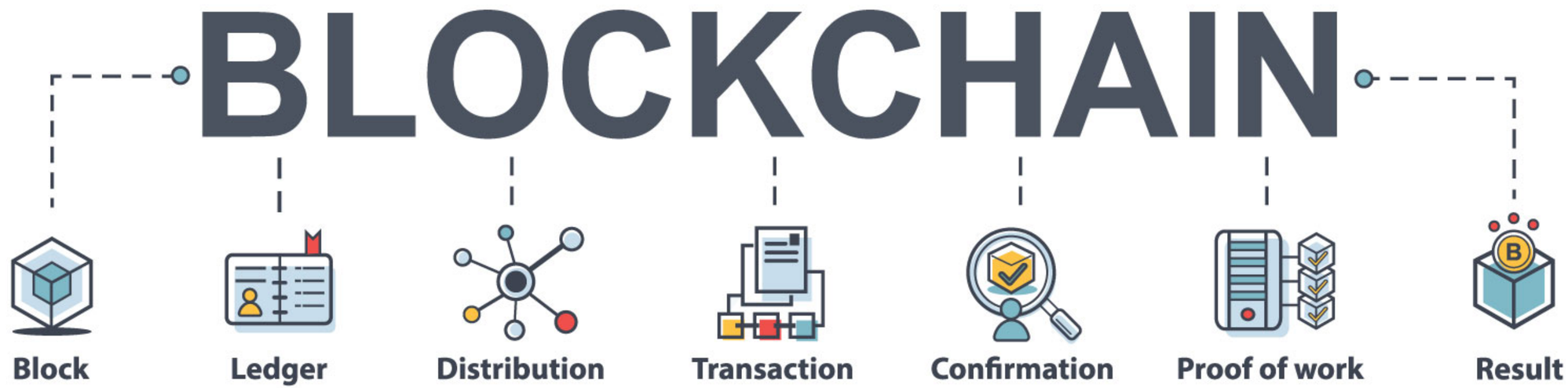
Blockchain

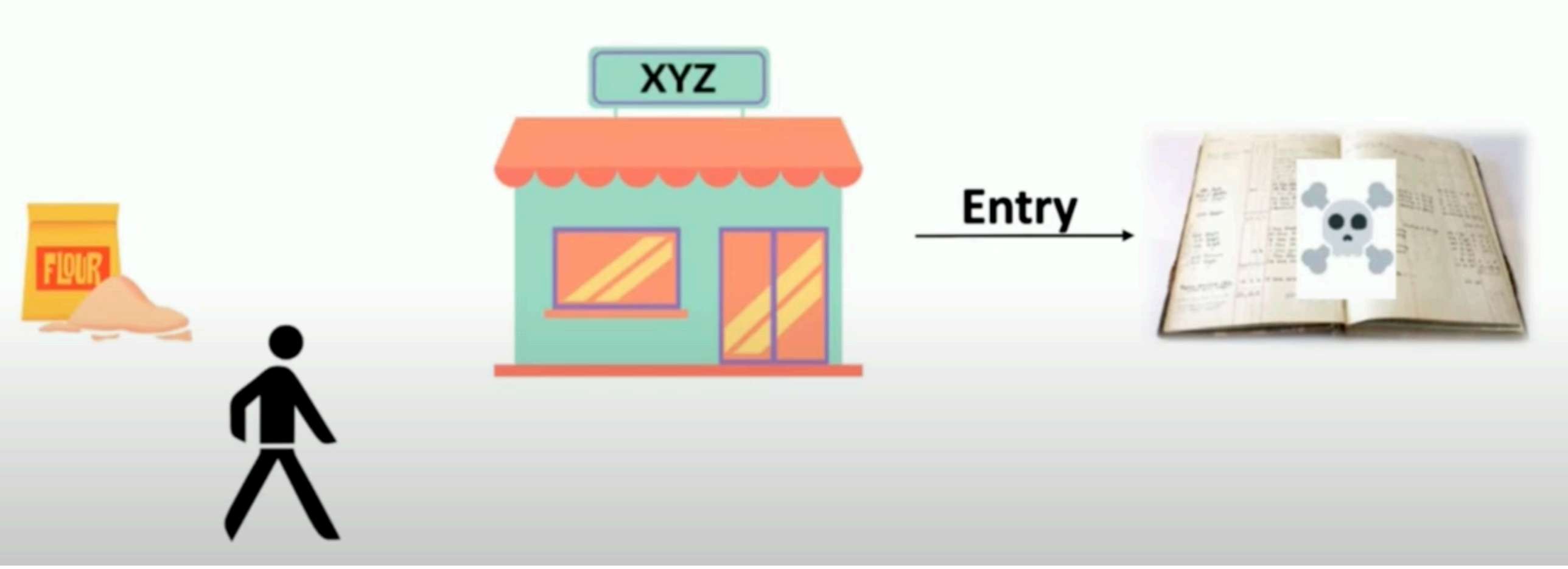
Why Blockchain?

- **Disruptive** technology - change traditional methods. Ex- horse carts replaced by cars and buses since less effort and more speed. Email replaced traditional mails
- Just like Internet changed the way communication happened, Blockchain changed **trust ecosystem.**
- What is **trust**? Can we trust a brand that sells expensive coffee and claims to import coffee from some foreign country? Can we trust an NGO whether the donated money is actually used for the needy?

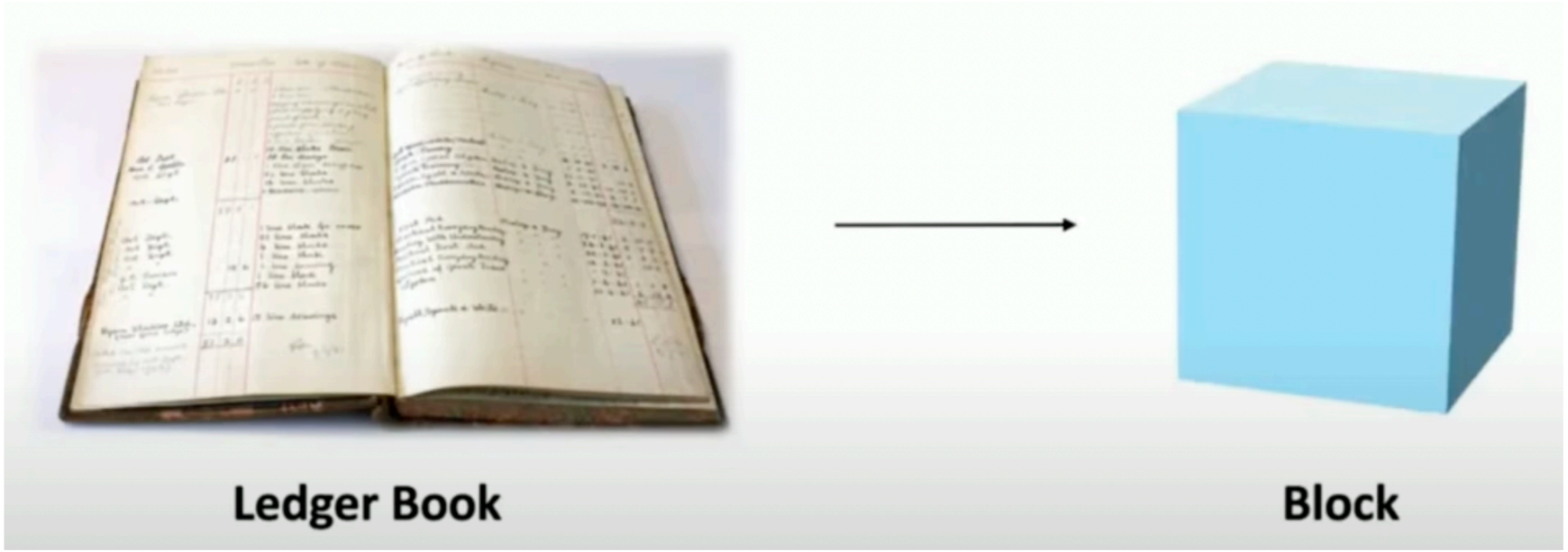
What is Blockchain?

- The idea originated from a research paper written by Stuart Haber and W Scott Stornetta.
- Blockchain is a **decentralized distributed immutable ledger** which is completely **transparent and verifiable**.

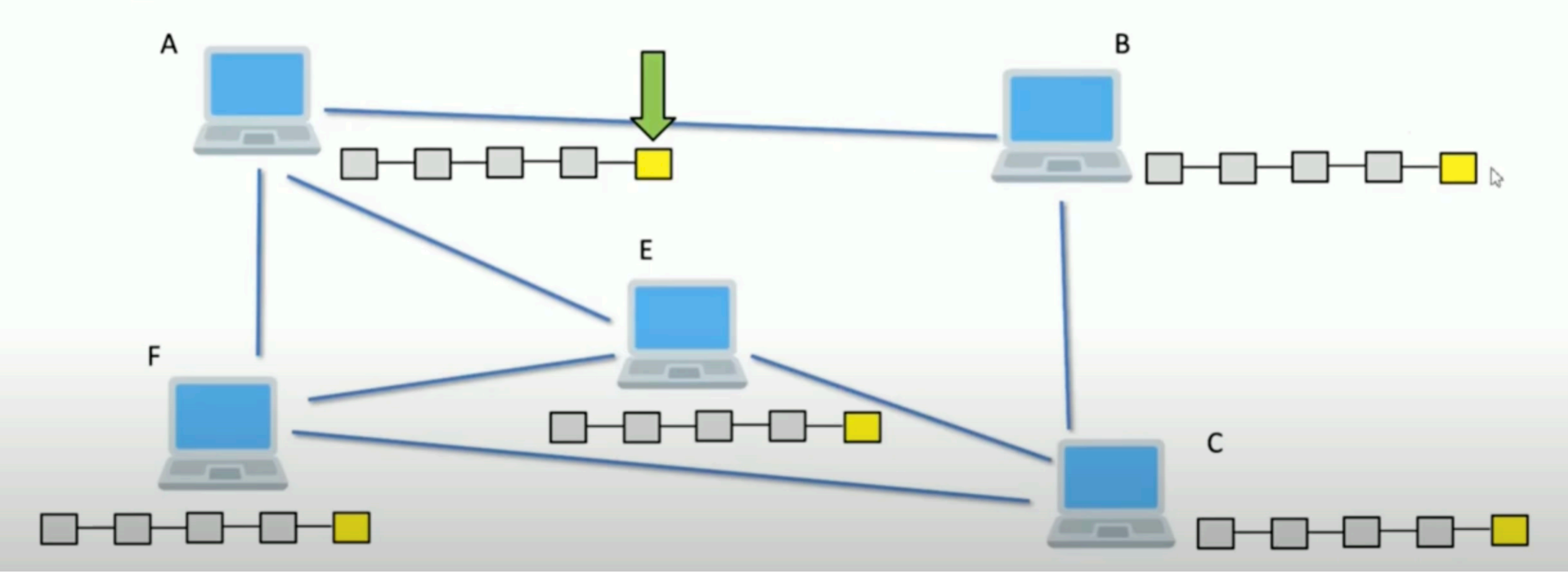




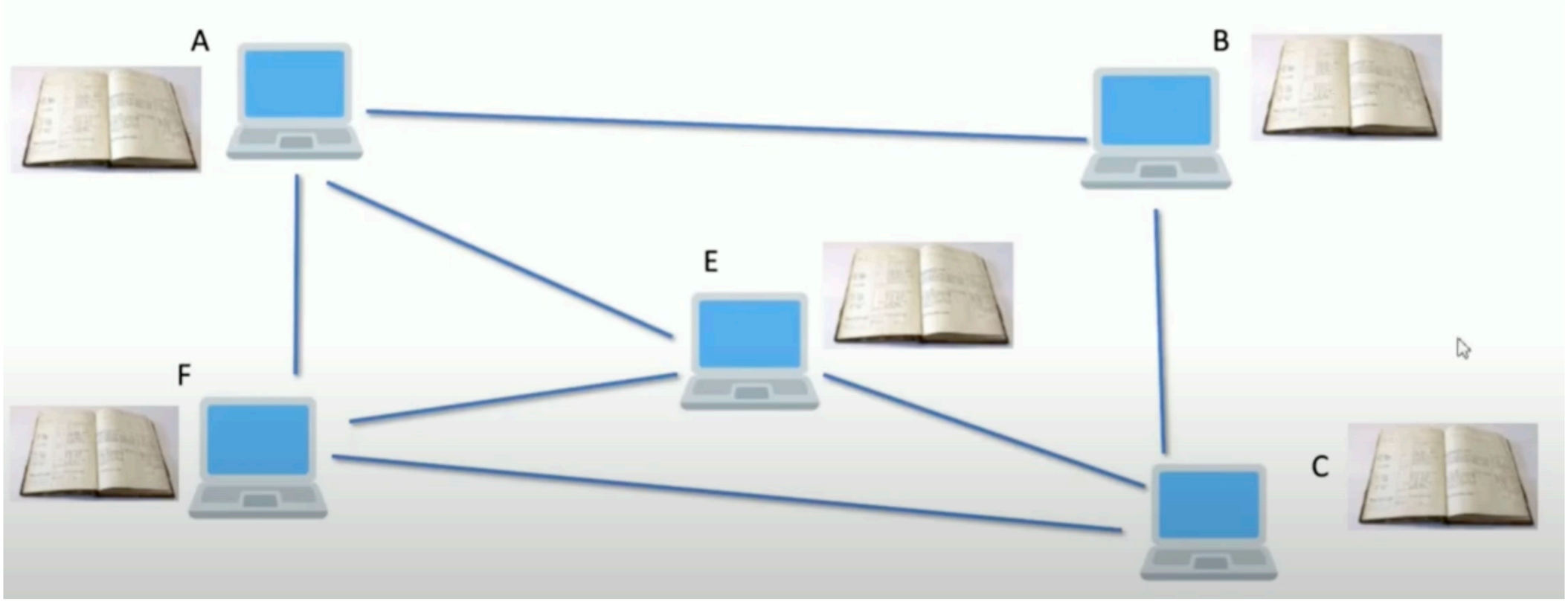
- What if a notification is sent on your mobile when the shopkeeper alters the record?



- Blockchain replaces ledger book with a block. Blocks represent transactions.
- Once some data is fed into a block or a transaction is written into a block, it cannot be altered or tempered with - **immutable**.



- The system is **decentralized** - no central server or agency is there for monitoring. All the machines are considered as peers.



- The ledger is **distributed** over many systems connected in a network.
- Once a transactional block is added to the blockchain on one computer, all the other computers connected to the network and part of the blockchain, start showing the newly added block.
- Any changes made by A are visible to all others. Identical ledger is stored with all peers - **transparency**.

Applications

Product Tracking

- Track the origin of the product and the entire route of the product supply chain.
- Ex- A supermarket in Denmark has implemented blockchain. Every product has a barcode which on scanning gives the complete details about the product.
- This prevents selling of fake products.

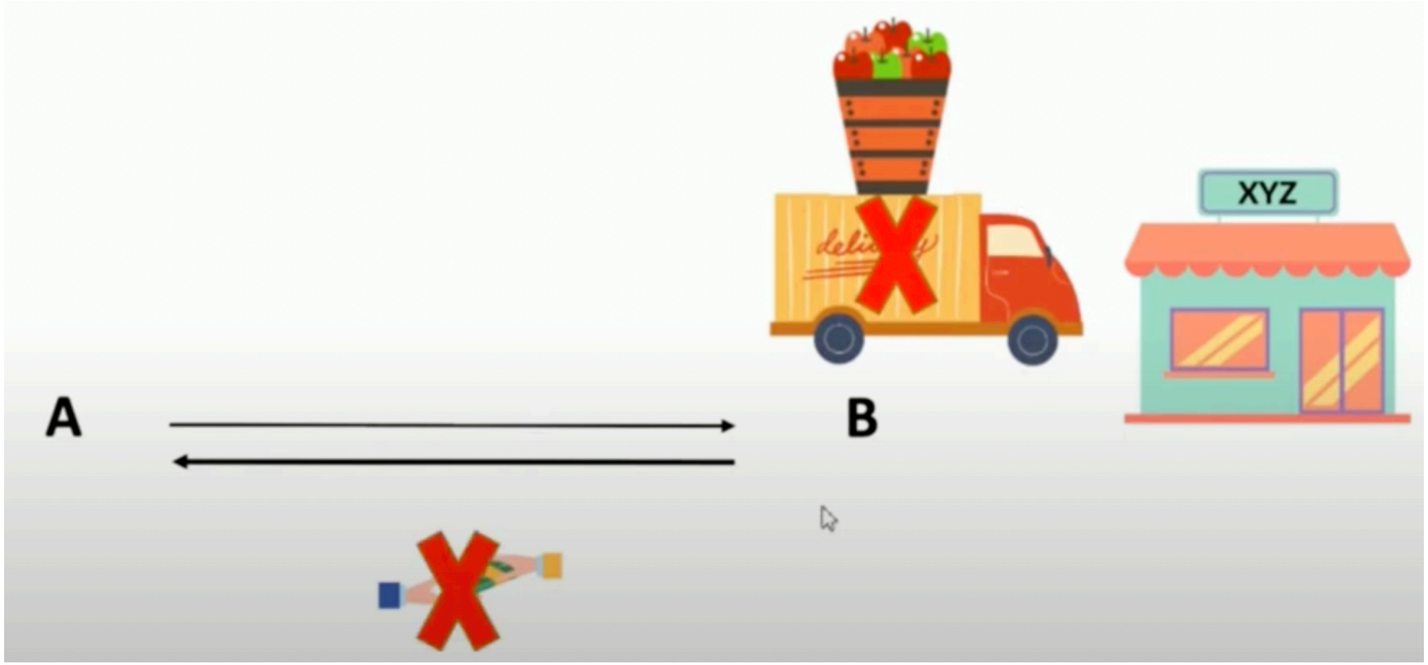
Smart Contract

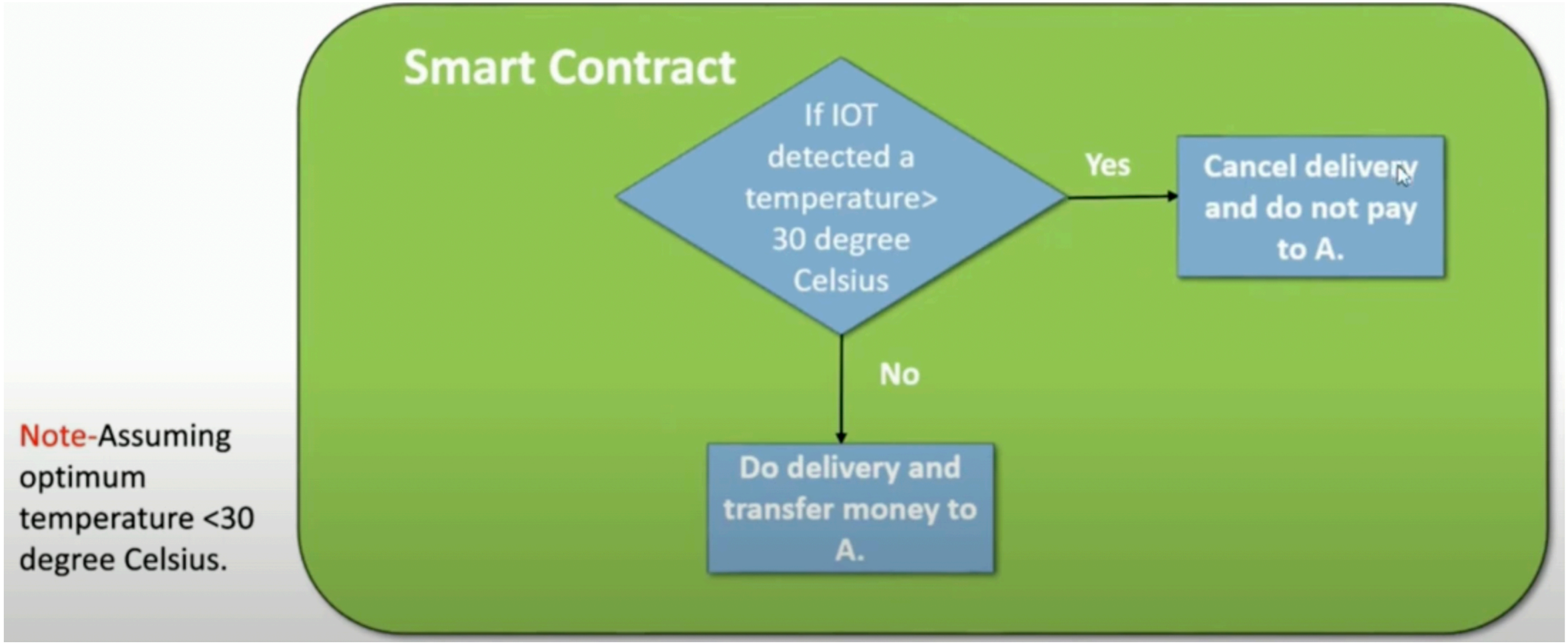
International Wire Transfer

Healthcare Systems

Smart Contract

- It is a program written in a programming language which runs on **ethereum** blockchain.
- Ex- Let A delivers fruits to a shopkeeper B. For the fruits to be kept fresh, a temperature is maintained in the container carried by A. On delivery of the fruits, B pays money to A. However, the fruits delivered to B may be stale or B can deny to pay money to A. Both parties may face losses when there is lack of trust.

