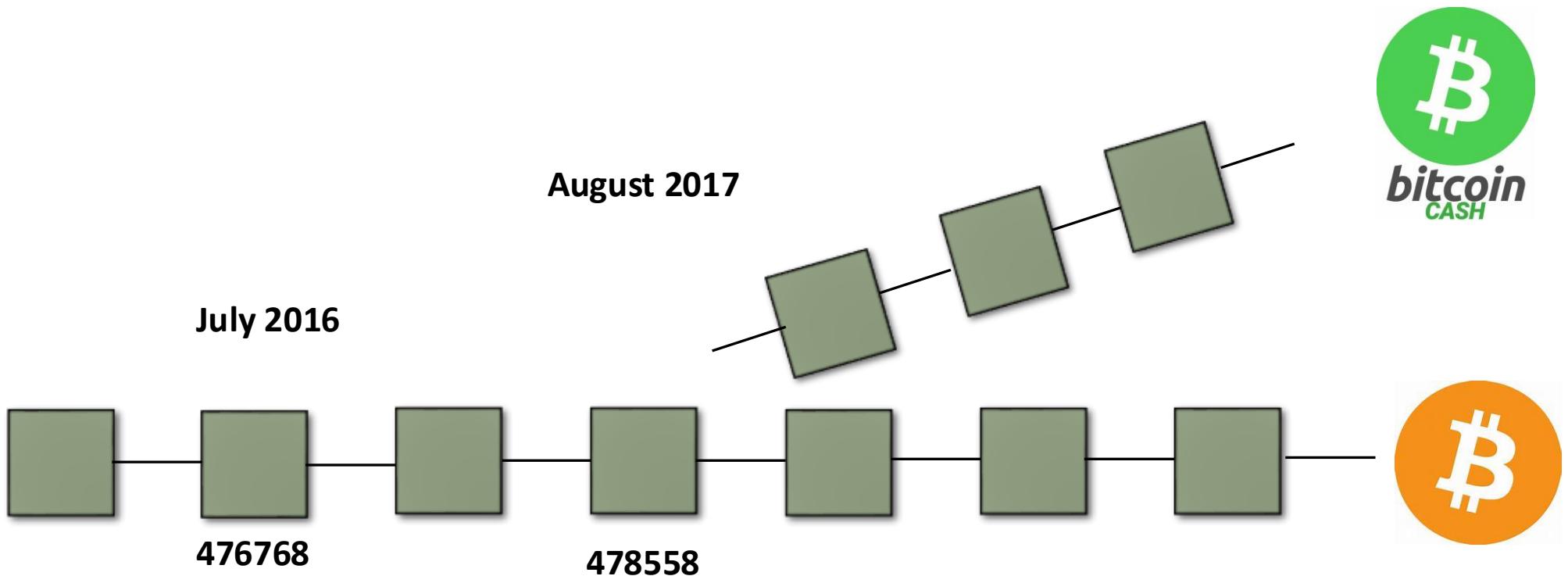
- During a hard fork, software implementing a protocol and its mining procedures is upgraded.
- Once a user upgrades their software, that version rejects all transactions from older software, effectively creating a new branch of the blockchain.
- However, those users who retain the old software continue to process transactions.