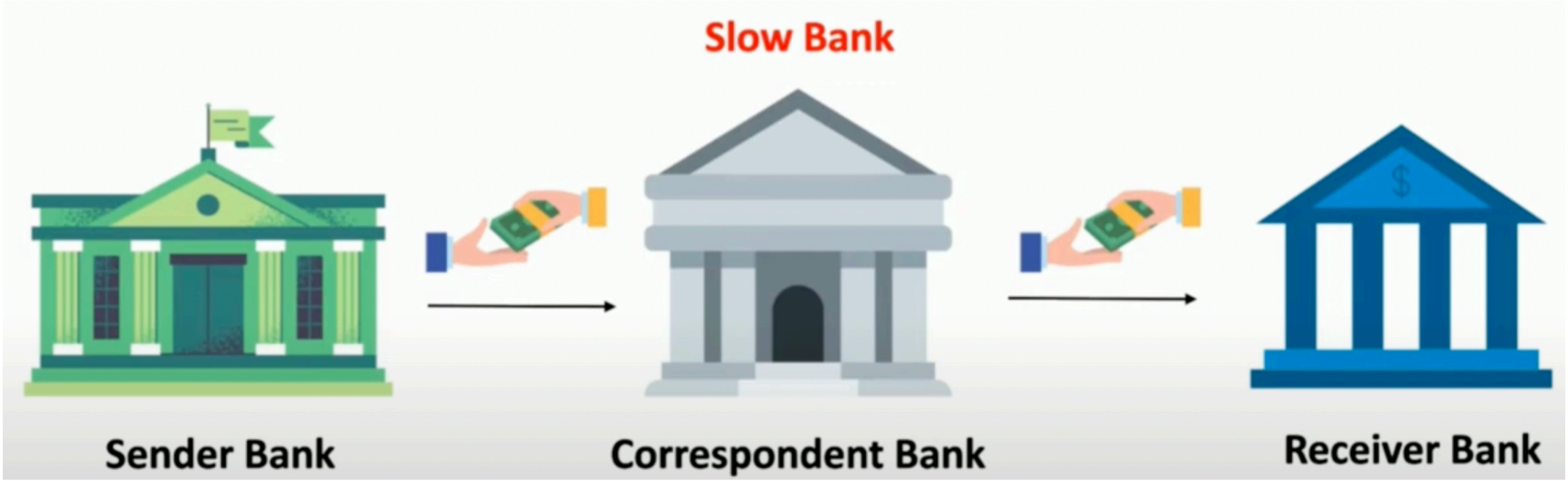




- Once the program is fed into a block of the blockchain, it becomes immutable and will be executed.
- No courts or a third centralized party is needed to resolve cases.

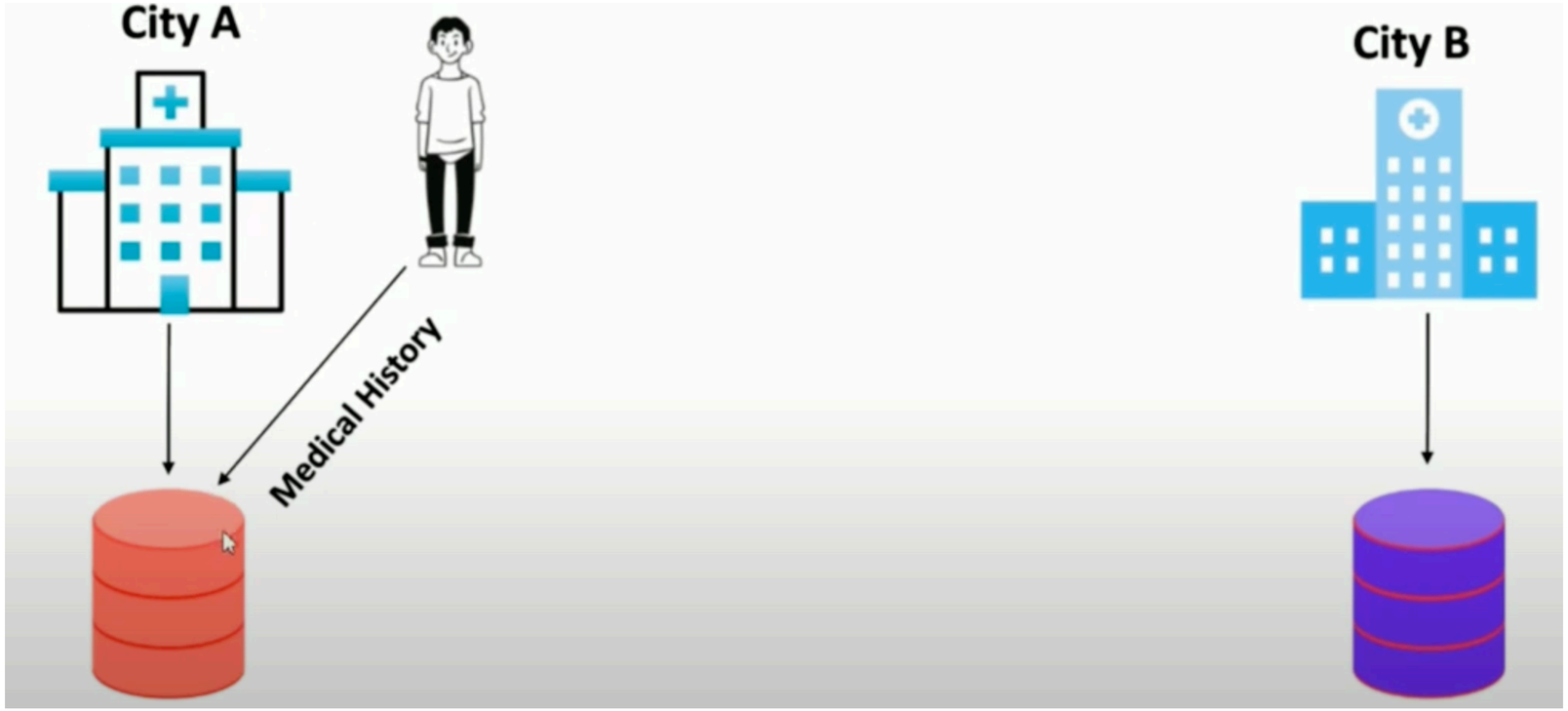
International Wire Transfer

- Transferring money from India to some other country, ex - USA, requires this process.
- Go to sender bank and deposit money. Sender bank doesn't directly transfer to receiver bank. Instead it transfers to a correspondent bank for verification and paper work. The money is then transferred to the receiver bank.
- This leads to huge processing fees (10-30%) and is a slow process.
- Blockchain requires 1-2% fees and is very fast.

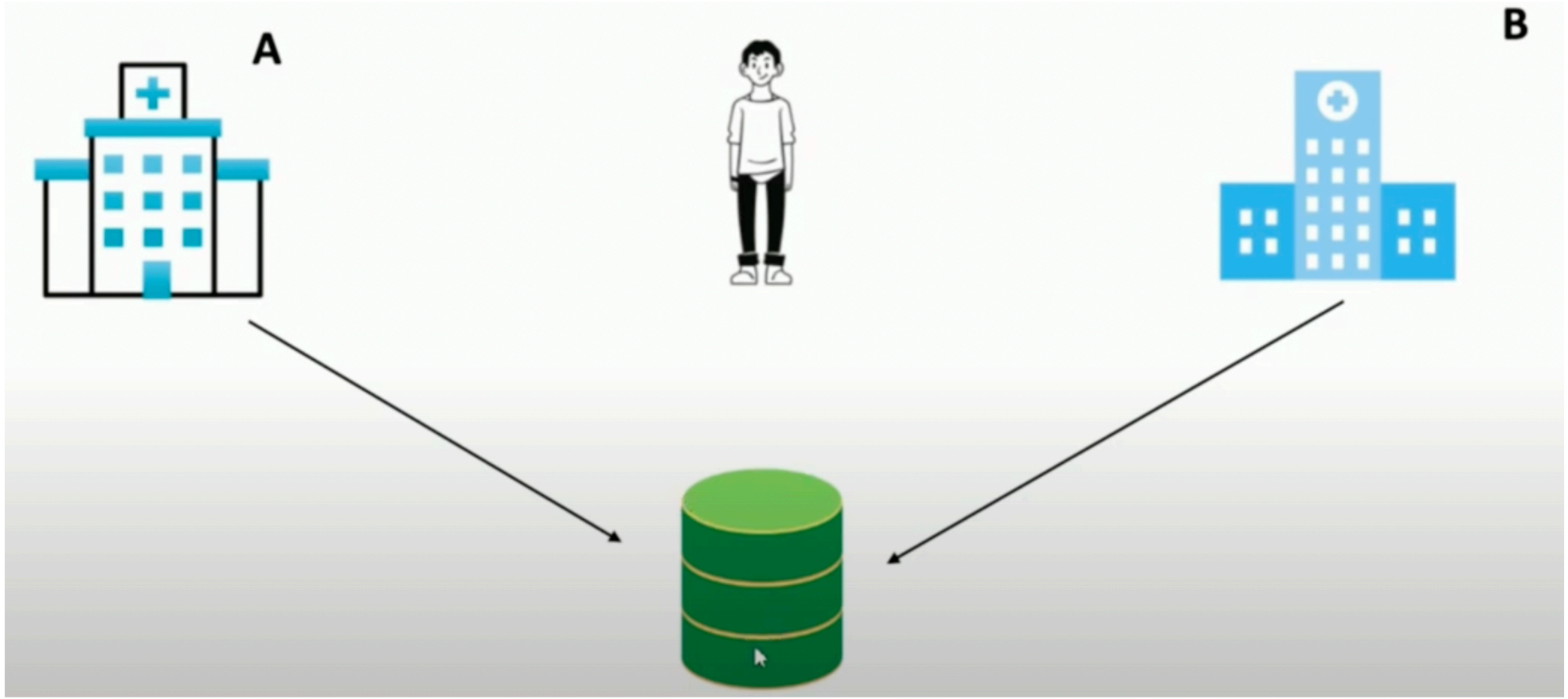


Healthcare Systems

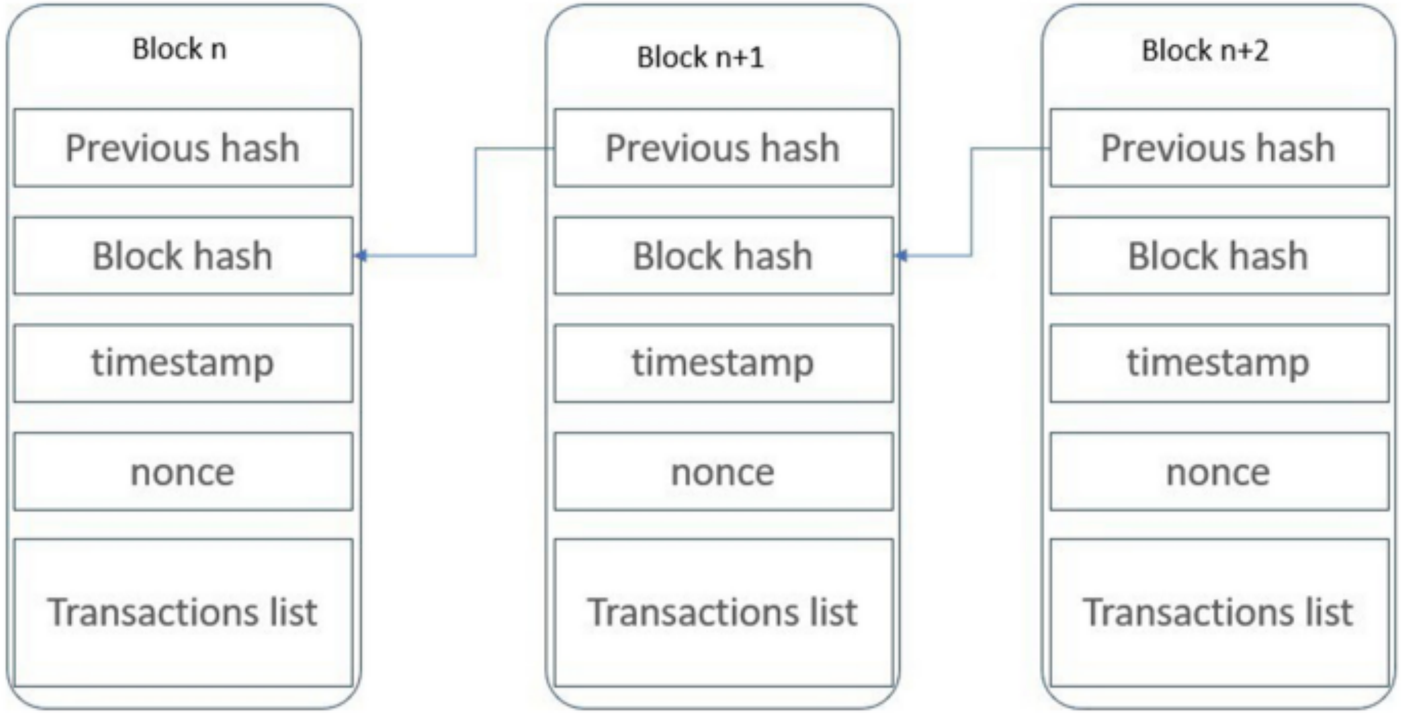
- A person X residing in city A moves to city B. However, his medical history was maintained with City A hospital.
- If X has an emergency in city B, his admission may be delayed due to several checkups.



- If a blockchain for X is maintained, A may update the blockchain and store X's history in terms of blocks.
- B can access X's blockchain for the medical history.



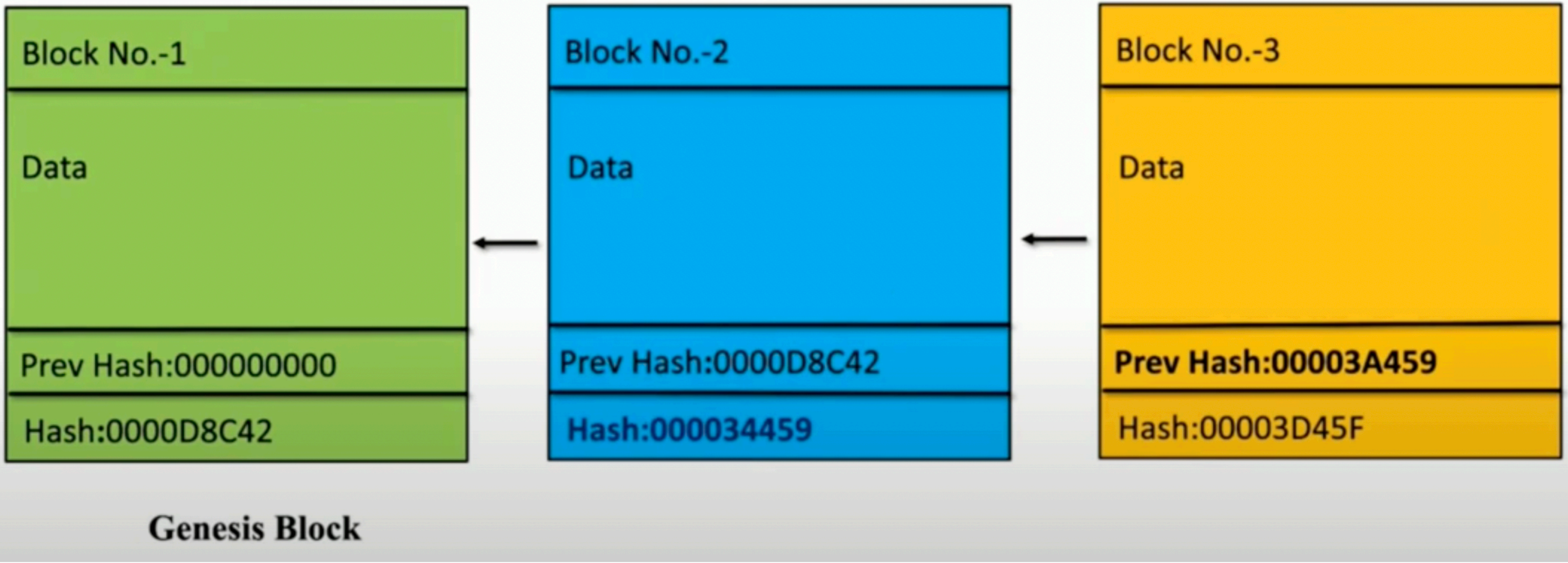
What's inside a Block?



- A block consists of several fields - Block No. , Data, Nonce, Timestamp, Prev Hash, Hash etc.
- **Block No.** Indicates which block it is in the blockchain.

What's inside a Block?

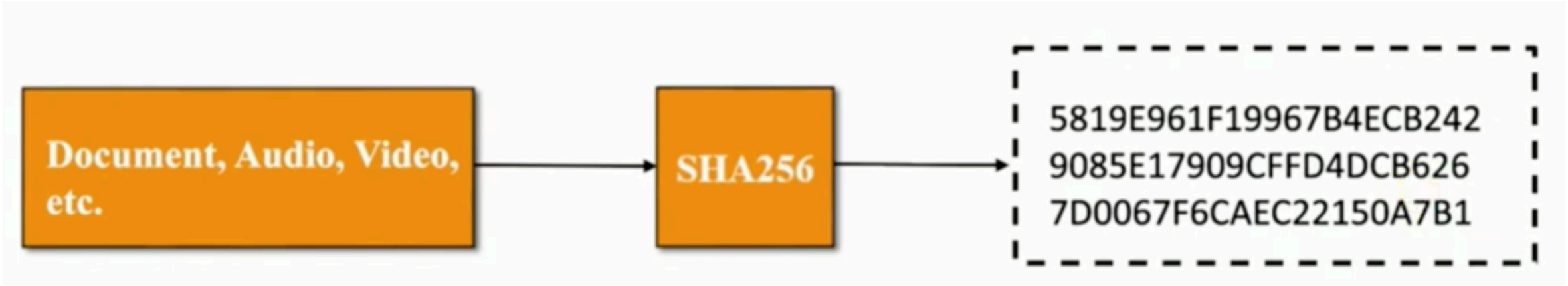
- **Data** represents the actual transactional data for which the block was added into the blockchain.
- Each block in the blockchain is represented by a **Hashcode (unique Fingerprint)** which is computed on the entire block contents - Block No, Nonce, Data, Timestamp and Prev Hash.
- **Prev Hash** is the Hashcode of the previous block in the blockchain and Hash is the Hashcode of the current block computed on all the content including Block No., Data, Nonce, Timestamp and Prev Hash.
- **Nonce** - Number used only once. Block No., Prev Hash, Timestamp and Transaction data cannot be altered. In case some other targeted hash value is needed, nonce value can be changed.
- **Timestamp** - a record that pinpoints when a specific transaction or event occurred, often detailing the exact date and time



- Each block points to the previous block using prev hash just like the prev pointer in double linked list.
- The Prev Hash field of the first block is empty and it is usually called **Genesis** Block.

SHA256

- Secure Hash Algorithm is used for generating Hashcode comprising of 256 bits in Blockchain.
- Takes a message as input, encrypt it and generate a 64 digit hex number or hash.
- Each hex digit is 4 bits hence total 64*4 = 256 bits.

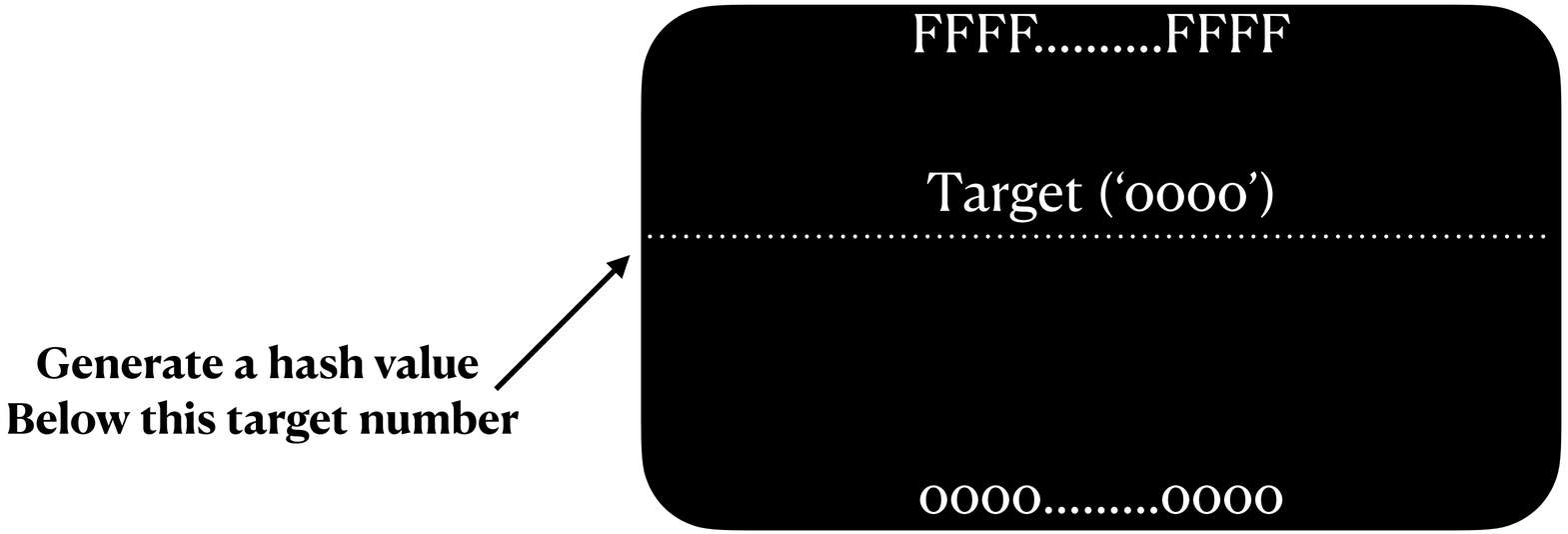


Five requirements of hashing algorithm

- **One way** - Input data is provided to the algorithm to generated the encrypted message. However, the encrypted message can’t be decrypted to get back the original data.
- **Deterministic** - Same input data will generate the same output no matter how many no. of times the input is provided to the algorithm.
- **Fast Computation** - The algorithm should be fast otherwise much time will be required for encryption.
- **Withstand collisions -** Given a hashing function H, no arbitrary x and x' can be found where H(x)=H(x'). In words, no two x's can be found where the hashing function would create a collision.
- **Avalanche Effect** - A little change in the input data leads to significant change in the encrypted output.

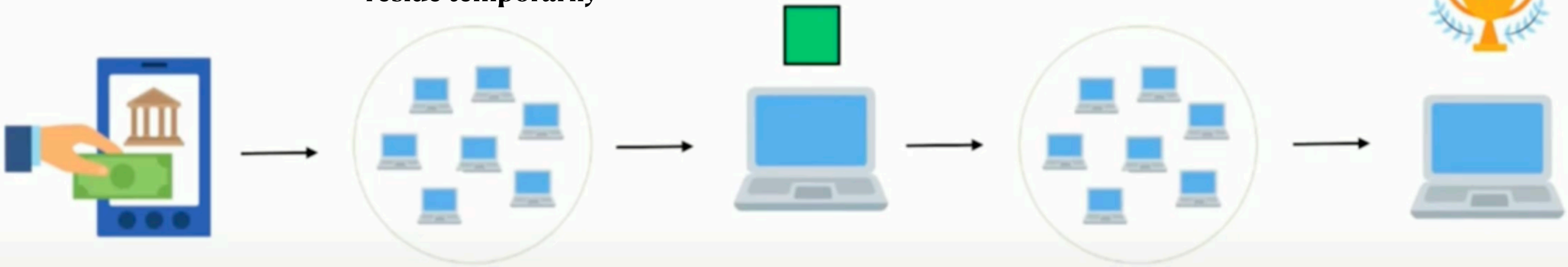
Mining

- The process of generating a hash value in a target area.
- The generated hashcode is then assigned to a block and the block is then added to the blockchain.
- Different nonce values may lead to different hash codes. Mining involves trying different values of nonce to generated a targeted Hashcode, since other entries can't be modified.
- Mining requires high computation power and is time consuming. People who perform mining are called **miners**.
- There is no direct or predictable relationship between nonce value and generated Hashcodes.
- Visit https://demoblockchain.org/blockchain



Reward

Mempool - where transactions reside temporarily



Transaction

Solve Mathematical Problem

Miner Solved Problem First

Miners Verify the Validity

Block is added

Find Nonce value to generate target hash

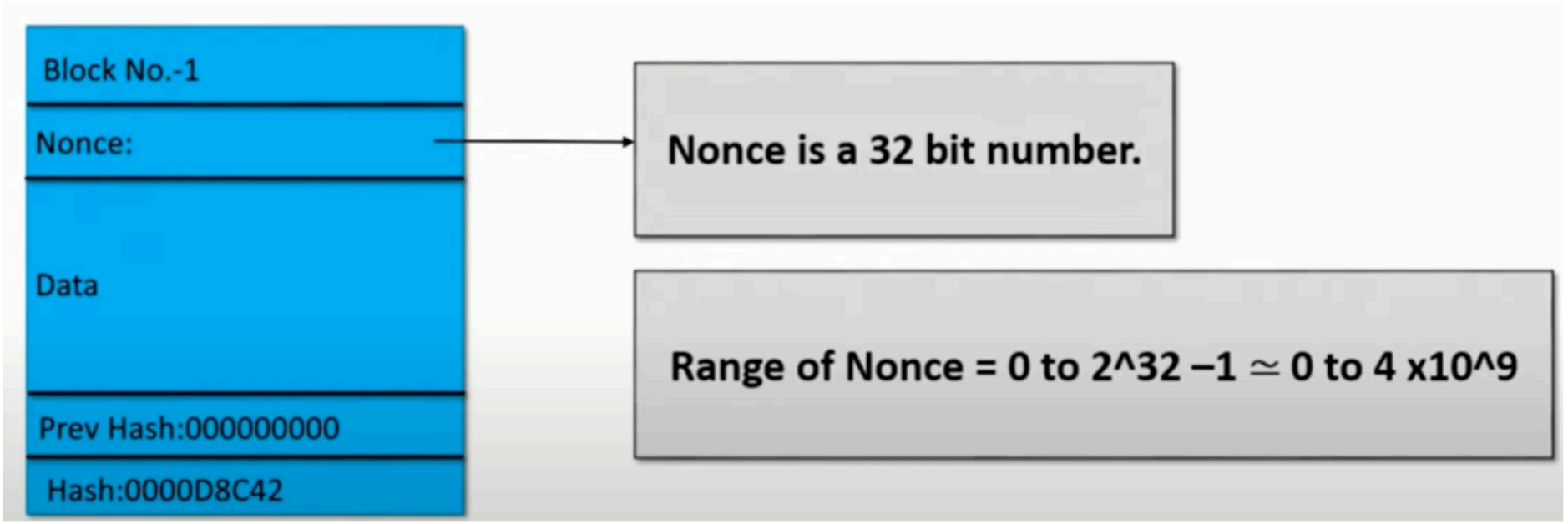
Proof of Work (PoW)

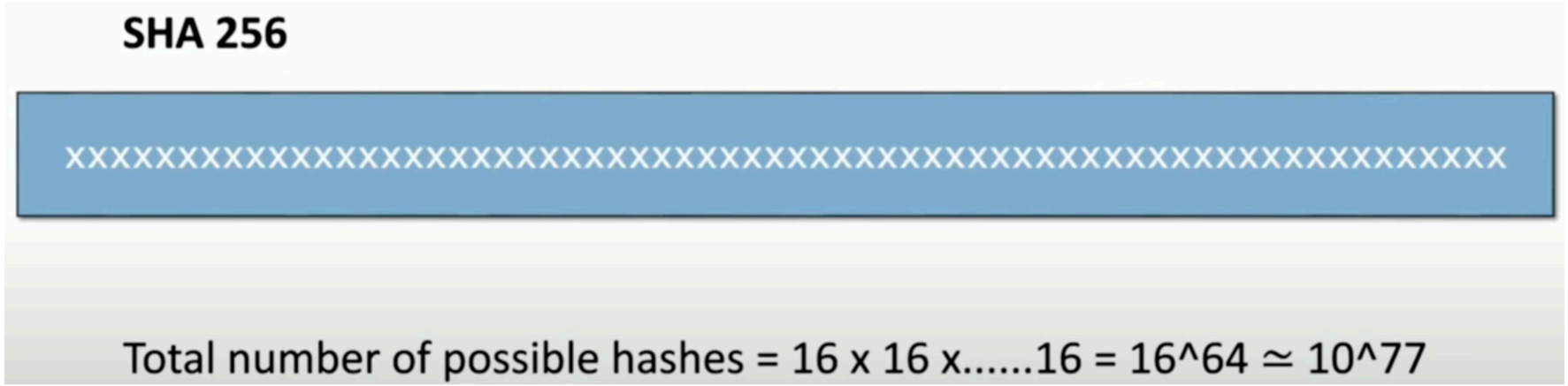

Block No.- 6
Nonce: 23
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 00001ba1


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


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


Block No.-7
Nonce:512
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000b6aa
All Possible Hashes
Largest
Smallest
Target('0000')





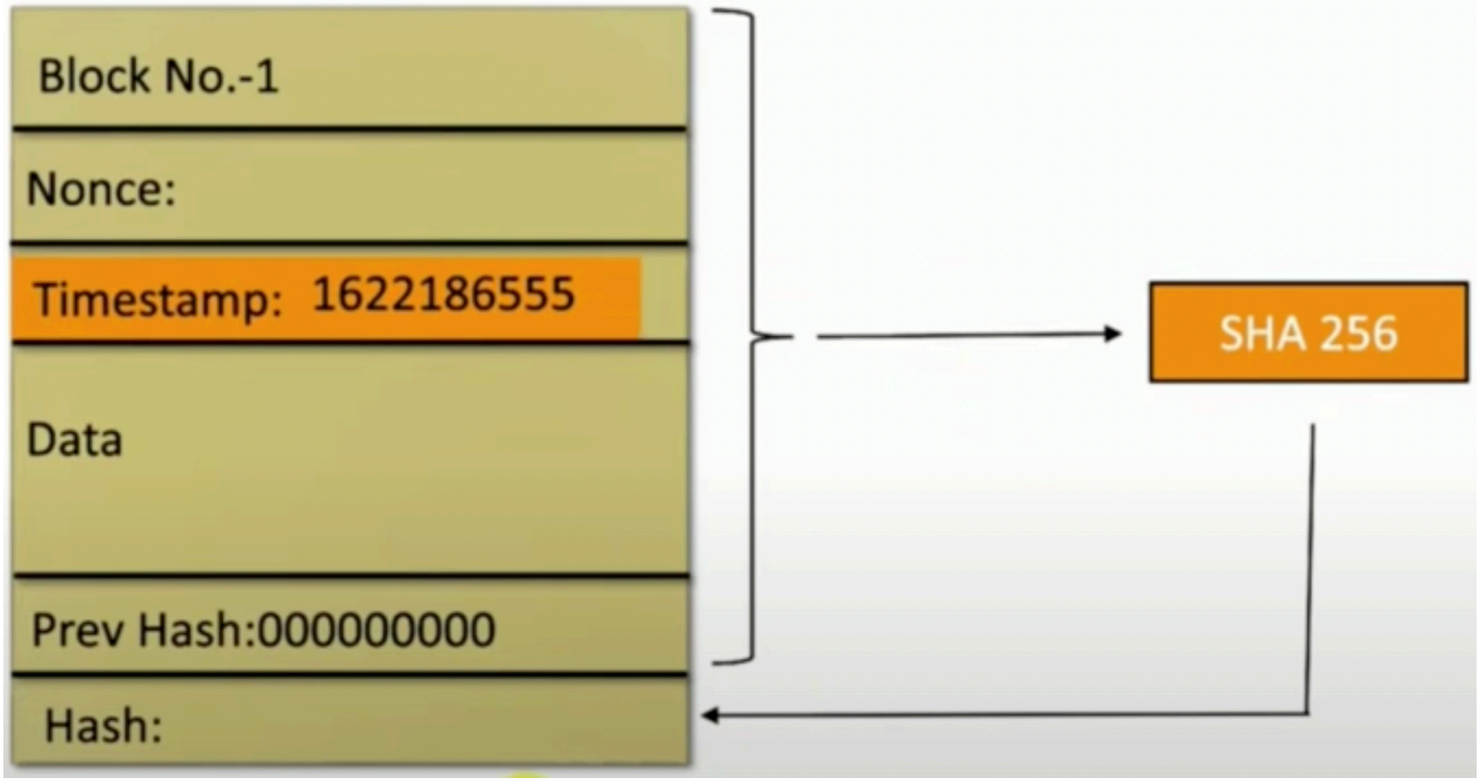
- 4 Billion possible values of nonce, hence 4 billion different values of hash can be generated.
- There are not enough nonce to generate the valid hash. It may be possible that the valid hash is not obtained.

A modest mines does 10^8 hashes/sec.

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

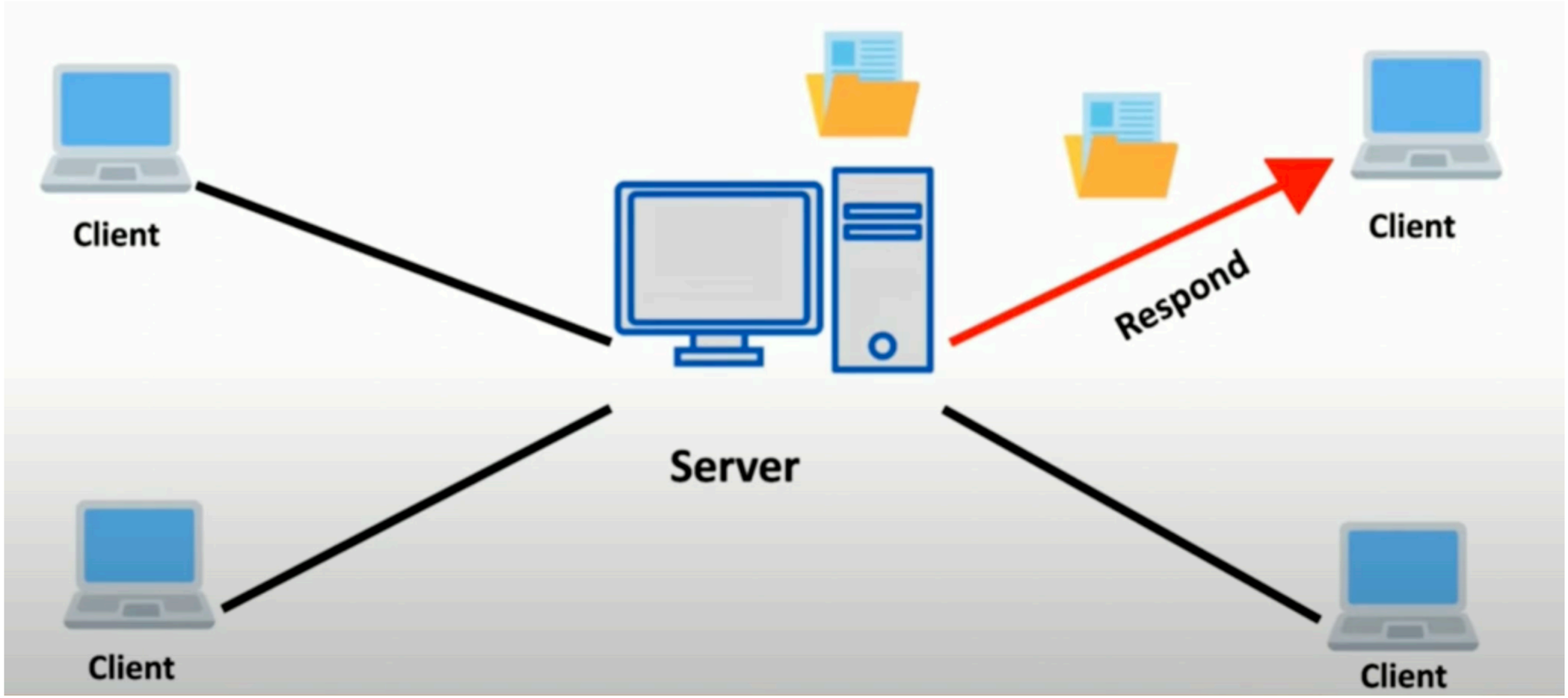
Q) So what the miners do when all the nonce get exhausted and miners have not hit the target ?

- To solve this issue, **Timestamp** was introduced in the block. It represents **unix time** - number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970.
- The 1 January 1970 00:00:00 UTC was selected arbitrarily by Unix engineers because it was considered a convenient date to work with.



- In 40 seconds, 4 billion nonce values are tested. In 1 sec - 0.1 billion nonce values will be tested.
- After 1 second, the value of timestamp will be changed and starting nonce from beginning will generate a new set of hashes. So nonce are not exhausted.
- However, Current hash rate is more than 650 million trillion hashes/second. (blockchain.com -> charts -> total hash rate). So all nonce will be exhausted in <<<<<<1 sec. What should miners do in idle time till timestamp is not changed?

Centralized Network



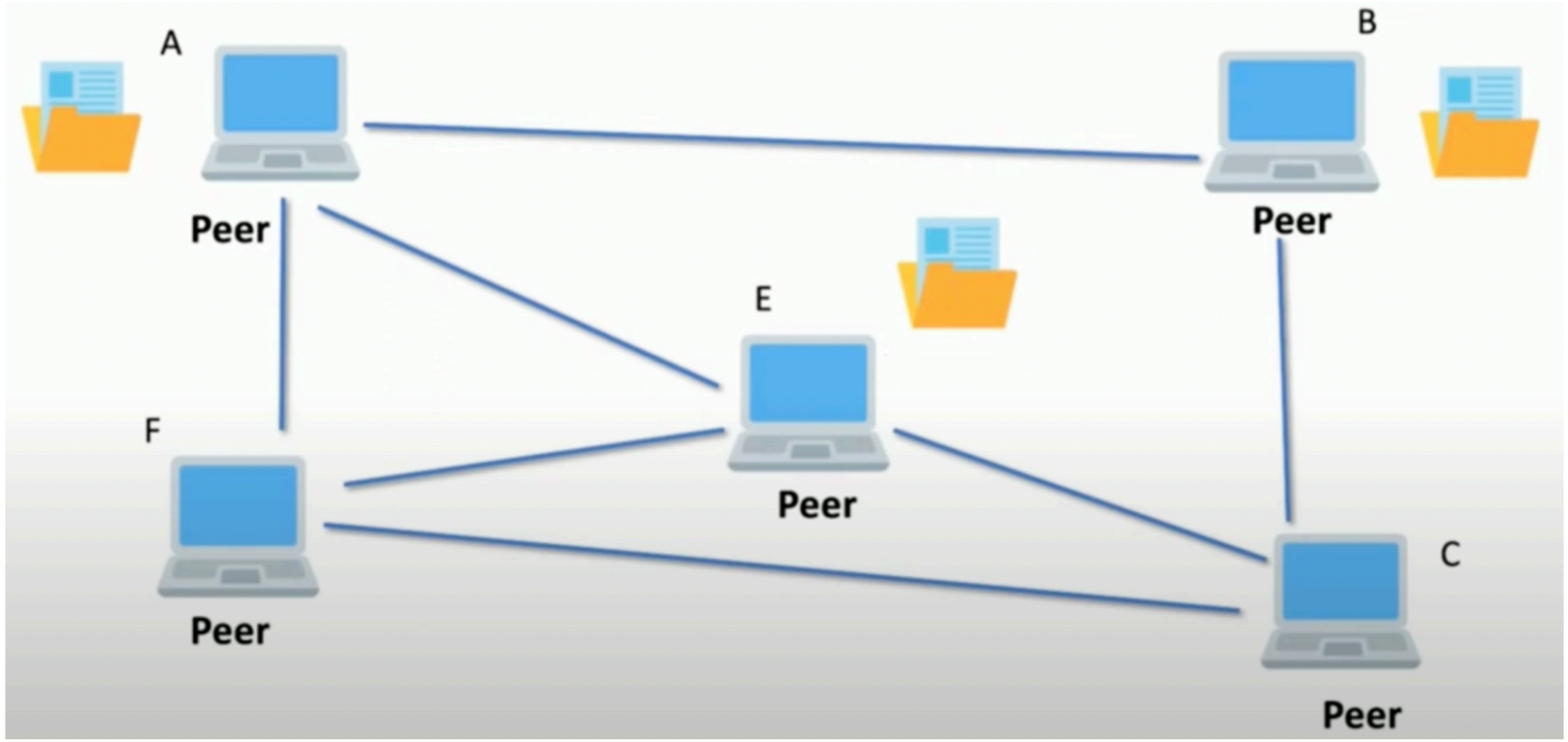
- In a centralized network, there is a central server where all the data resides. The client machines request the server for user specific data.
- Ex - Banks, Social Media etc.

Disadvantage

- This system can be easily hacked since all the data resides on a single machine. This compromises data privacy.
- If the server is down, the entire network will be down.