Hard Fork

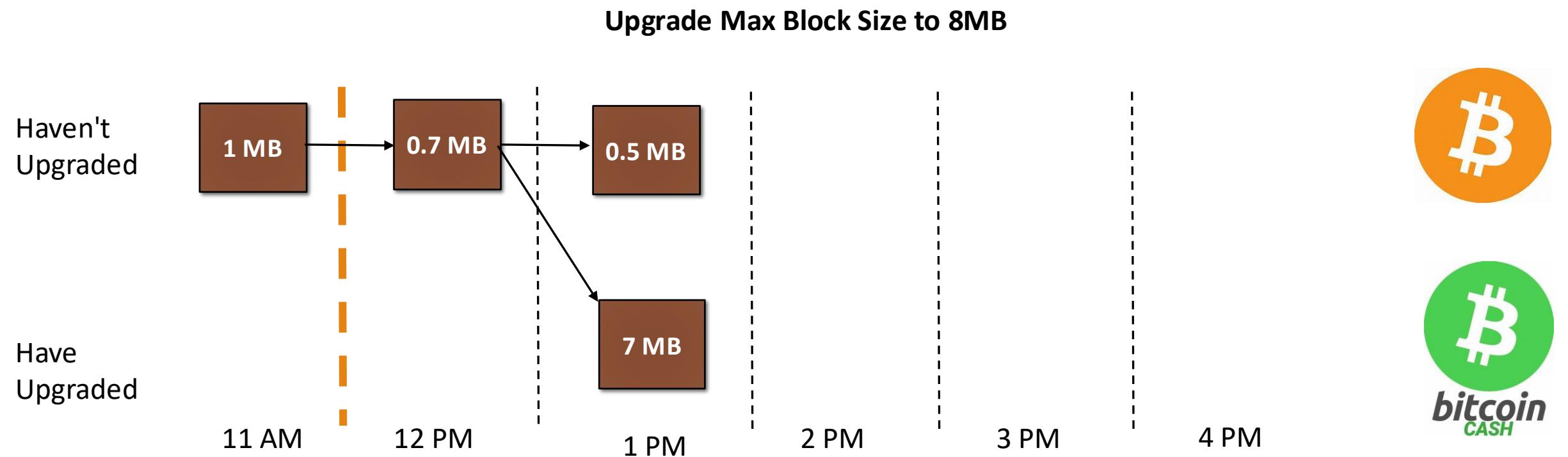
July 2016



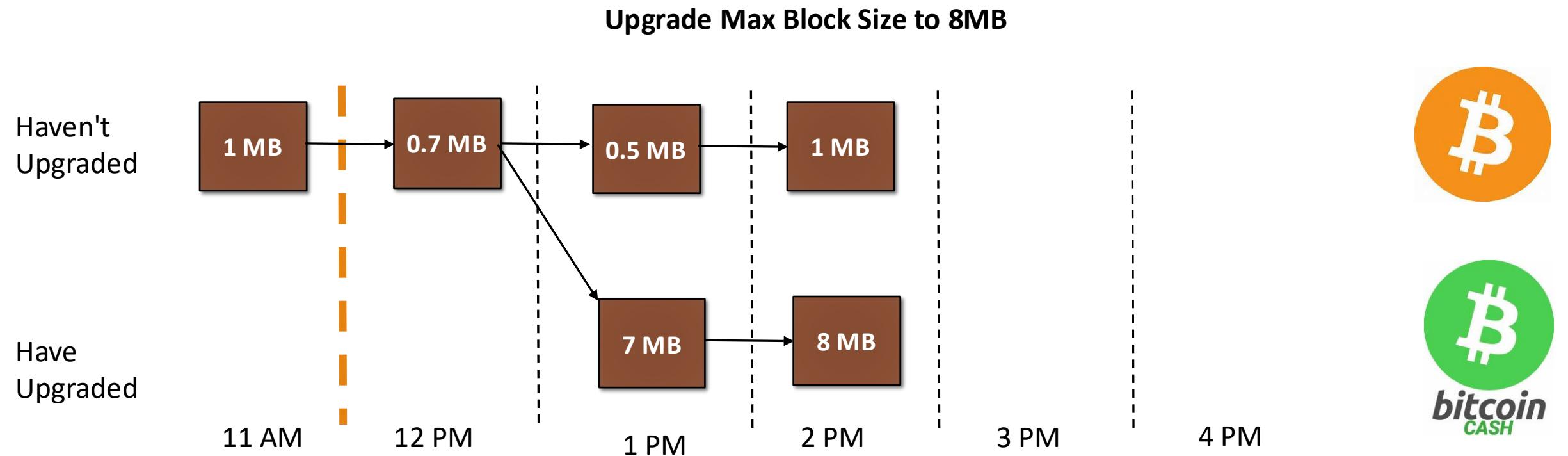
Hard Fork



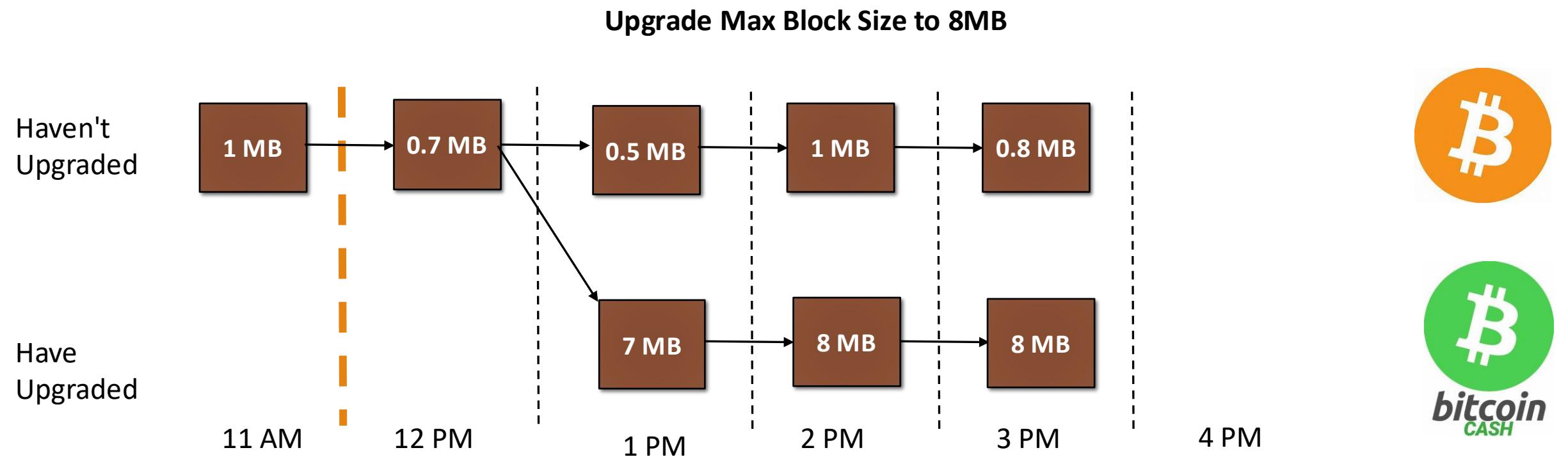
Hard Fork



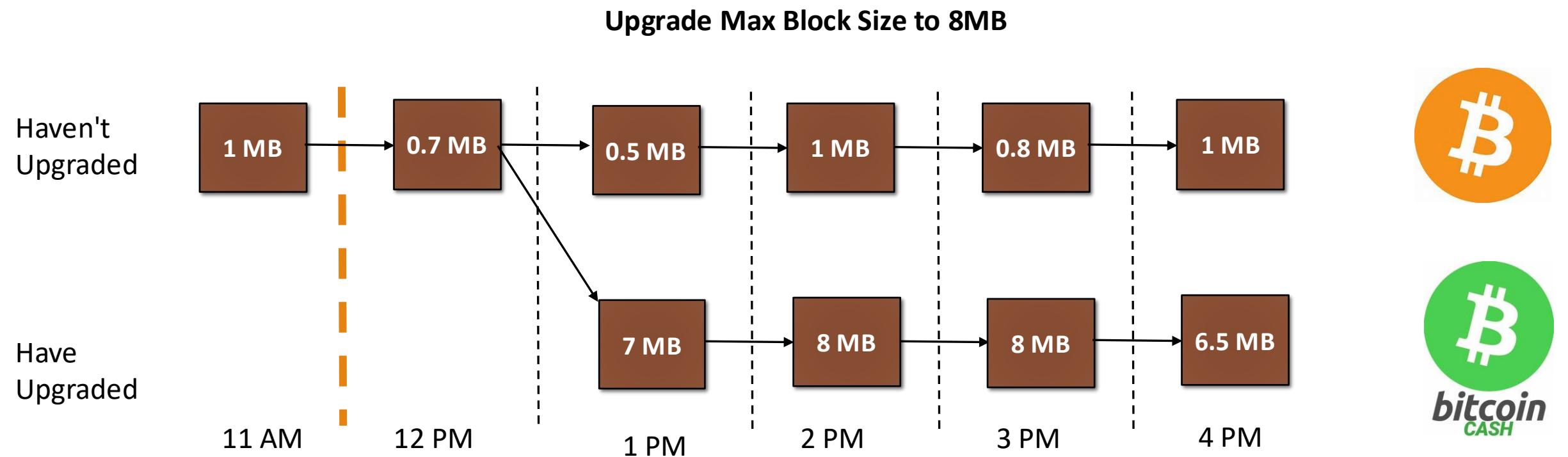
Hard Fork



Hard Fork

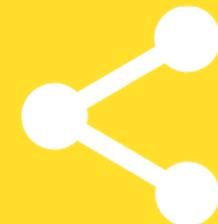


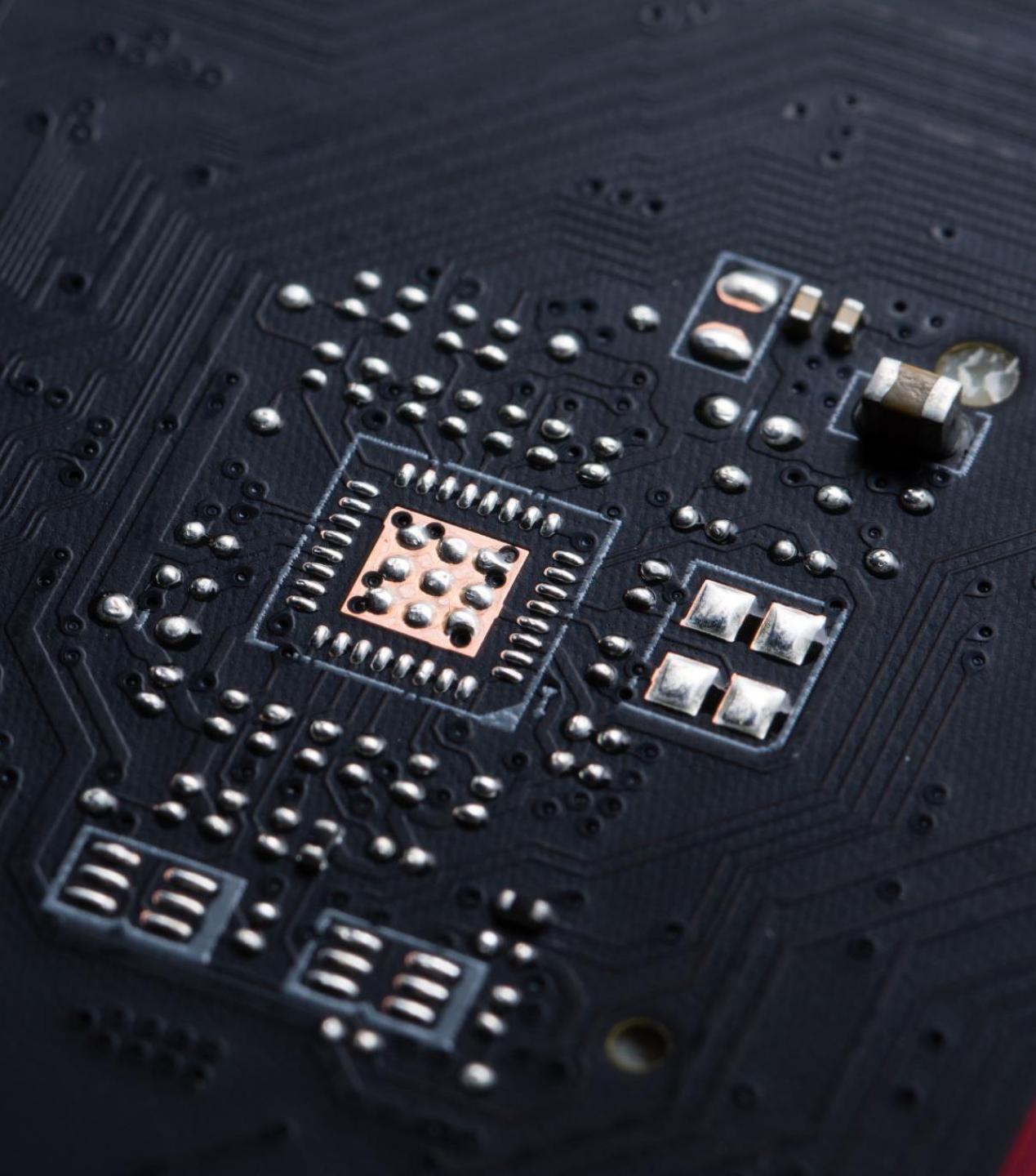
Hard Fork