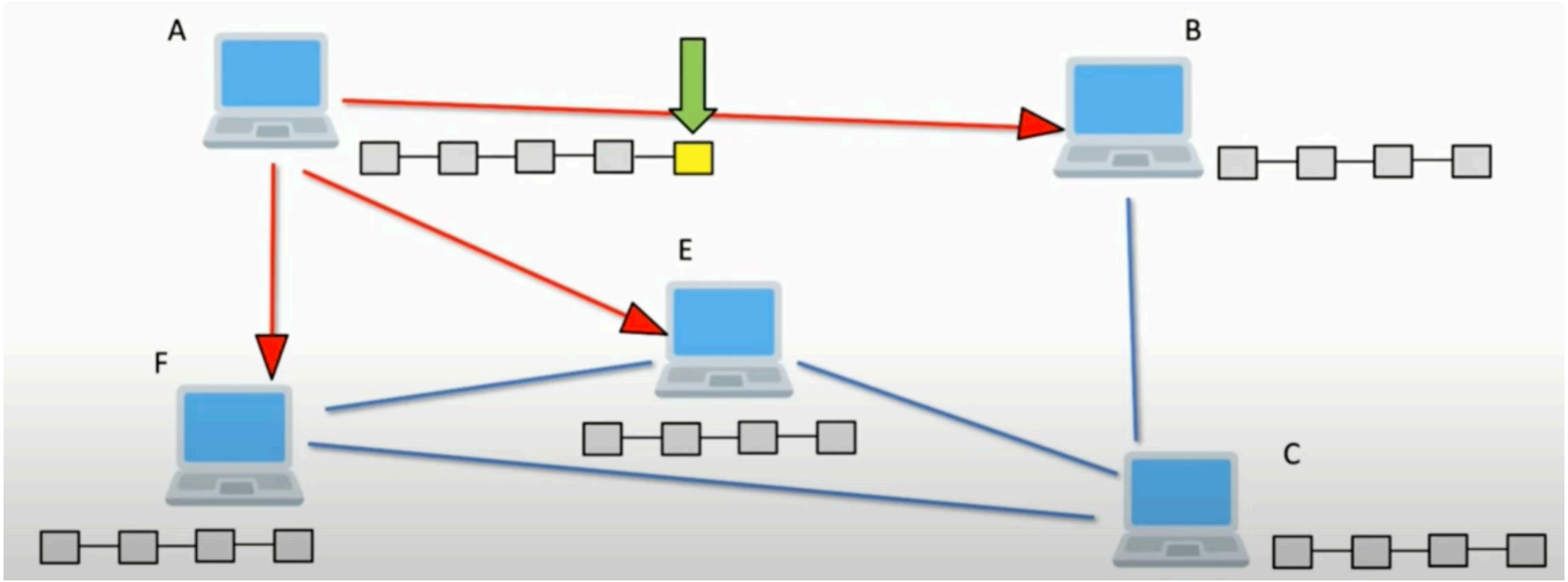
Distributed P2P Network

- All the machines are considered as **peers**. The data is distributed among all peers.
- The peers can request each other for data. Data copies reside on multiple peers.
- Even if a system is hacked, the data will be available on other peers.

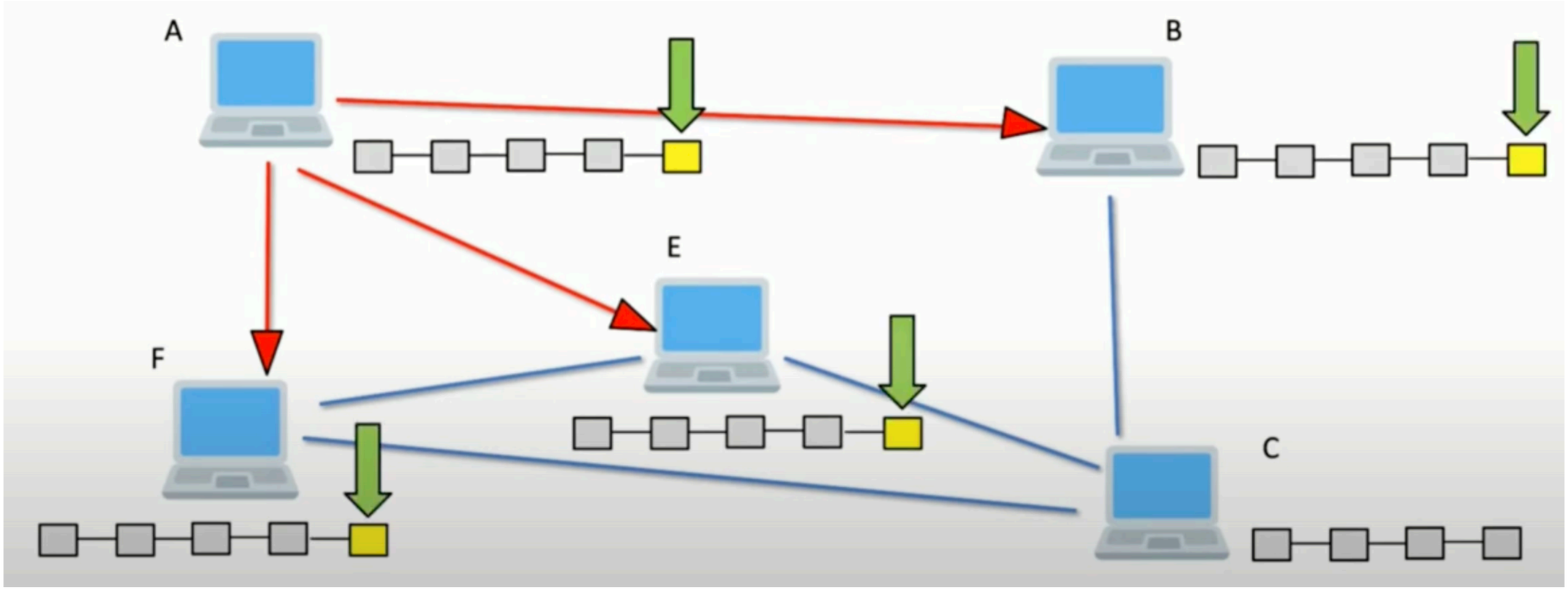


Distributed P2P Network in Blockchain

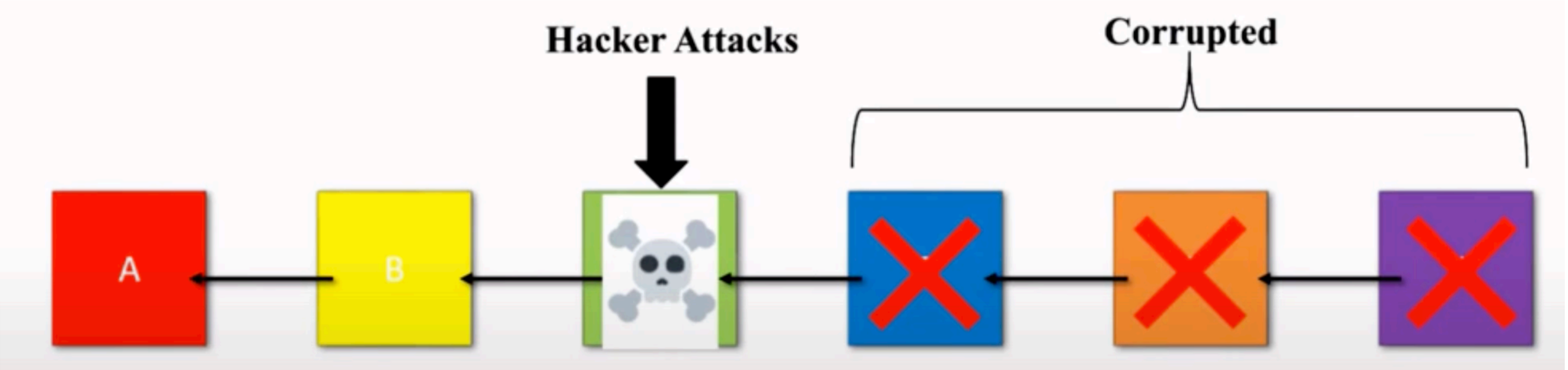
- All the machines have their own copy of the blockchain.
- If a block is mined let's say by miner A, it will be added to A's blockchain.
- Once the block is inserted, all the miners connected to A - B, E, F, are informed and their corresponding blockchains are updated after verification of the block.



- B,E and F further inform their neighbor nodes about the newly added block and this continues until the block is added in the entire network.

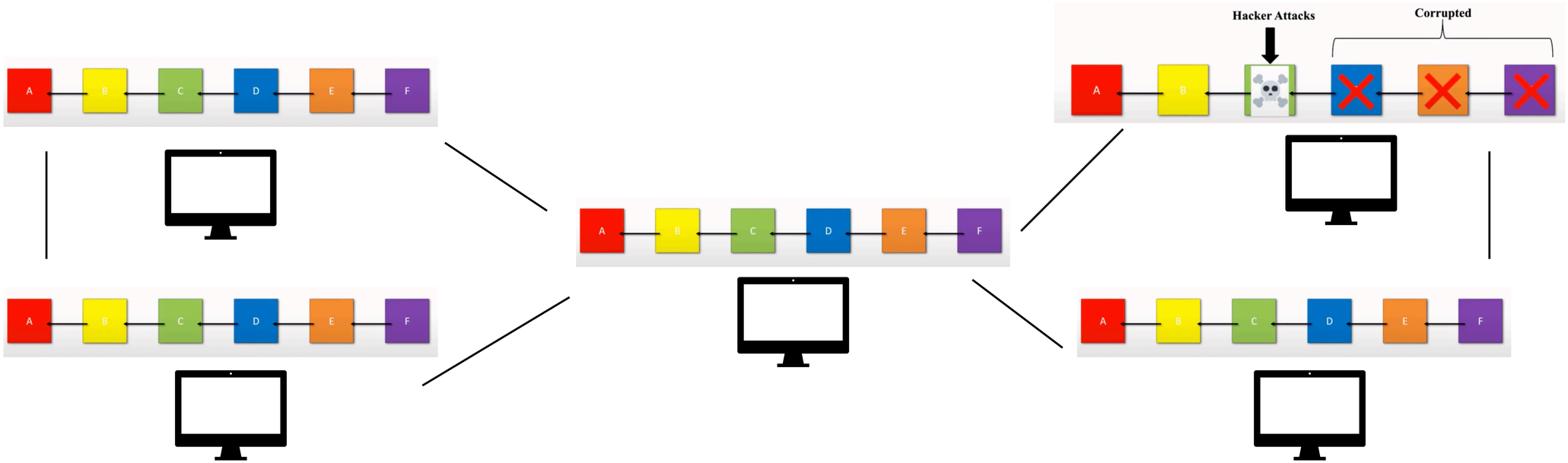


Immutable Ledger



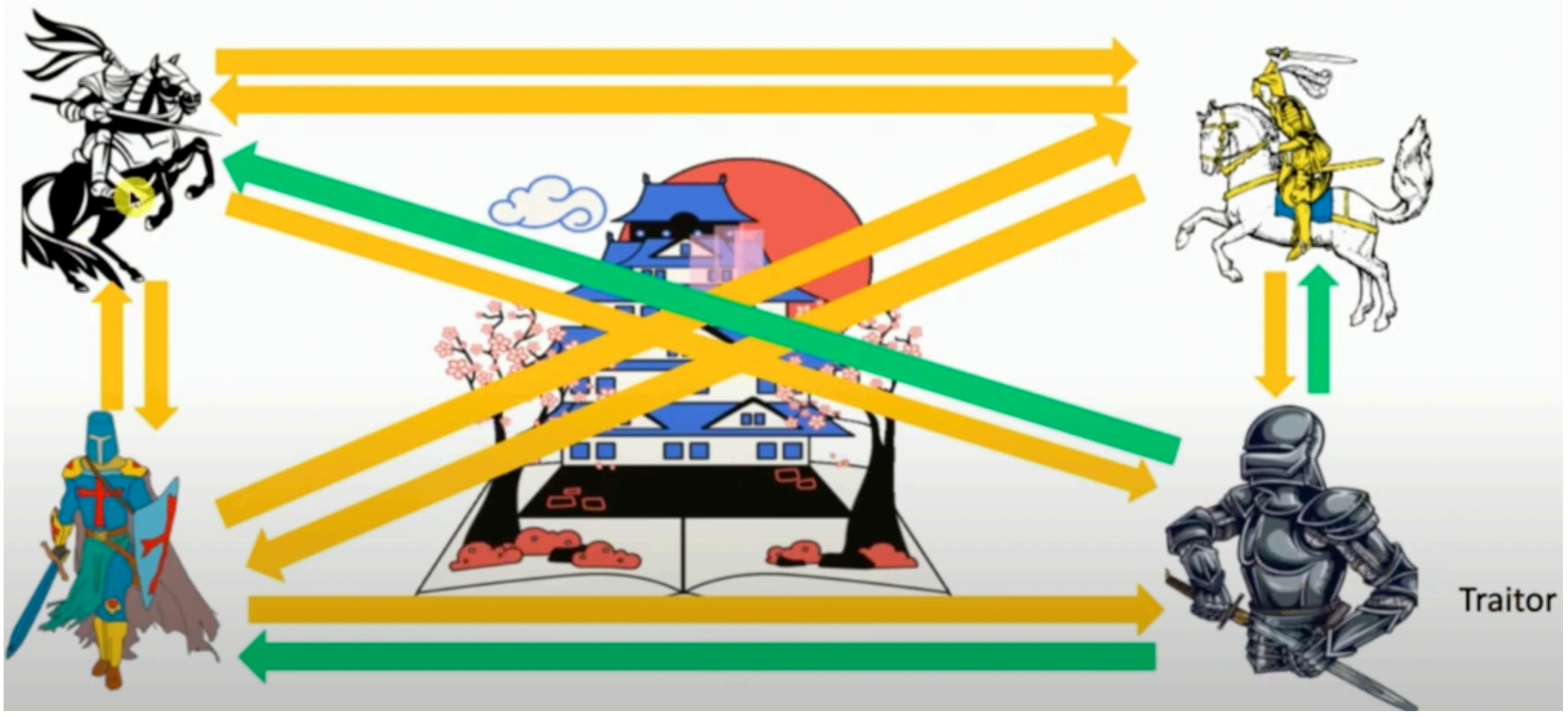
- Let's say we have a blockchain with six blocks - A,B,C,D,E and F. Suppose a hacker attacks and tempers block C.
- This tempering leads to corruption of all the blocks ahead of C since the block D contains the Prev Hash which is the Hashcode value of C. If C is tempered, its Hashcode is also significantly changed which leads to changes in D.
- Now, since D's contents are changed, its Hashcode is also changed significantly and this continues. Hence, the user get to know it has been hacked.

- However, the blockchain is not stored on a single node or machine. It's local copy is distributed over all the nodes connected to the network.
- After fixed interval of times, the blockchain is **verified** for consistency on all the nodes. If the blockchain is corrupted on one of the nodes, it will be recovered to its original state since the majority says otherwise (**Majority Voting**).
- Hence, in order to actually corrupt a blockchain, the hacker must corrupt on at least 51% of the machines, which is impossible to do so within the stipulated time in which the blockchain is verified again.



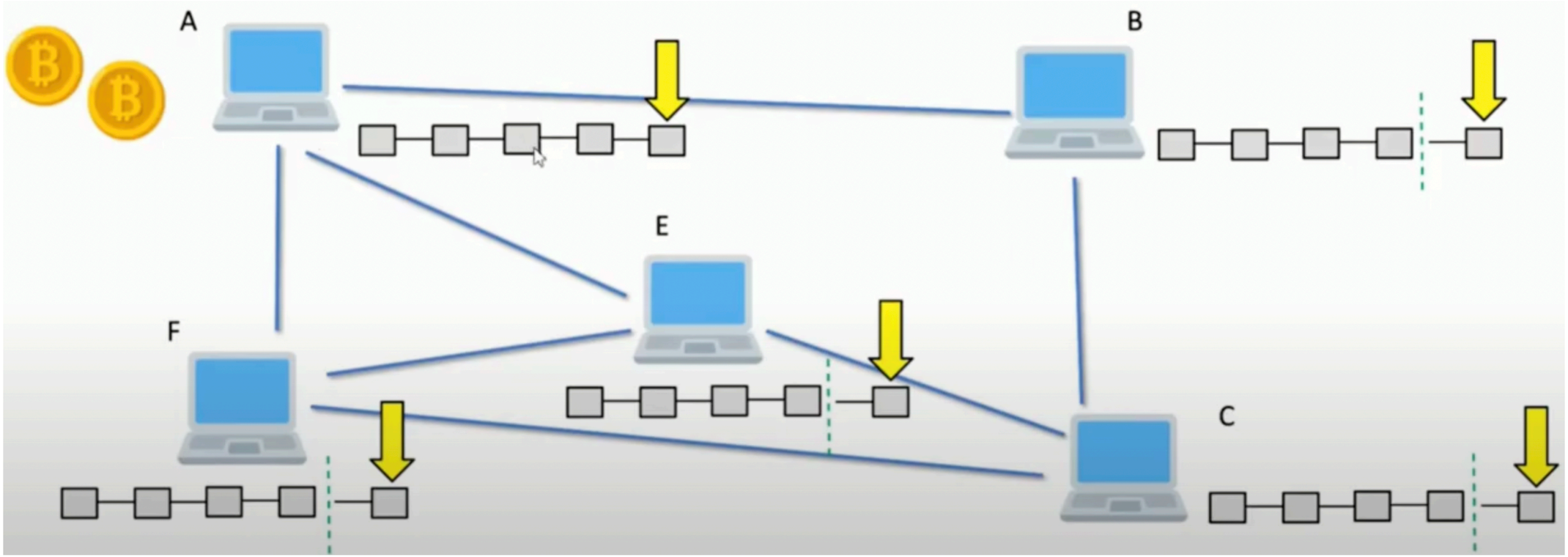
Byzantine Generals Problem

- There are four generals belonging to the same army, attacking the enemy kingdom from different directions.
- All four have to decide when they should attack.
- They communicate with each other and inform each other on whether they should attack or not.
- If any of them is a traitor, he may deny to attack and the army may lose.
- Same problem is encountered in distributed systems where there is no centralized system to guide whether the information provided by a node is correct or not.
- **Solution** : Byzantine Fault Tolerance - If less than or equal to 1/3 nodes are corrupted or say otherwise, accept what is said by 2/3 of the population.


Traitor

Consensus Protocol

- A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure.
- Used to prevent attacks
- Used for solving competing chain problem
- Mainly two types - Proof of Work (POW) and Proof of Stake (POS)

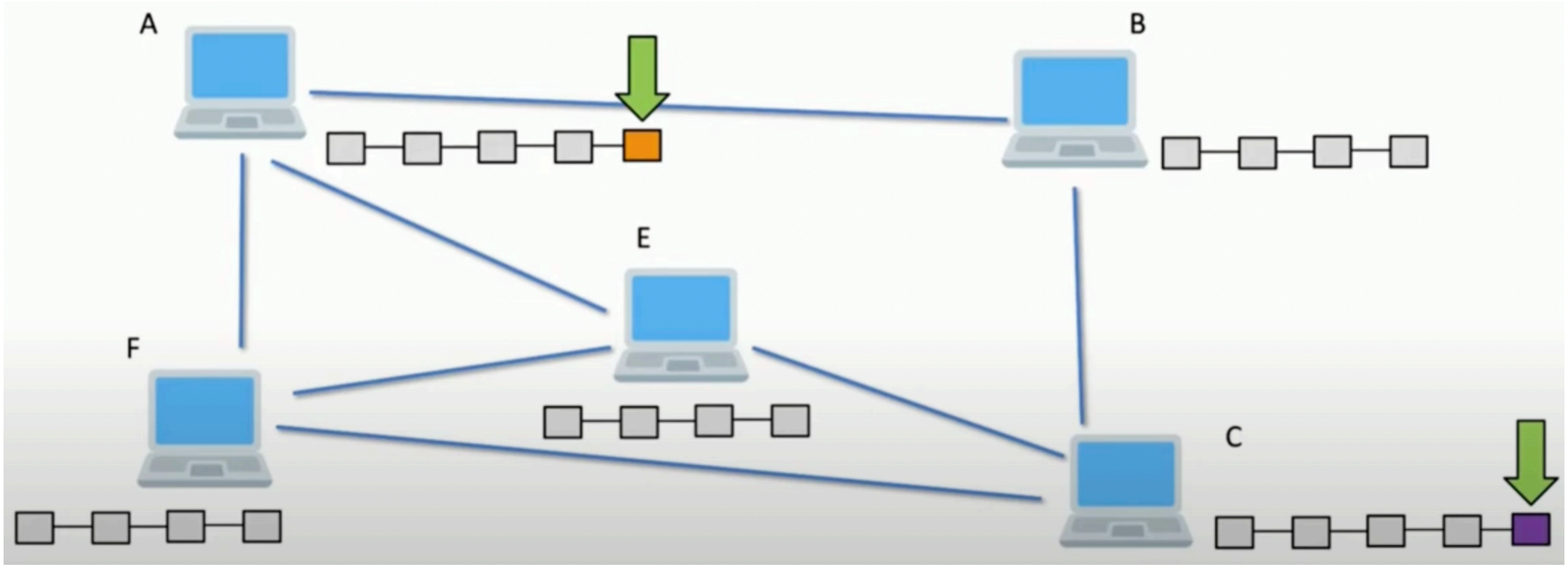


- POW is used in Bitcoin. Whenever a miner solves the mathematical problem of finding a target hash, the block is added to the blockchain after verification from all the nodes.
- This is called POW and the miner is then rewarded with bitcoins.
- Let's say a miner A adds a malicious block in the end of the blockchain. Then there are no blocks ahead of it that will be corrupted.
- However, this doesn't practically happen since a lot of computational power is required for mining and if a corrupt block is identified then the miners lose their reward.
- Also, before adding the block to the blockchain, all the other nodes verify the validity of the block by running an algorithm.

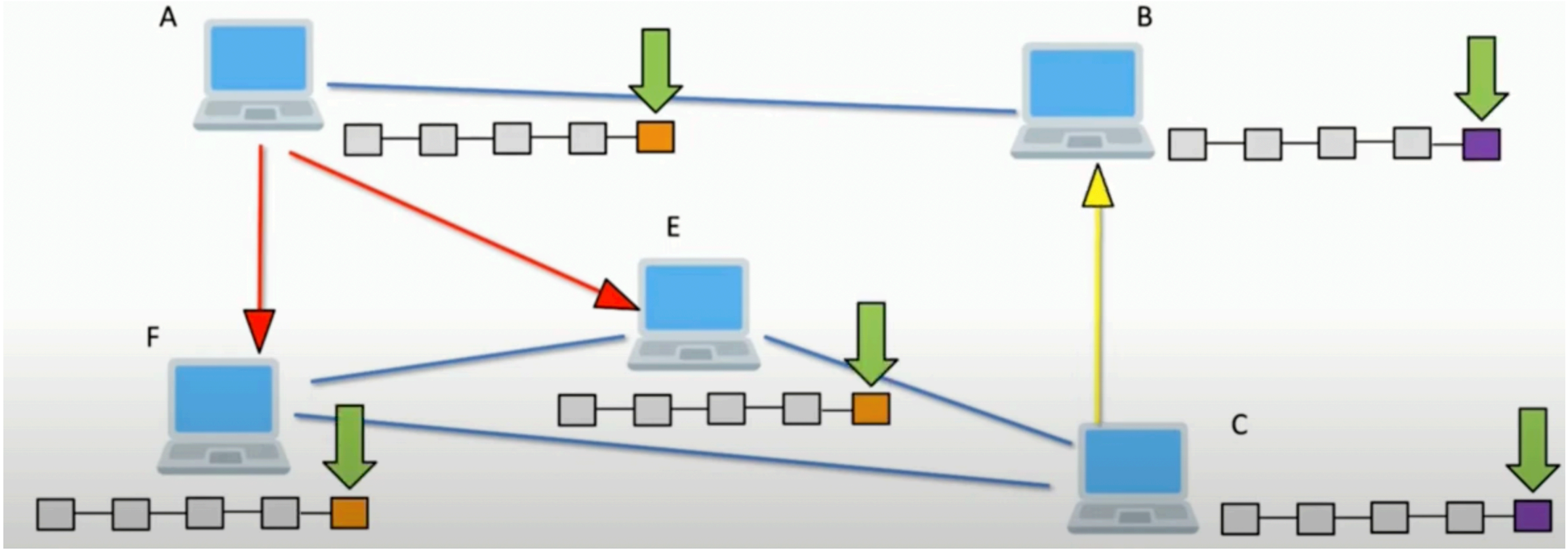
1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed nBits proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. 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:

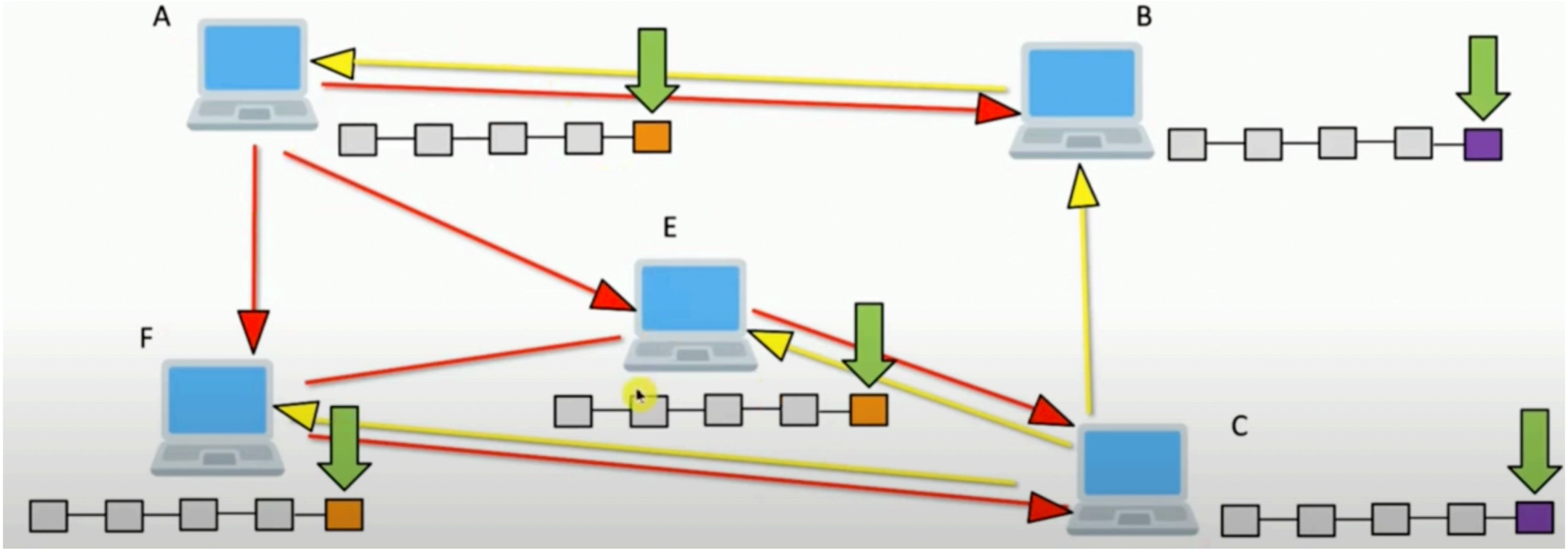
Competing Chain Problem

- Let two miners A and C mine different blocks at the same time. Now both will transfer this information to the rest of the network.

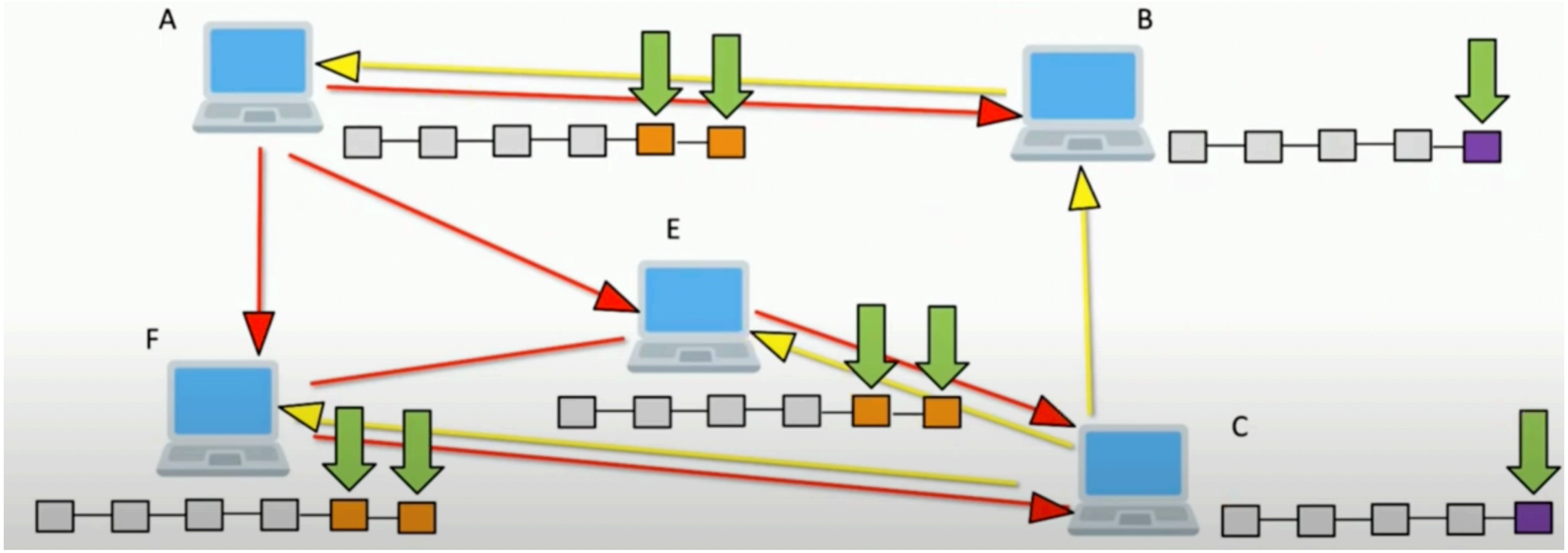


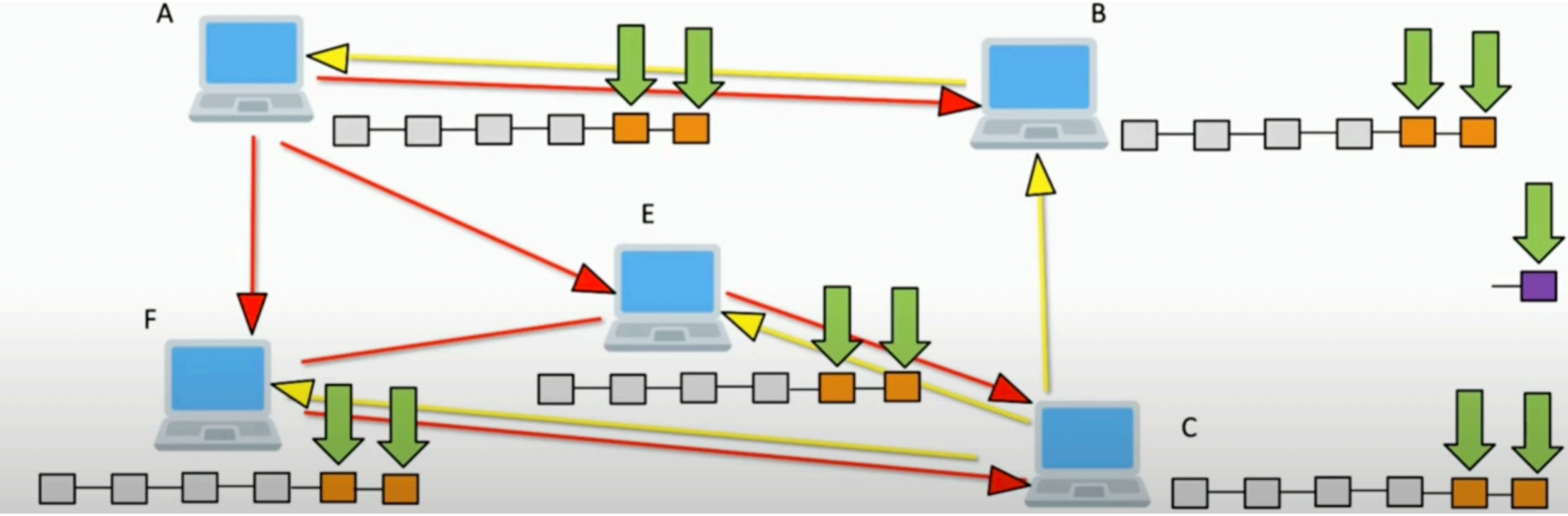
- Since E and F are closer to A and B is closer to C, the information reaches these nodes earlier.
- F and E validate the A's block and B validate the C's block and add to their blockchain.
- There now exists a conflict since different sets of blockchain exist on different set of nodes.




A
B
E
F
C

- Consensus protocol says that only the blockchain having maximum blocks will be considered valid. Others will be discarded.
- All the nodes now wait for the next block to be mined and added. Whichever miner is successful in doing so, it informs its subnetwork of the same and that subnetwork becomes more powerful.
- The other subnetworks then discard their added block and accept the longest blockchain.




A
B
E
F
C

- The discarded blocks are called **orphan blocks**.
- The consensus protocol of blockchain is much better than the byzantine fault tolerance as it only needs a 51% majority while BFT needs approximately 66%.
- All the transaction in the orphan blocks will be dropped and the miner that had mined the block will not get any reward.
- So that's why wait for 5 additional blocks to be added before assuming payment to be successful.

Proof of Stake (PoS)

- Proof-of-stake is a blockchain consensus mechanism for processing transactions and creating new blocks.
- Under PoS, block creators are called validators. A validator checks transactions, verifies activity, votes on outcomes, and maintains records.
- To "buy into" the position of becoming a block creator, you need to own enough coins or tokens to become a validator on a PoS blockchain.
- The owners offer their coins as collateral—called staking—for the chance to validate blocks and earn rewards.
- Validators are selected randomly to confirm transactions and validate block information.

Proof of Stake (PoS)

- Proof-of-stake is designed to reduce network congestion and address environmental sustainability concerns surrounding the proof-of-work (PoW) protocol.
- In PoW, miners earn bitcoin by verifying transactions and blocks. However, they pay their operating expenses, such as electricity and rent, with fiat currency.
- So what's really happening is that miners exchange energy for cryptocurrency, which causes PoW mining to use as much energy as some small countries.
- The PoS mechanism seeks to solve these problems by effectively substituting staking for computational power, whereby the network randomizes an individual's mining ability.
- This means there should be a drastic reduction in energy consumption since miners can no longer rely on massive farms of single-purpose hardware to gain an advantage.

Bitcoin

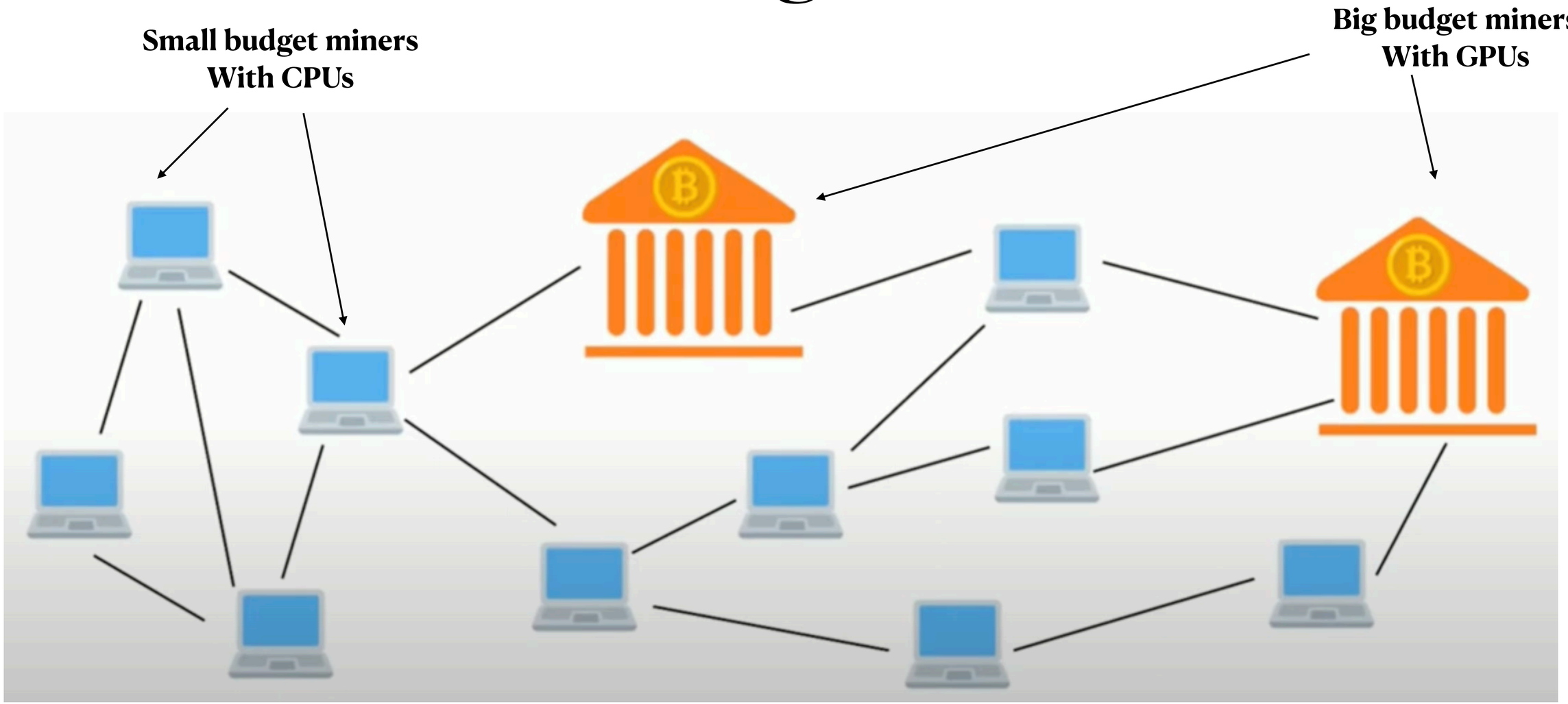
- Cryptocurrency based on Blockchain technology
- Founded by Satoshi Nakamoto in 2008
- There is a central authority for every country that determines how much amount of money will be floated in the system so that there is a balance between supply and demand
- Two principles given by Satoshi Nakamoto: **The Halving** and **Block Frequency**
- **The Halving:** After every four years or after every 210000 block is added, whichever is earlier, the new bitcoins introduced in the system in terms of rewards to miners will be halved. Ultimately, it will reach 0.
- **Block Frequency:** This states that on an average, it will take 10 minutes to create a new block. Visit https://www.blockchain.com/explorer

The Halving

- This process is expected till 2140 because there is a limit on the supply of Bitcoin - 21 million. This means a maximum of 21 million bitcoins can be produced. This makes the bitcoin currency rare - like gold, which can't be made at home. All this is automatically handled by bitcoin protocol.
- If supply of money is increased too much, the value of currency is decreased.
- After 2140, miners will be getting the transaction fee from users since the users will be too much by then.

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

Mining Pool

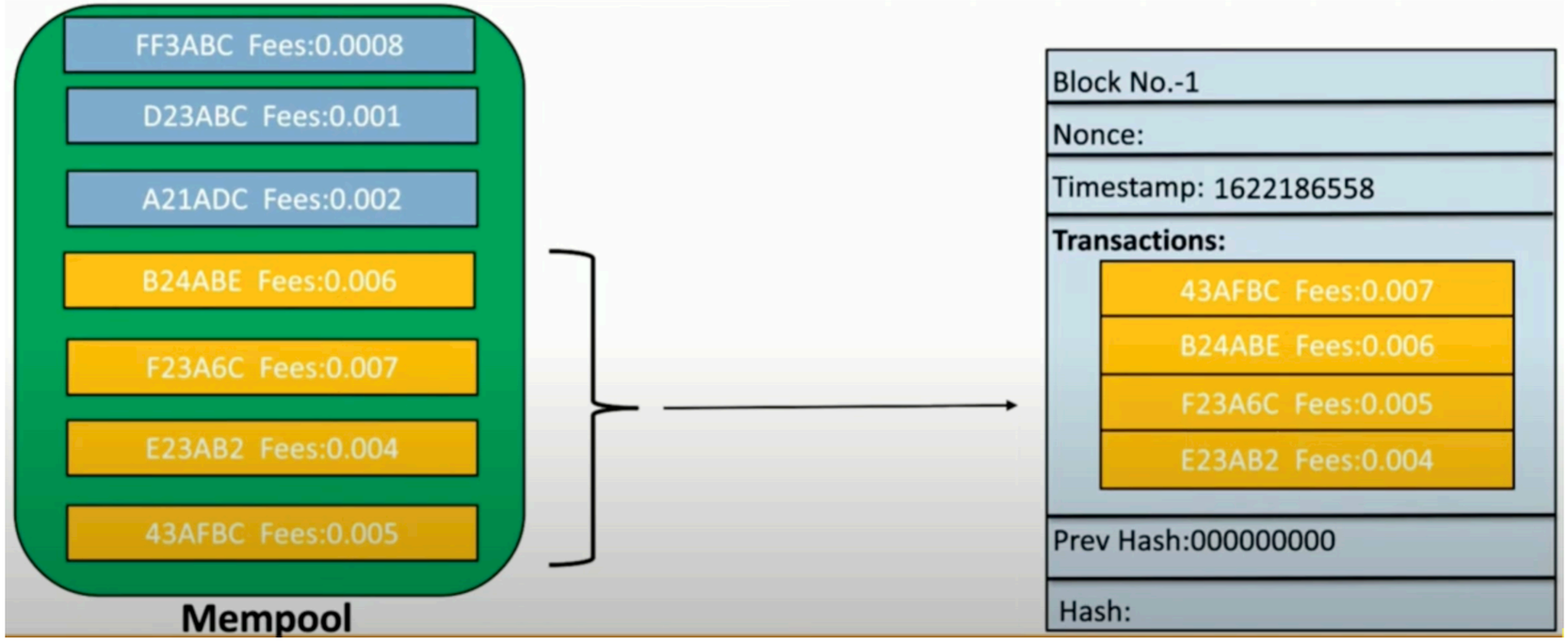


- Small budget miners are at a disadvantage if there are big budget miners with expensie technologies since big budget miners have more hashing power and therefore can reach the target hash earlier.