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



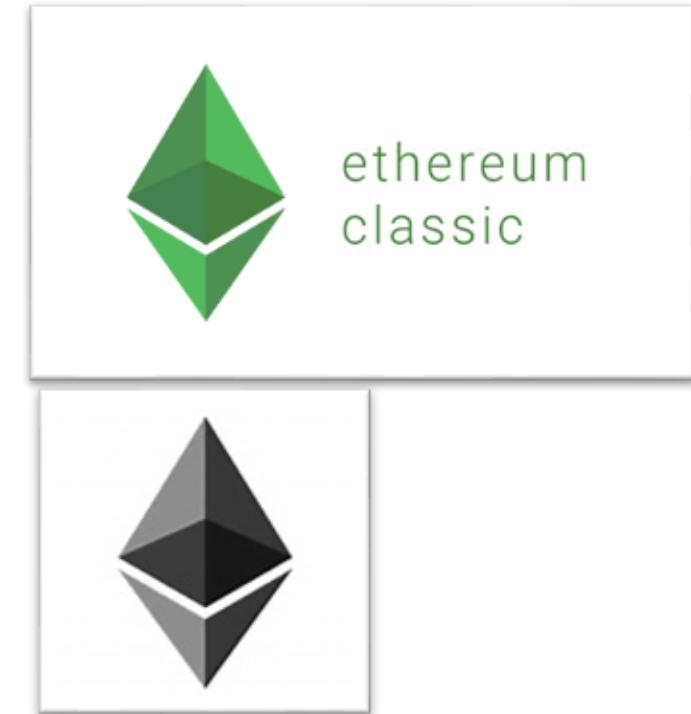
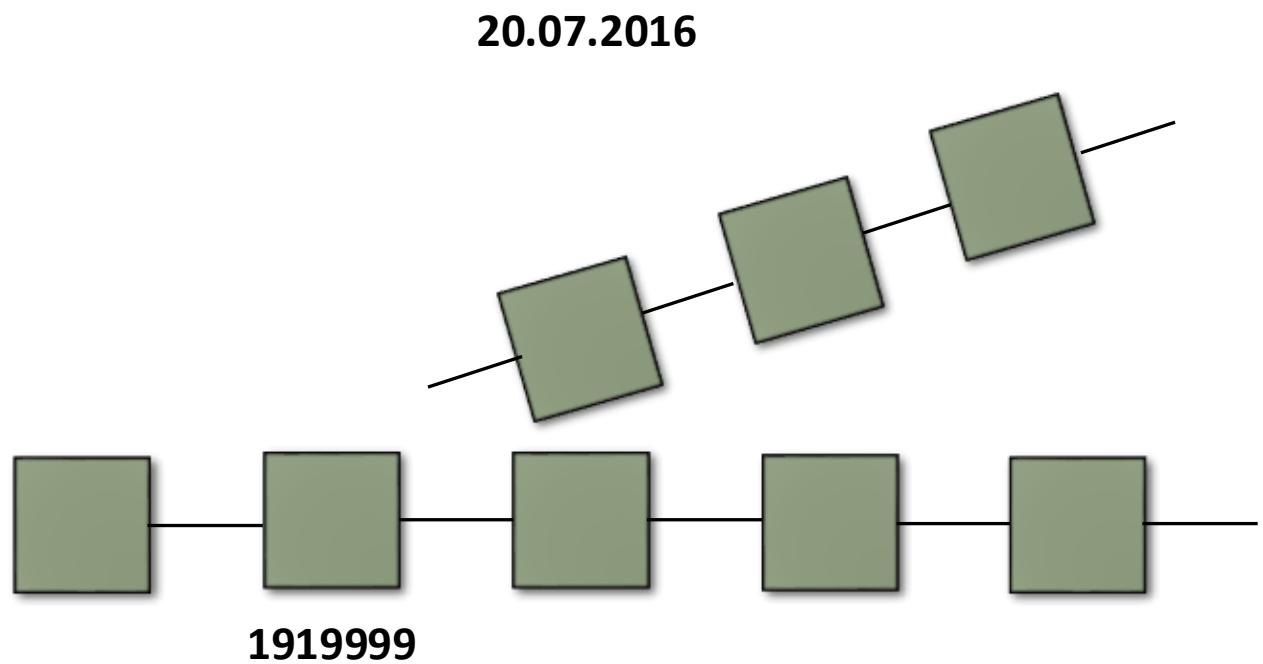


Soft Fork

Soft Fork

- Soft forks are a change to the protocol, **but the end product remains unchanged.**

Hard Fork



Soft Fork

- Soft forks are a change to the protocol, **but the end product remains unchanged.**
- A soft fork is a *backward-compatible* upgrade, meaning that the upgraded nodes can still communicate with the non-upgraded ones.
- Old nodes(not upgraded nodes) could still validate blocks and transactions (the formatting didn't break the rules), but they just wouldn't understand them.