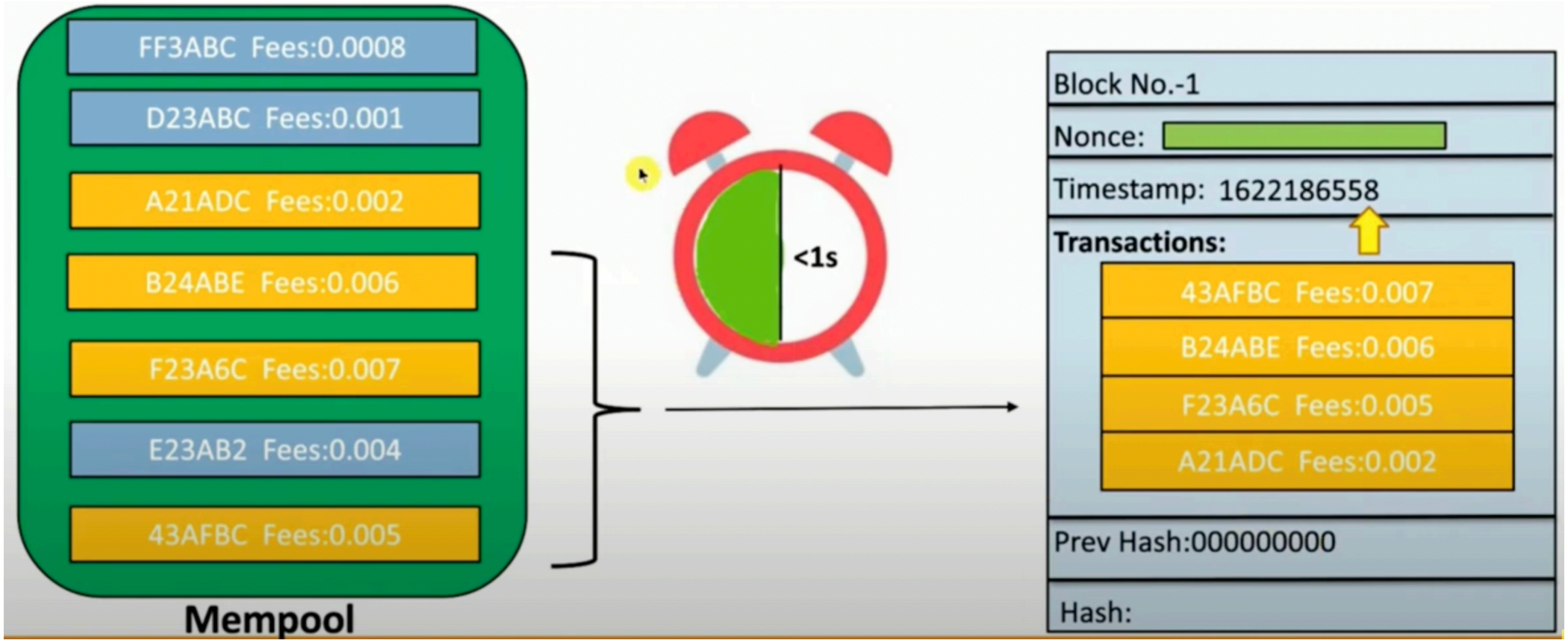
- Small budget miners therefore create mining pools to combine their hashing power and share profits as per their hashing power. Then they can compete with big miners.
- Becoming a part of a large mining pool may provide more hashing power but may lead to less rewards.

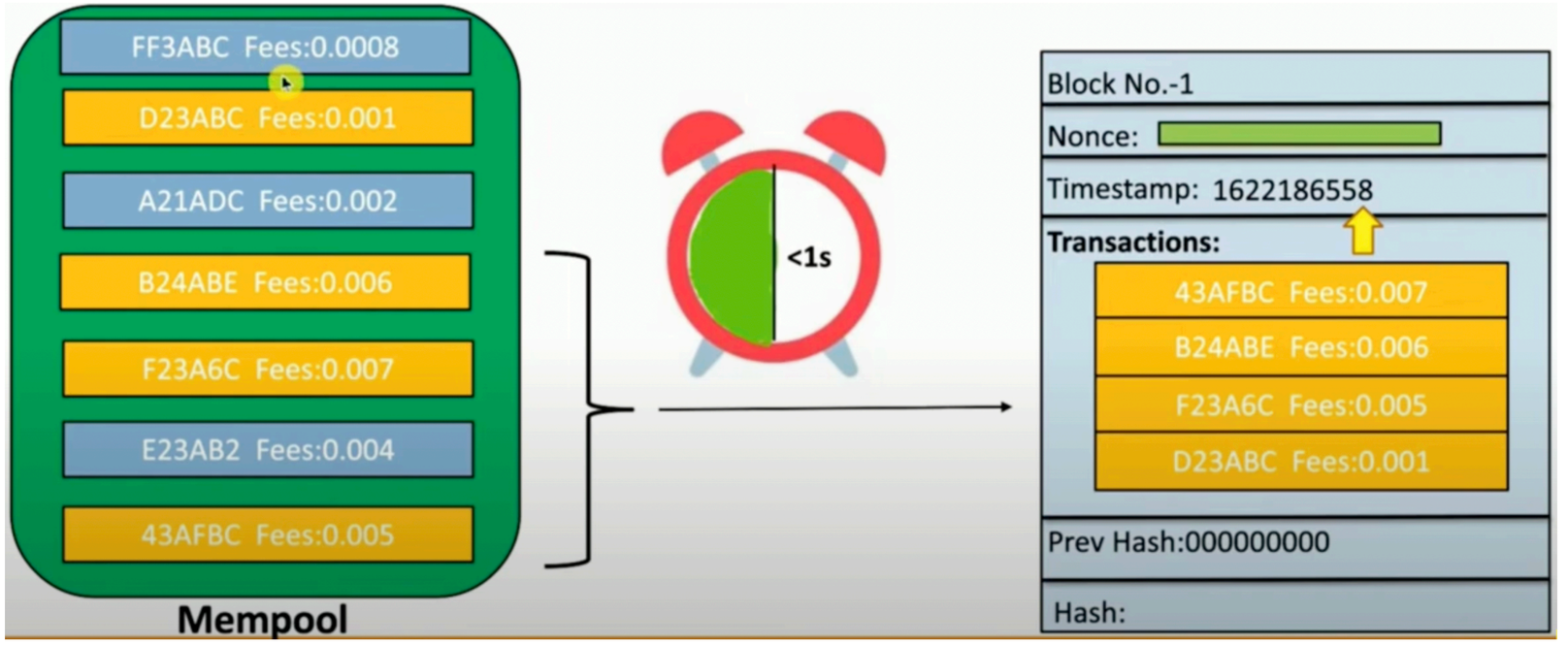
MemPool

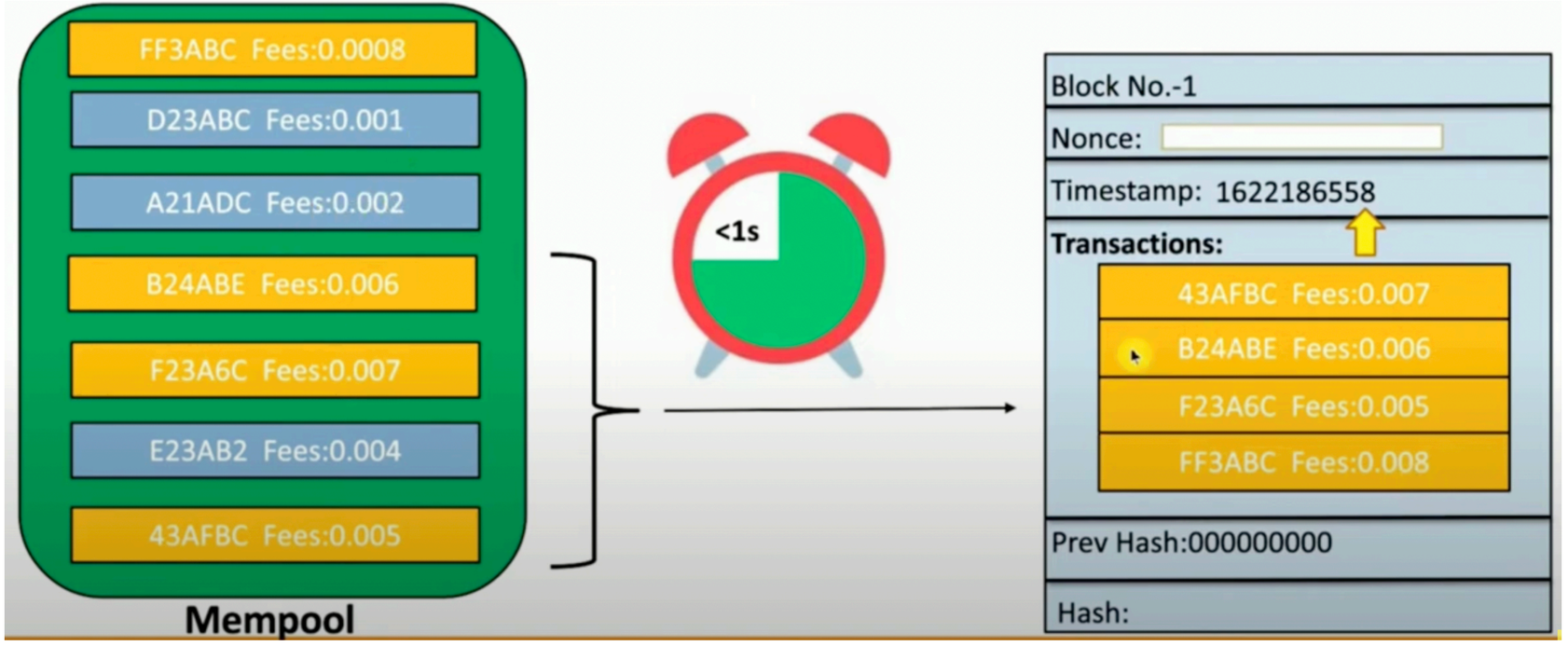
- Area of memory which consists of thousands of unconfirmed transactions. Transactions are temporarily stored there before they are assigned to a block.
- A transaction fee is associated with each transaction that are given to miners if they succeed in generating target hash.
- Let's say four transactions are allowed to be placed in a block.



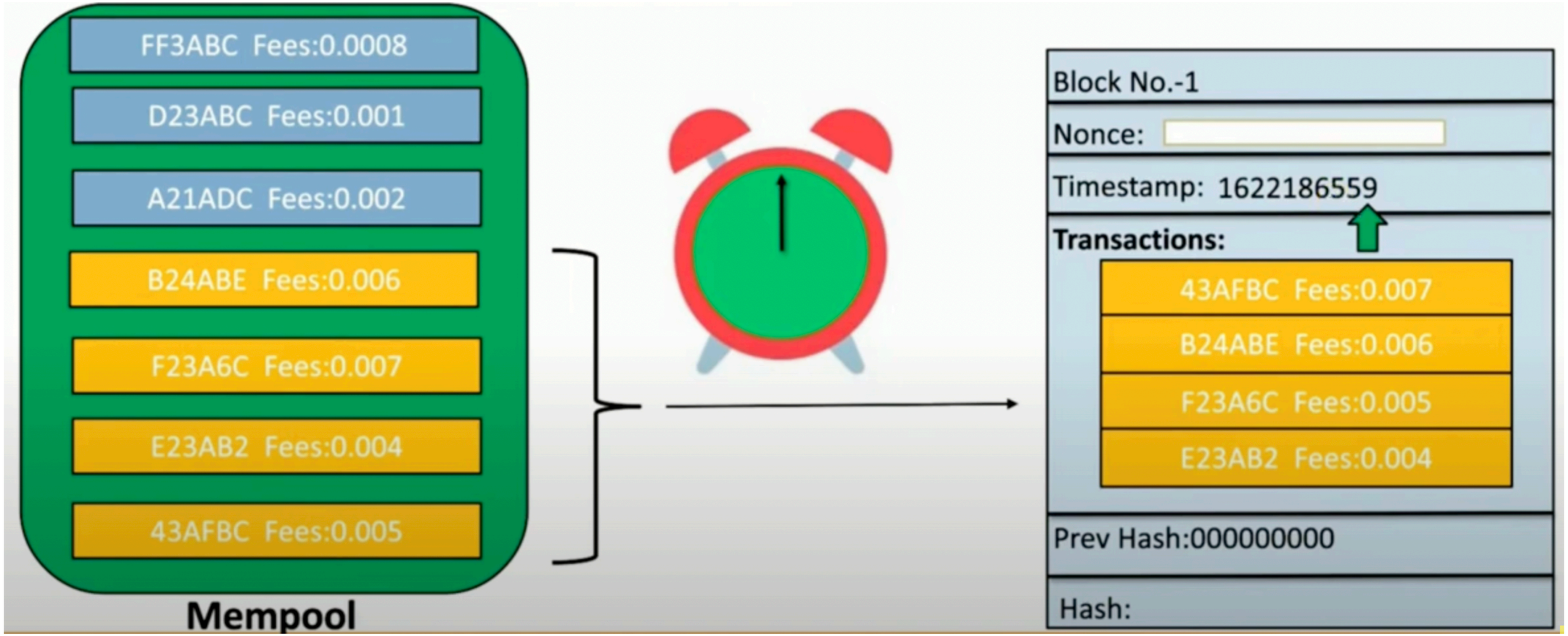
- What do miners do when all nonce are exhausted and timestamp has not been changed?
- Miners replace the least fee transaction with another one from the Mempool. This changes hash significantly because of Avalanche effect.
- Then all values of nonce are tried again to generate target hash.




FF3ABC Fees:0.0008
D23ABC Fees:0.001
A21ADC Fees:0.002
B24ABE Fees:0.006
F23A6C Fees:0.007
E23AB2 Fees:0.004
43AFBC Fees:0.005
Mempool
<1s
Block No.-1
Nonce:
Timestamp: 1622186558
Transactions:
43AFBC Fees:0.007
B24ABE Fees:0.006
F23A6C Fees:0.005
D23ABC Fees:0.001
Prev Hash:000000000
Hash:

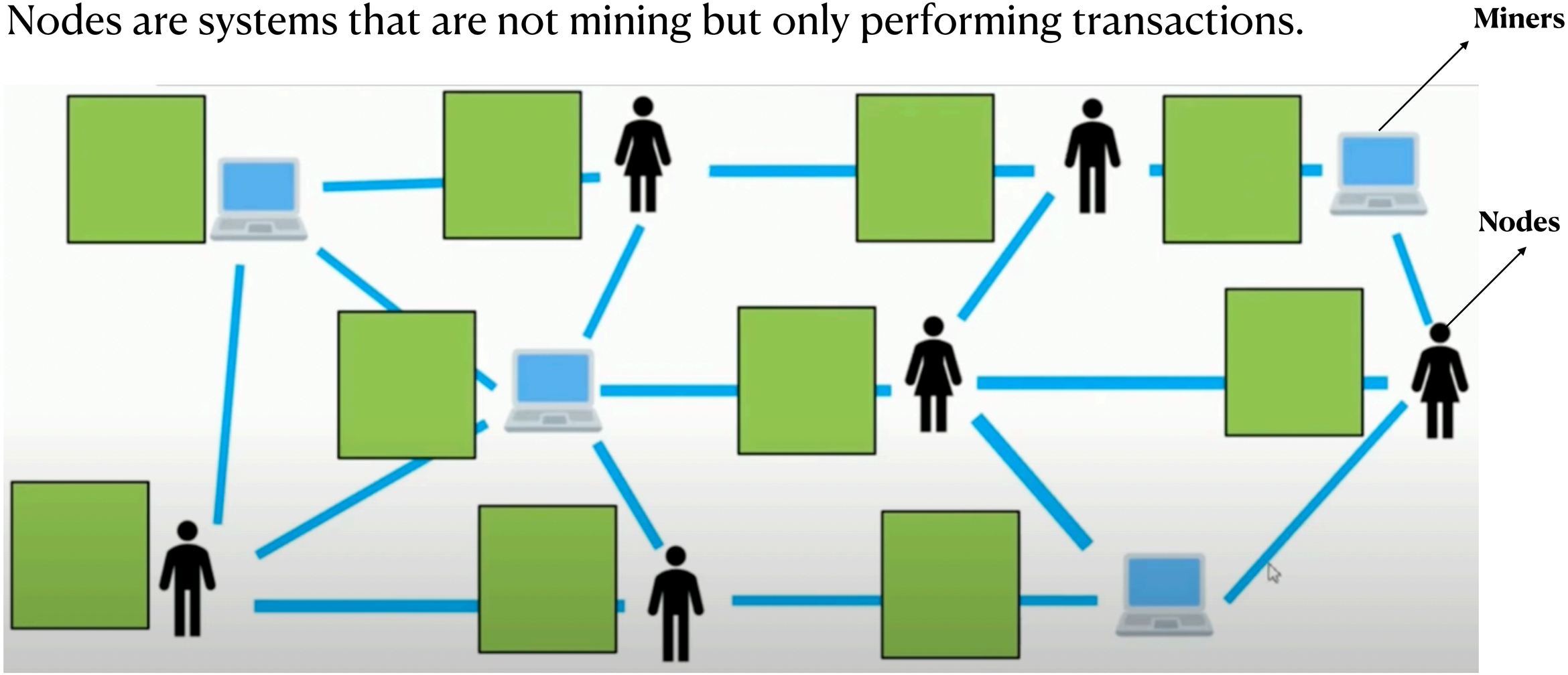

FF3ABC Fees:0.0008
D23ABC Fees:0.001
A21ADC Fees:0.002
B24ABE Fees:0.006
F23A6C Fees:0.007
E23AB2 Fees:0.004
43AFBC Fees:0.005
Mempool
<1s
Block No.-1
Nonce:
Timestamp: 1622186558
Transactions:
43AFBC Fees:0.007
B24ABE Fees:0.006
F23A6C Fees:0.005
FF3ABC Fees:0.008
Prev Hash:000000000
Hash:

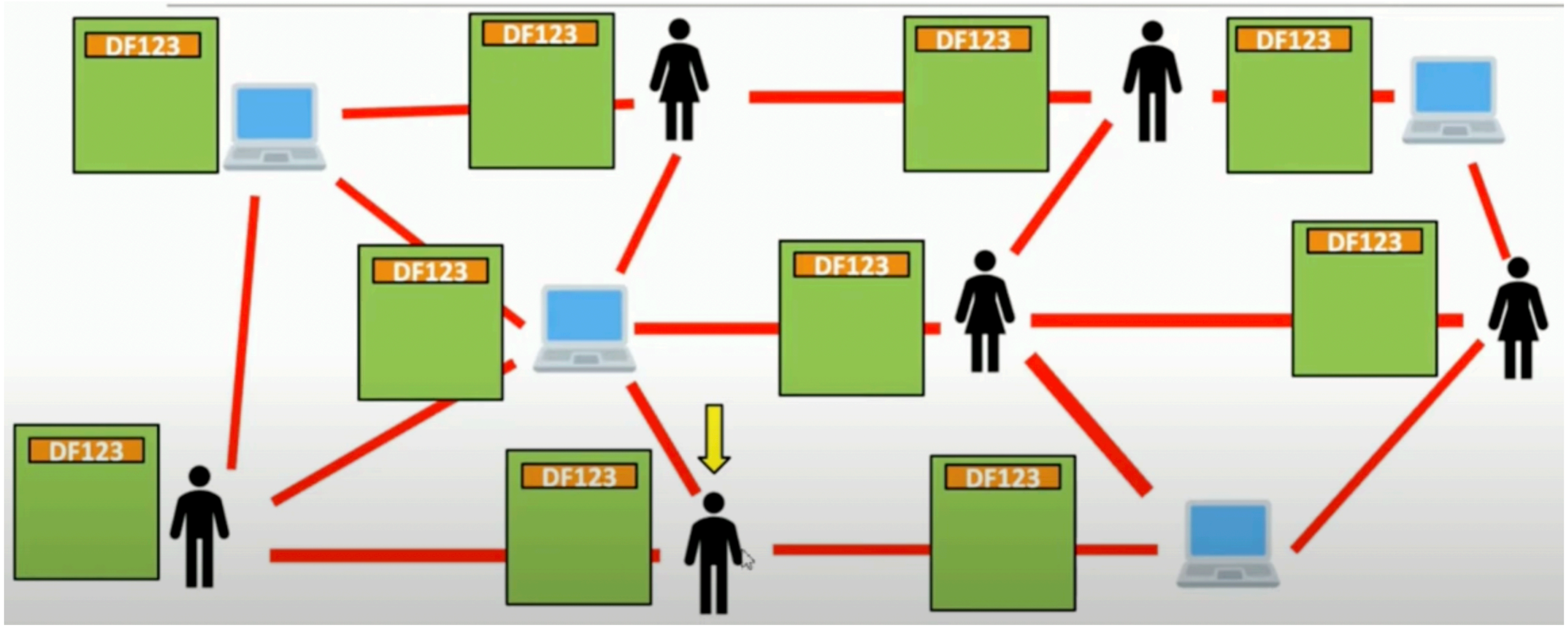
- At last, if still none are exhausted but target hash is not reached, the timestamp is updated and the nonce generation starts again.
- Now the higher fee transaction can again be checked.
- Low fee transactions may never be picked up and will be removed after 72 hours.



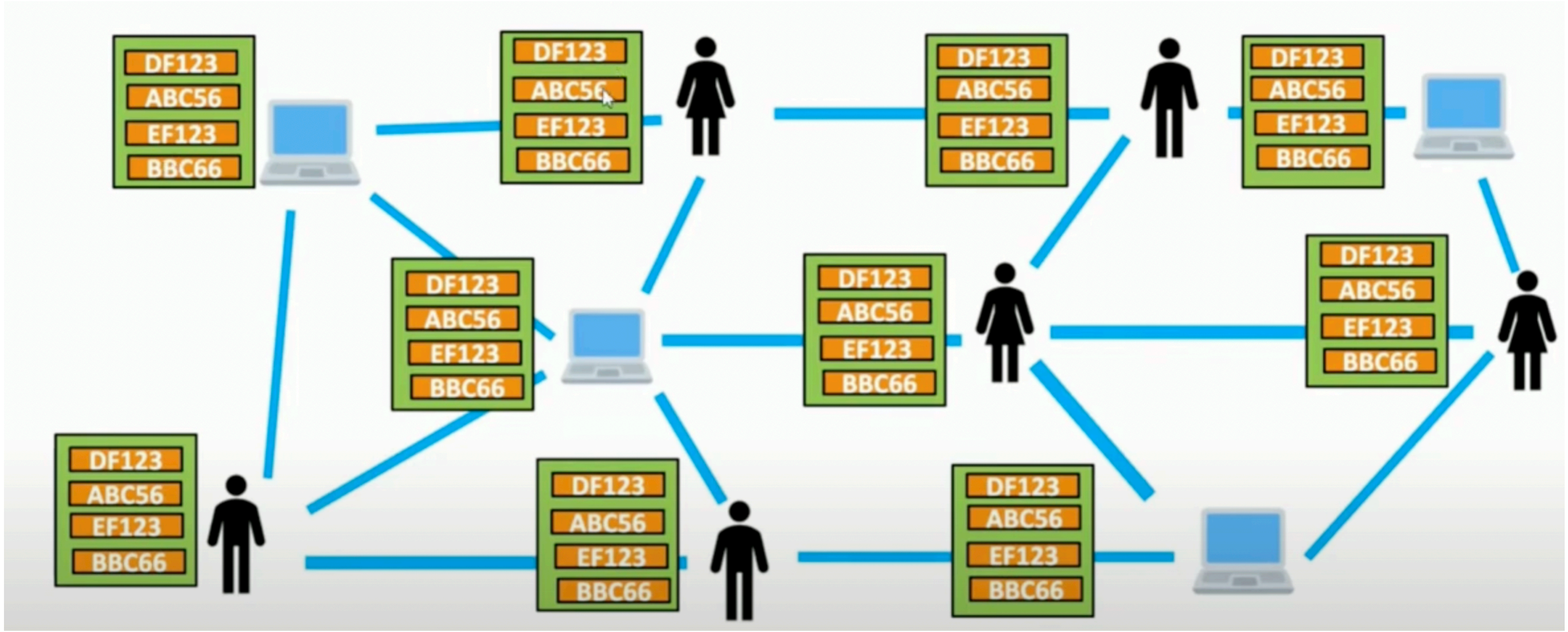
How does Mempool works?

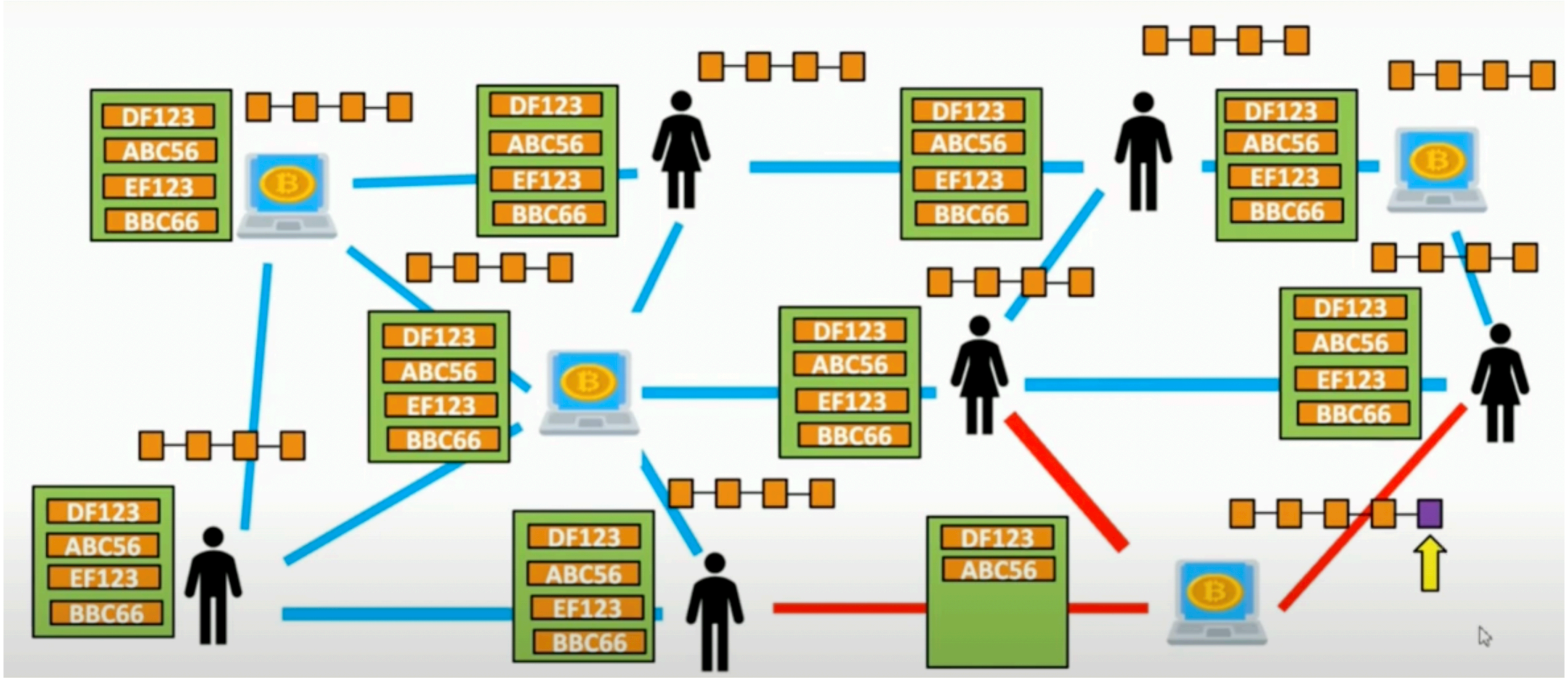
- **Mempool** is not a centralized area. It is associated with all the nodes and miners. Nodes are systems that are not mining but only performing transactions.



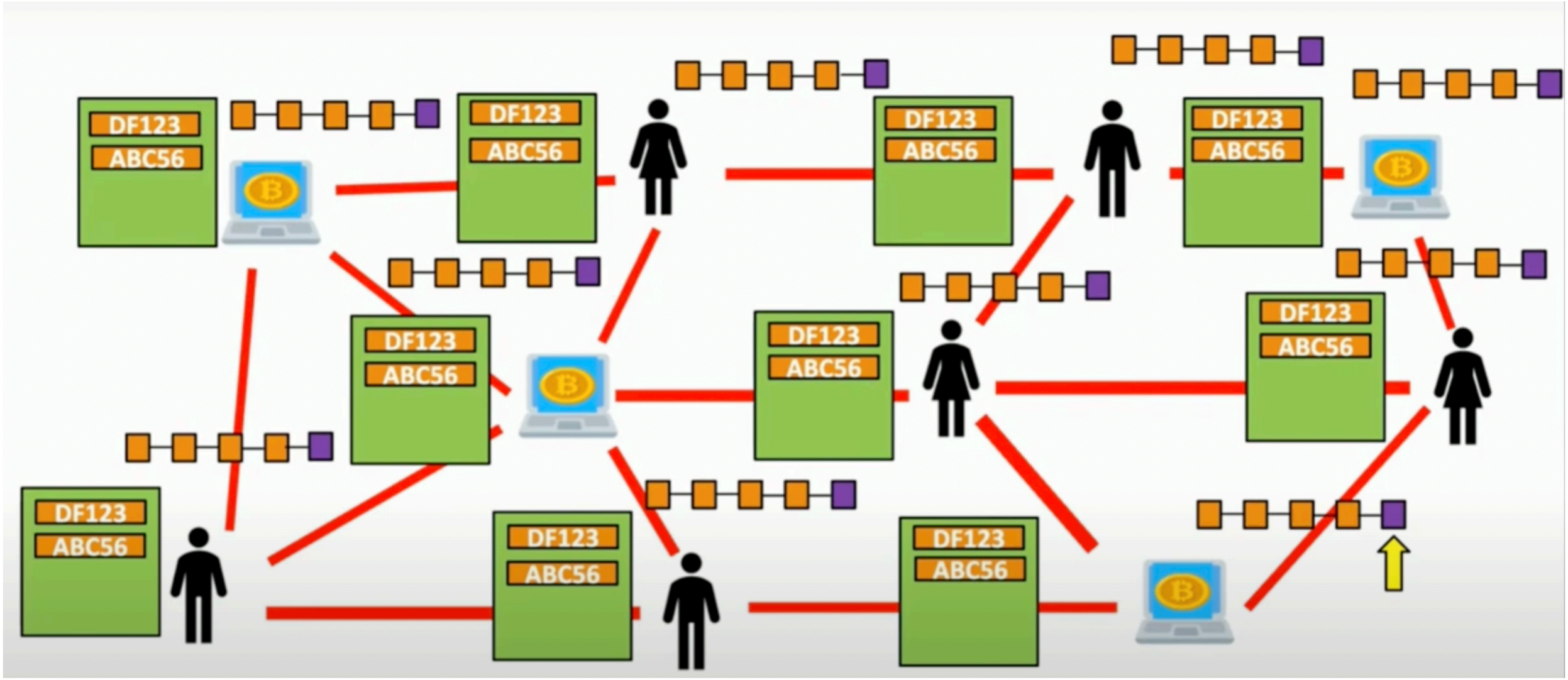


Other Systems are informed of the Transaction done by this Node


DF123
ABC56
EF123
BBC66



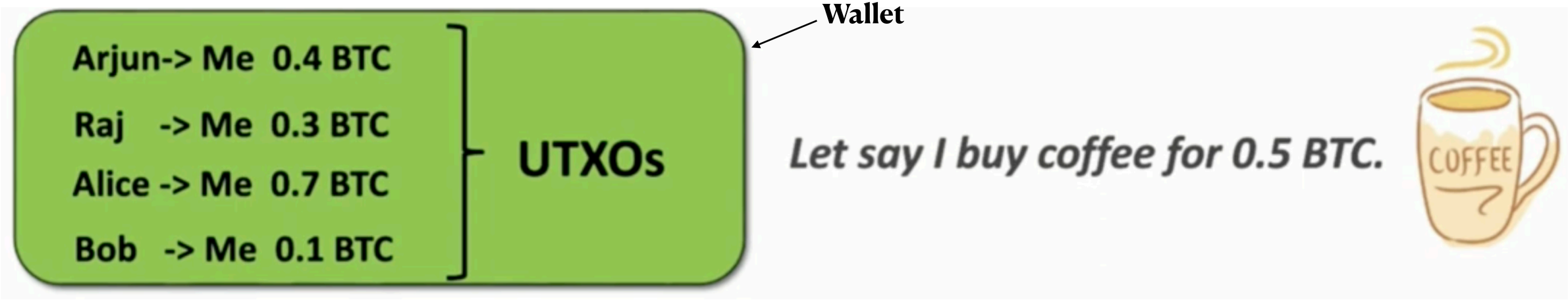
Let this miner mines a particular block using the last two transactions and inform its neighbors.

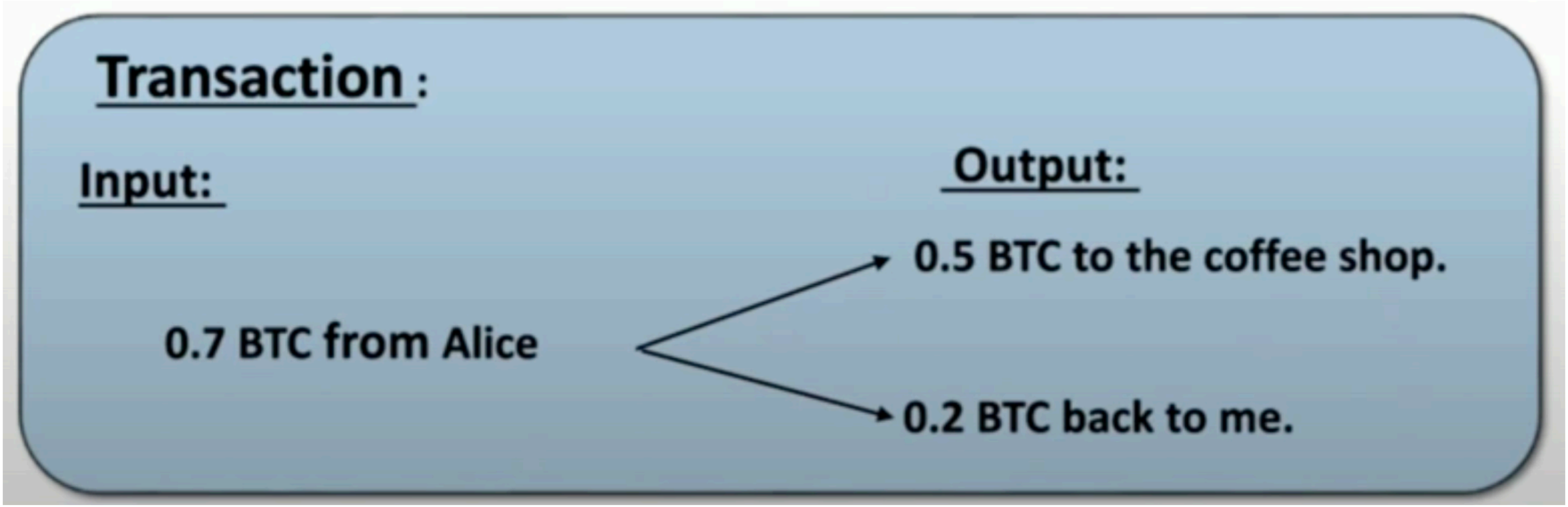


After verification, all the other Systems also add the block to their Blockchain.

Transaction

- For transfer of cryptocurrency, **wallet** is created. For ex- Google Pay is used for transfer of digital money.
- **Unspent Transaction Output (UTXO)** refers to a transaction output that can be used as input in a new transaction.
- In Banking Sector, all the transaction amounts are added and stored. When spent, the amount is subtracted from the stored value.
- However, in cryptocurrency, the ledgers are immutable. Hence the data cannot be modified. So find a transaction where amount is greater than or equal to the amount to be spent.





- Everything is recorded as new transactions in the Blockchain and reflected in the wallet.
- If some money is spent by an NGO, we would be able to see where that money go.

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

~~Alice -> Me 0.7 BTC~~

Bob -> Me 0.1 BTC

UTXOs

Let say I buy coffee for 0.5 BTC.

Transaction :

Input:

0.7 BTC from Alice

Output:

0.5 BTC to the coffee shop.

0.2 BTC back to me.

UTXO for the coffee shop.

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Bob -> Me 0.1 BTC

Me -> Me 0.2 BTC

UTXOs

~~Arjun-> Me 0.4 BTC~~

~~Raj -> Me 0.3 BTC~~

~~Alice -> Me 0.7 BTC~~

Bob -> Me 0.1 BTC

} UTXOs

Let say I buy Noodles for 1.4 BTC.

Transaction :

Input:

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

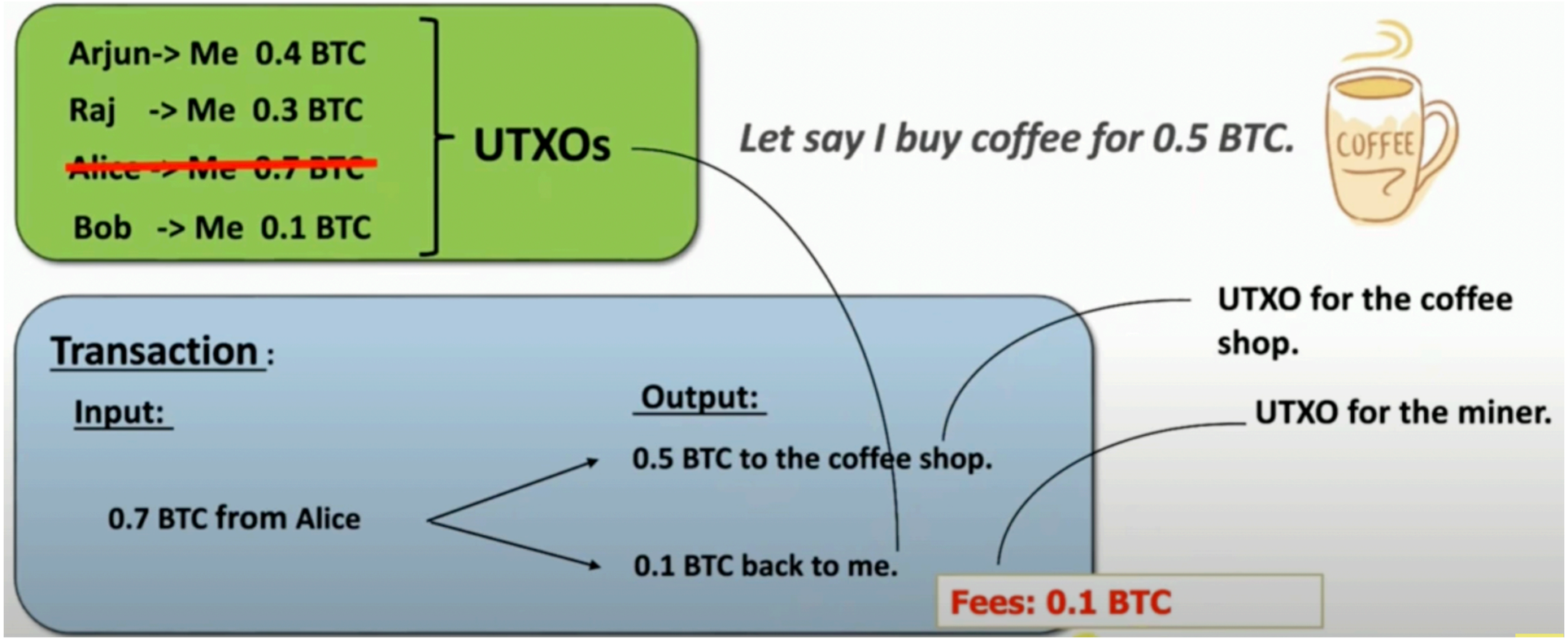
Output:

1.4 BTC to the noodles shop.

UTXO for the noodle shop.

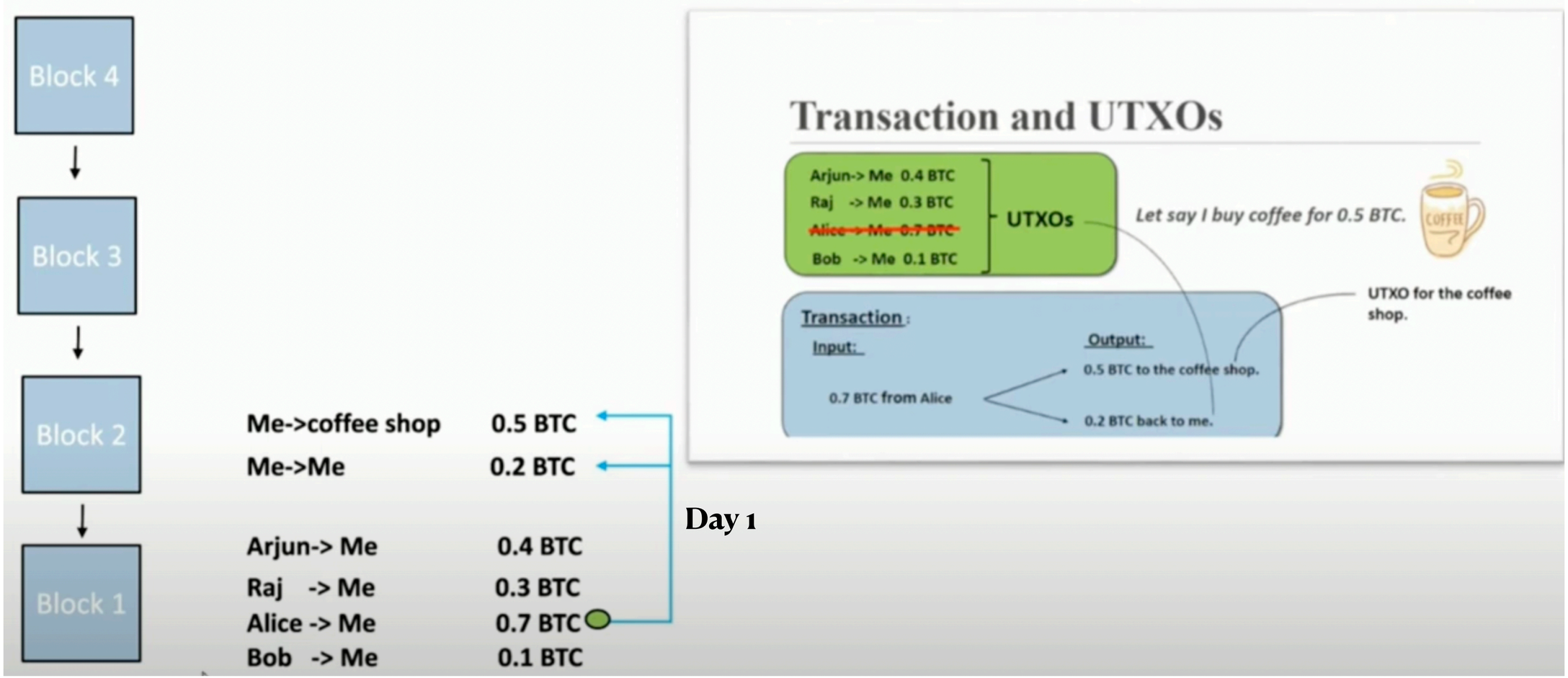
Transaction Fee

- Whenever an unconfirmed transaction is given to a miner from Mempool, a transaction fee is given to the miner after mining a block.
- Transaction Fee is decided by the user.
- The more the fee, higher the chance of the confirmation of the transaction.