Soft Fork



Soft Fork



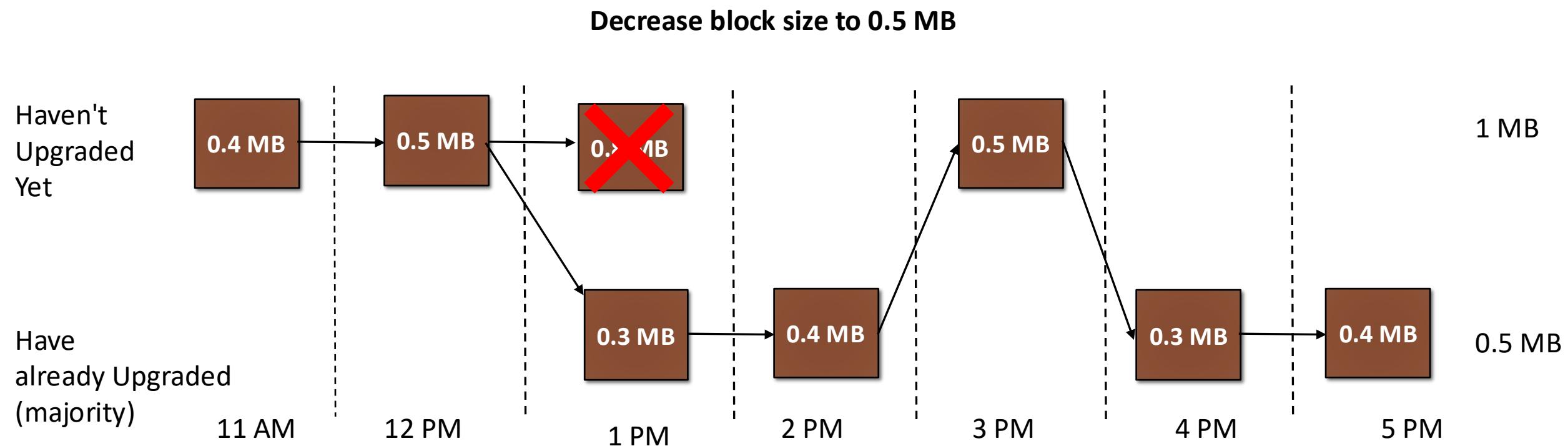
Soft Fork



Soft Fork

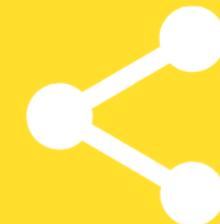


Soft Fork

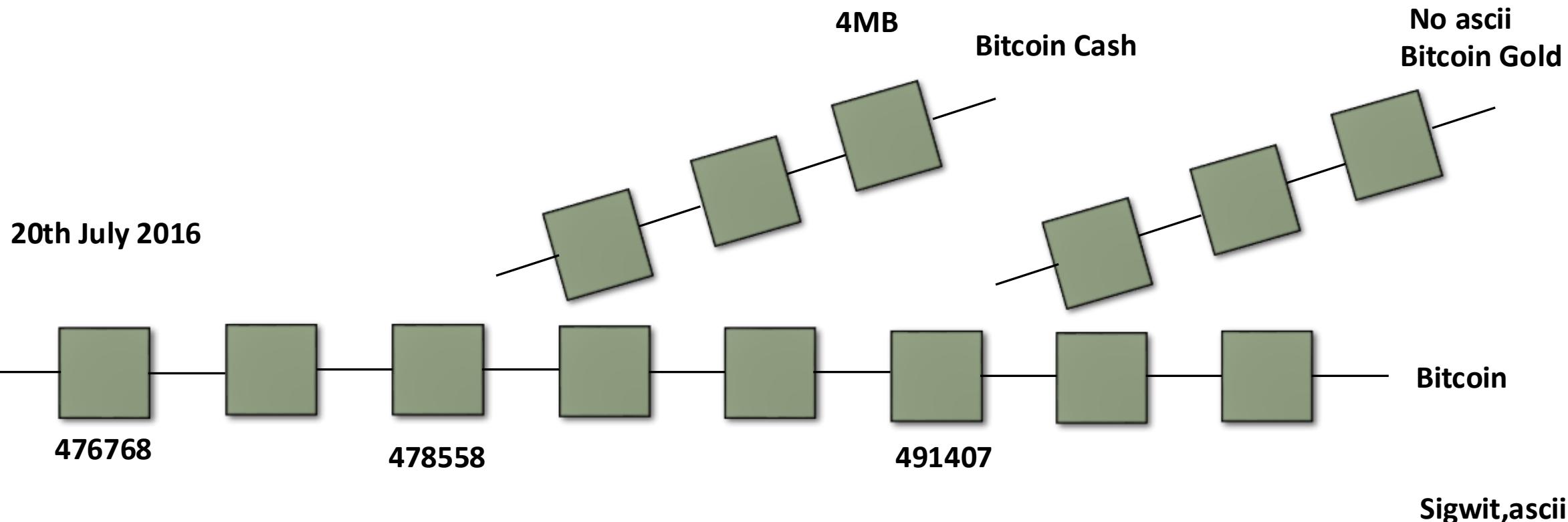


**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER



The DAO Attack





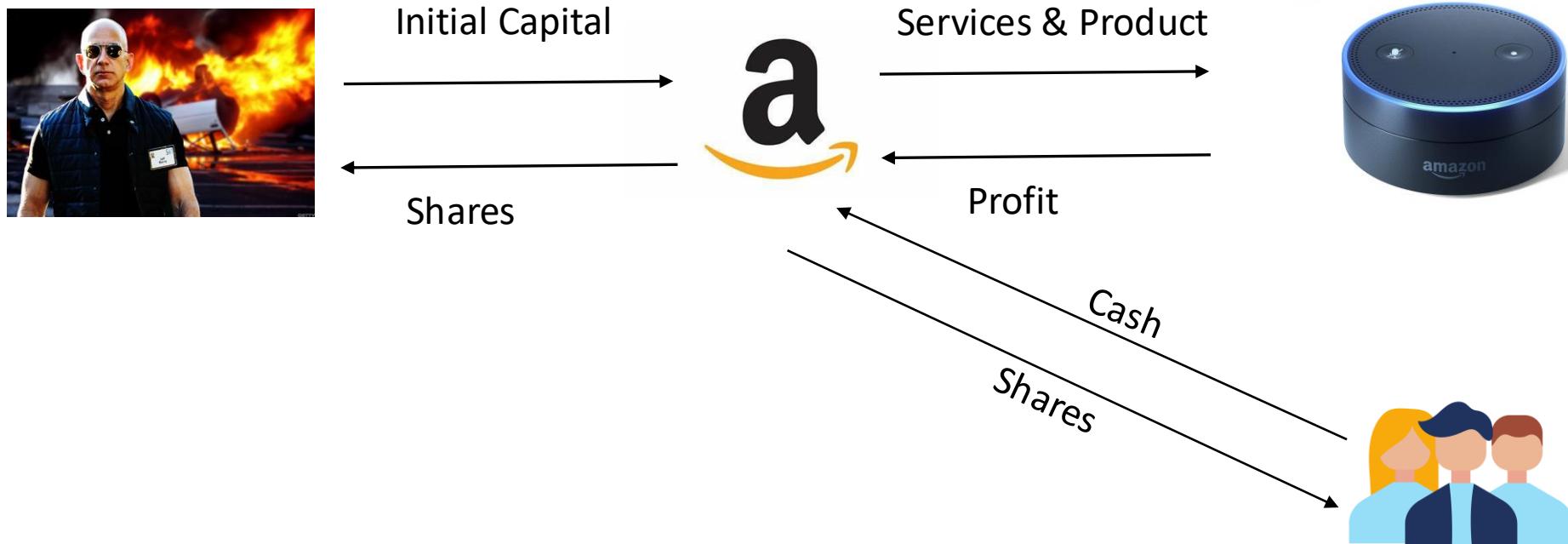
ICO's

Token

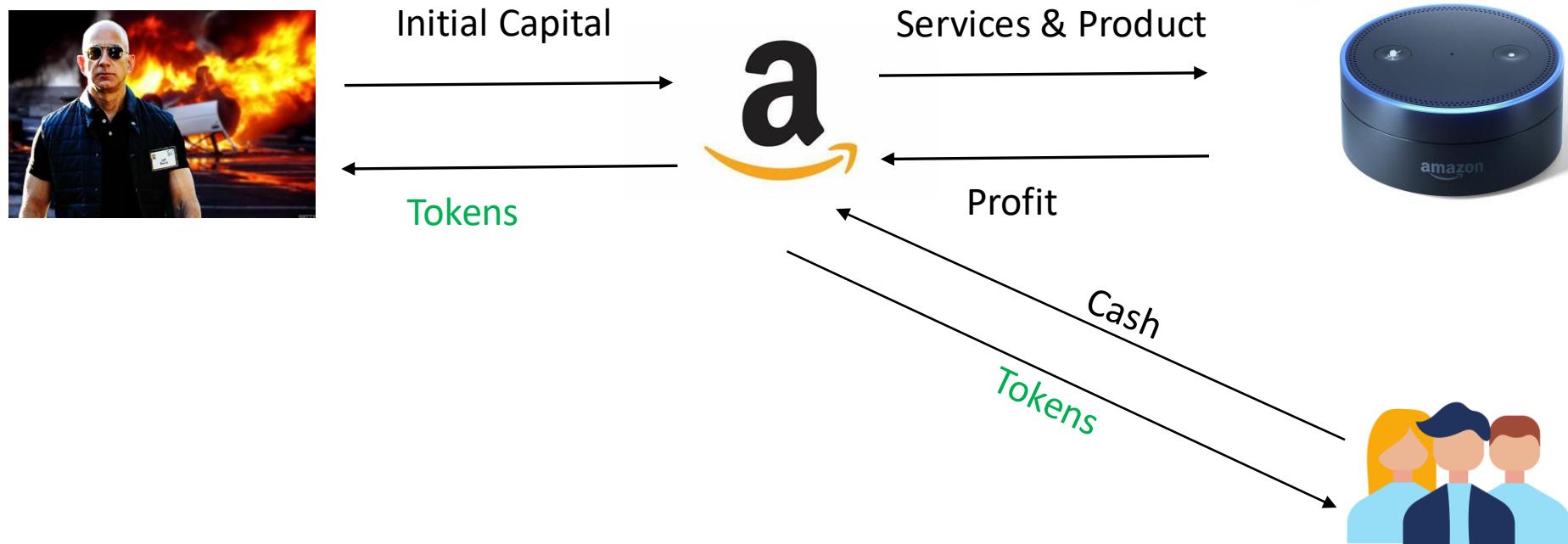
- **Tokens** are a type of **cryptocurrency** that represents an asset or specific use and resides on their **blockchain**



Initial Coin Offering (ICO)



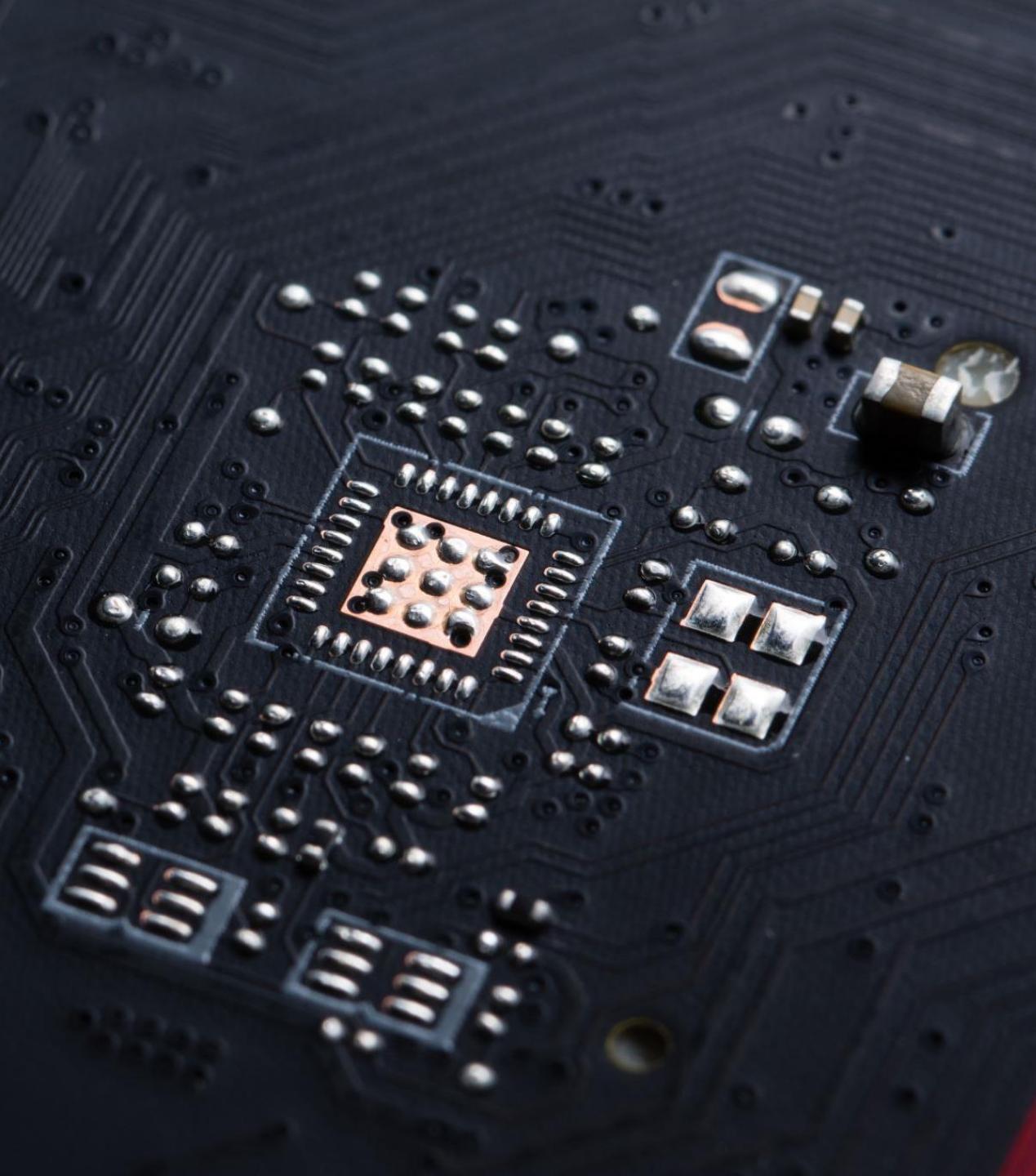
Initial Coin Offering (ICO)



**GIVE THIS VIDEO
A THUMBS-UP !**

CODE EATER





Alt Coins

Alt Coins

- Altcoins are generally defined as **all cryptocurrencies other than Bitcoin (BTC)**.

Alt Coins



LTC
Litecoin



THETA
THETA



USDT
Tether



ADA
Cardano



BNB
Binance Coin



LINK
Chainlink

What is the need of Alt Coins ?

Application and Uses

Protocol

Technology

CONGRATULATION



Mode of Contact



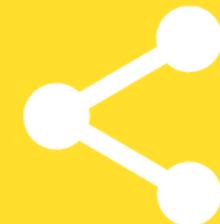
Instagram - @codeeater21



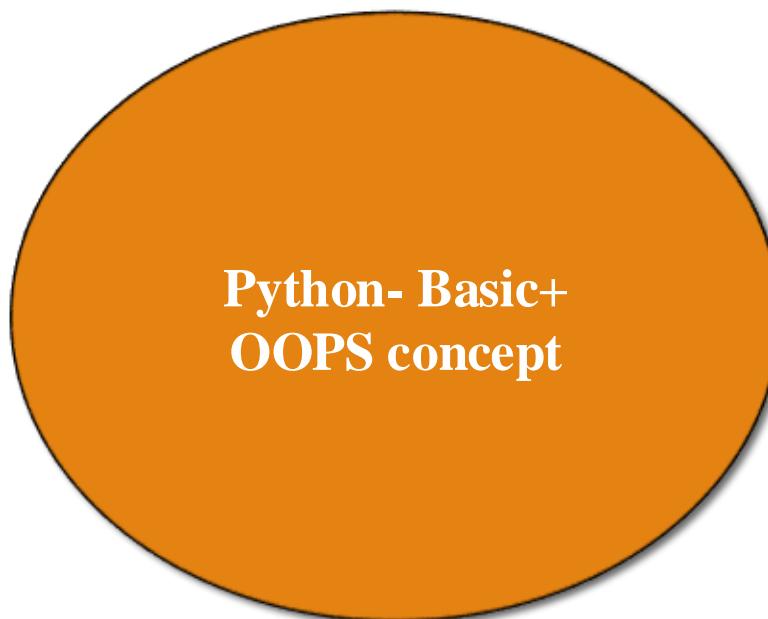
www.facebook.com/groups/codeeater21/

**GIVE THIS VIDEO
A THUMBS-UP !**

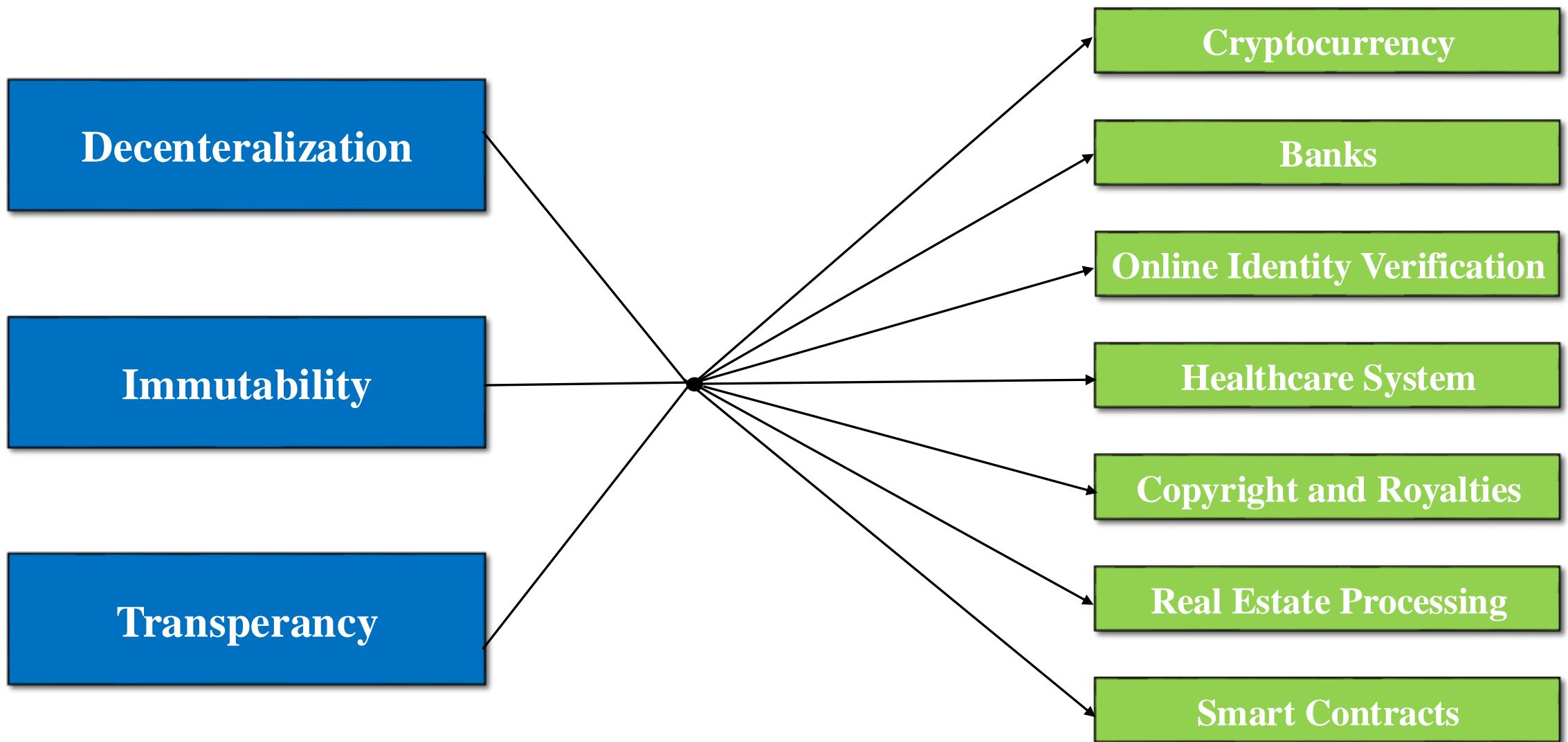
CODE EATER



Prerequisite for Implementation of Blockchain(Coding Part)



Python- Basic+
OOPS concept



Properties of Blockchain

Decentralization

Immutability

Transperancy