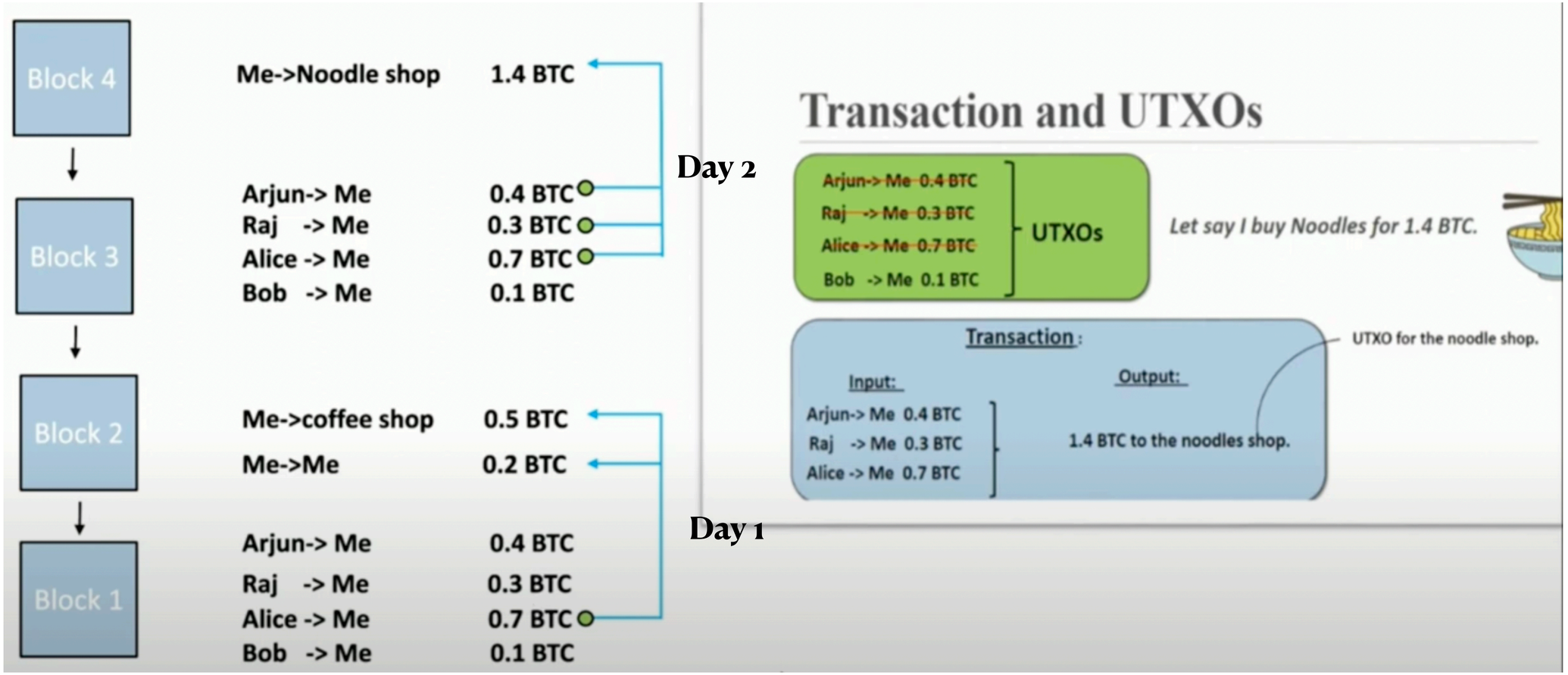
Cryptocurrency Wallets

- Wallet is not a central authority keeping all our data. It computes the remaining balance from Blockchain data.
- In the below diagram, green circle marks used UTXOs.

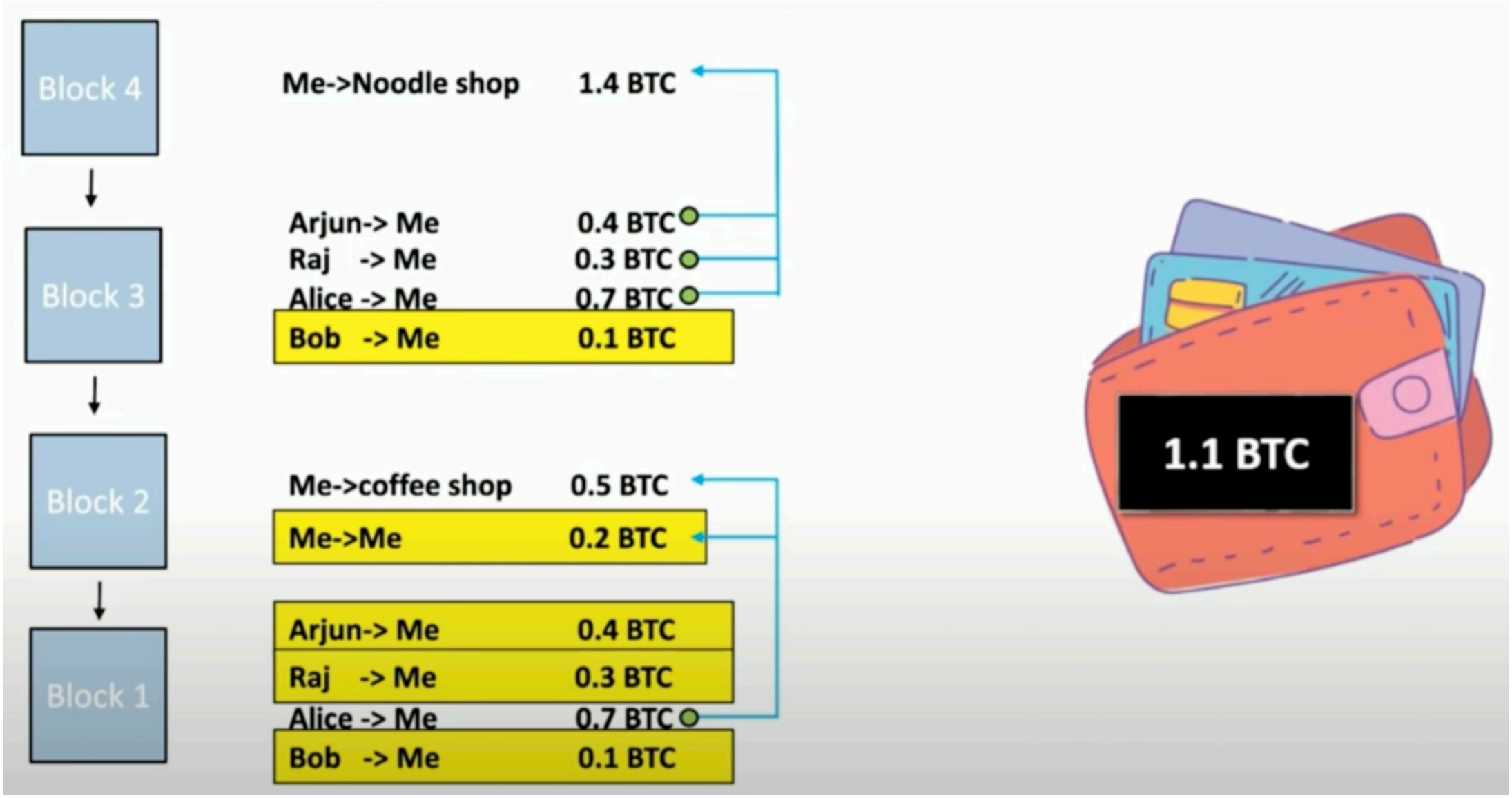


Cryptocurrency Wallets

- How does wallet identify the remaining balance? Add up all the UTXPs which are not used and the destination is me.

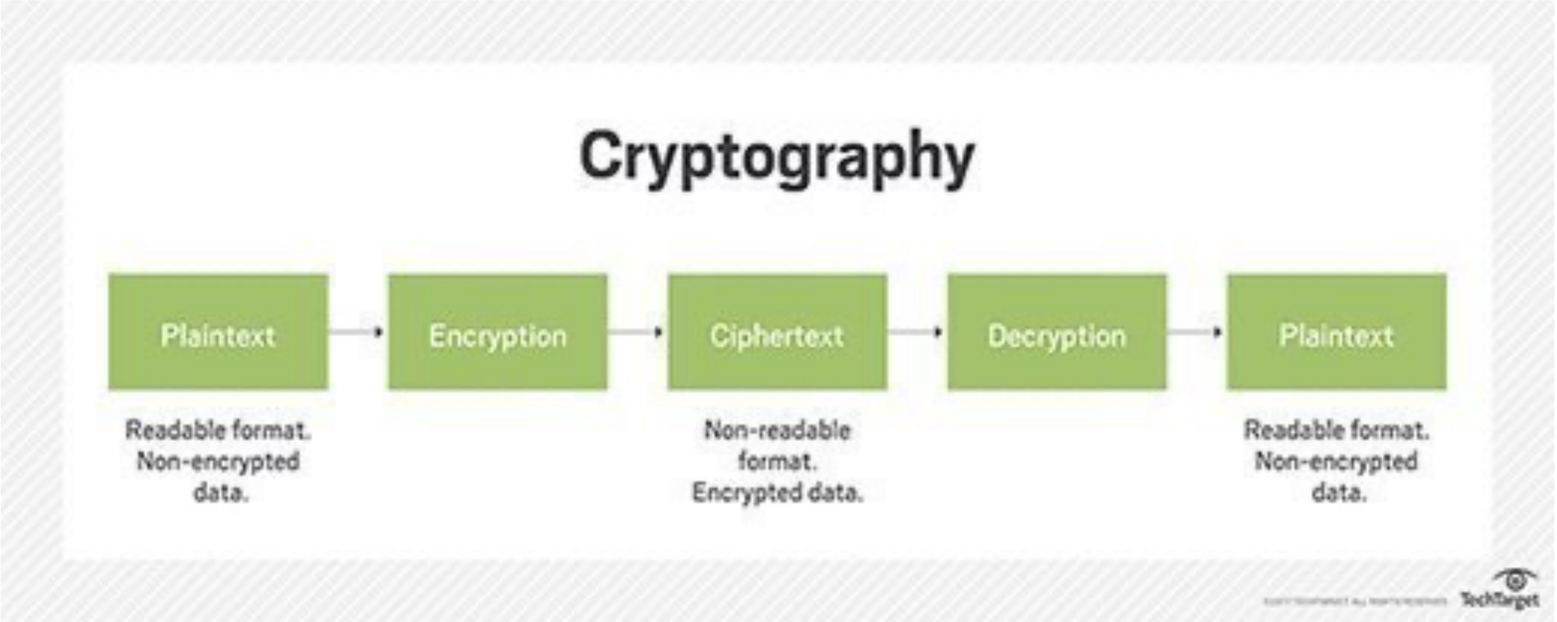


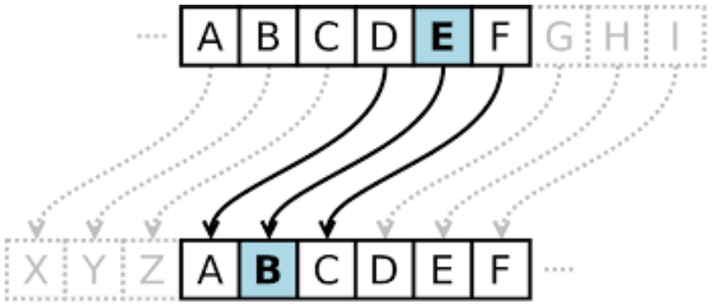
In banks, all the money and transactions are kept and stored with the Bank and then the balance is computed.



Cryptography

- Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.
- The Caesar Cipher, used by Julius Caesar around 58 BC, is a substitution cipher that shifts letters in a message to make it unreadable if intercepted.





Symmetric and Asymmetric

Symmetric ciphers use the same key for both encryption and decryption. Key = 3 in Ceasar Cipher.

- **Encryption: C= E(K,P)** where C is the ciphertext, E is the encryption function, K is the secret key, and P is the plaintext.
- **Decryption: P= D(K,C)** where D is the decryption function.

Asymmetric ciphers use a pair of keys: a public key for encryption and a private key for decryption.

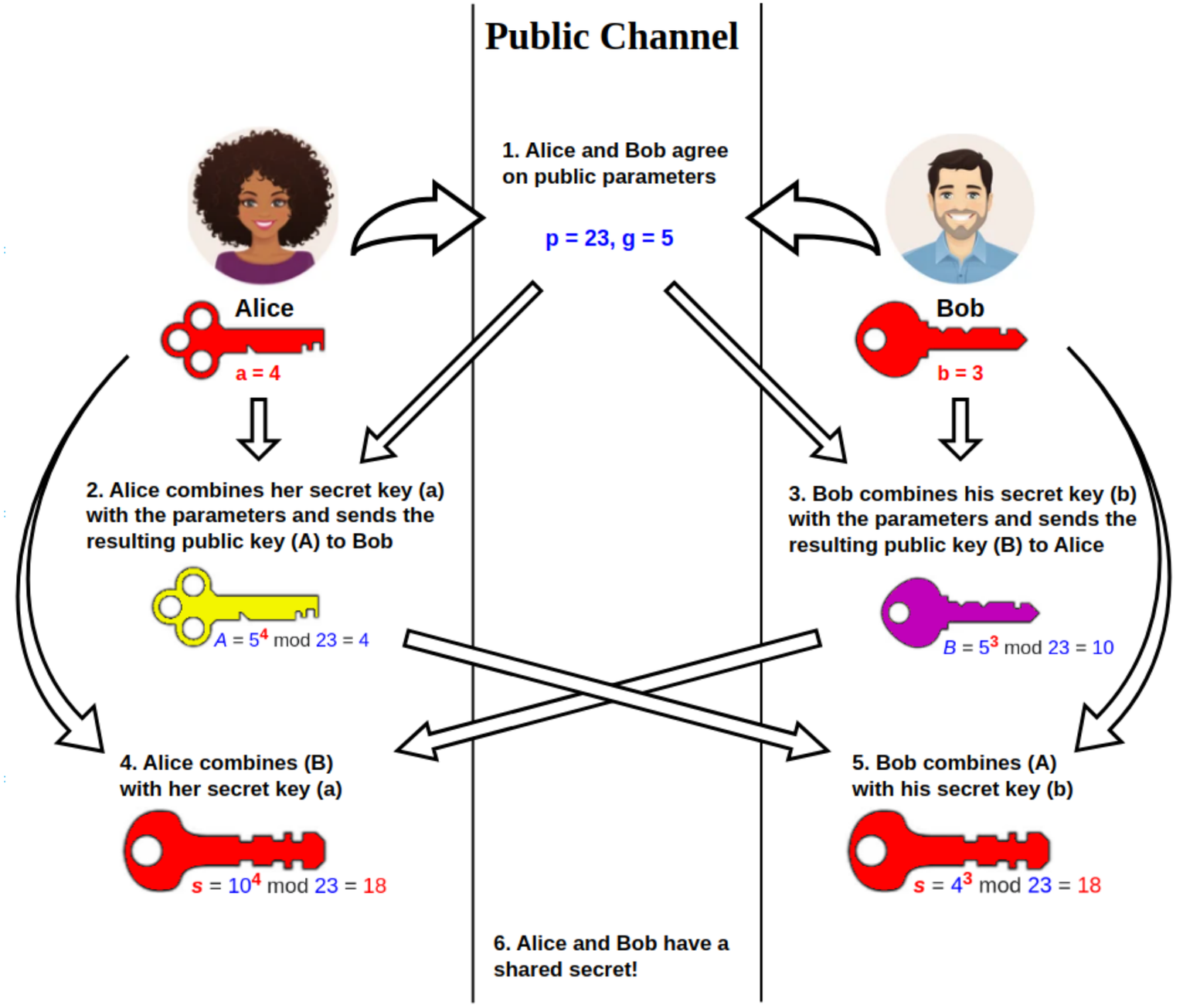
- **Encryption: C= E(PubK,P)** where C is the ciphertext, E is the encryption function, PubK is the Public key, and P is the plaintext.
- **Decryption: P= D(PrivK,C)** where D is the decryption function and PrivK is the private key.

Diffie Hellman Key Exchange

Public and Private Keys

- The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network.
- It is an asymmetric algorithm that makes use of two different keys for encryption and decryption.
- A **public** key is a cryptographic key that can be shared openly and is used to encrypt data or verify a digital signature. Ex- Email id
- A **private** key is a cryptographic key that is kept secret and is used to decrypt data encrypted with the corresponding public key or to create a digital signature. Ex - Email password

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = $x = G^a mod P$	Key generated = $y = G^b mod P$
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key = $k_a = y^a mod P$	Generated Secret Key = $k_b = x^b mod P$
Algebraically, it can be shown that $k_a = k_b$	
Users now have a symmetric secret key to encrypt	


Public Channel
1. Alice and Bob agree on public parameters
p = 23, g = 5
Alice
a = 4
Bob
b = 3
2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob
A = 5^4 mod 23 = 4
3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice
B = 5^3 mod 23 = 10
4. Alice combines (B) with her secret key (a)
s = 10^4 mod 23 = 18
5. Bob combines (A) with his secret key (b)
s = 4^3 mod 23 = 18
6. Alice and Bob have a shared secret!

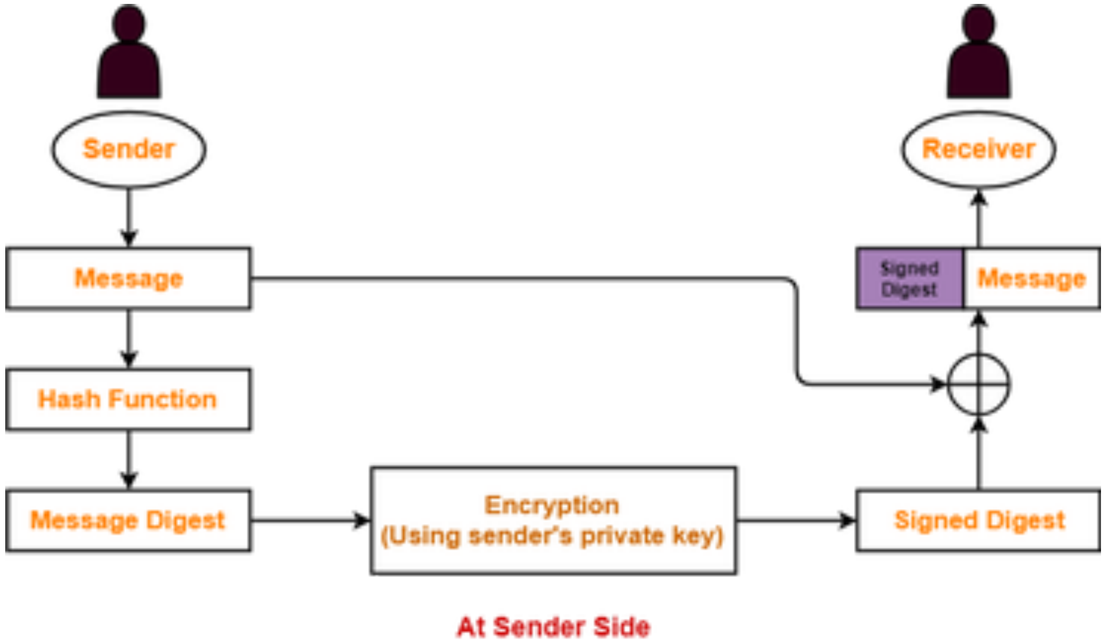
Encryption and Decryption:

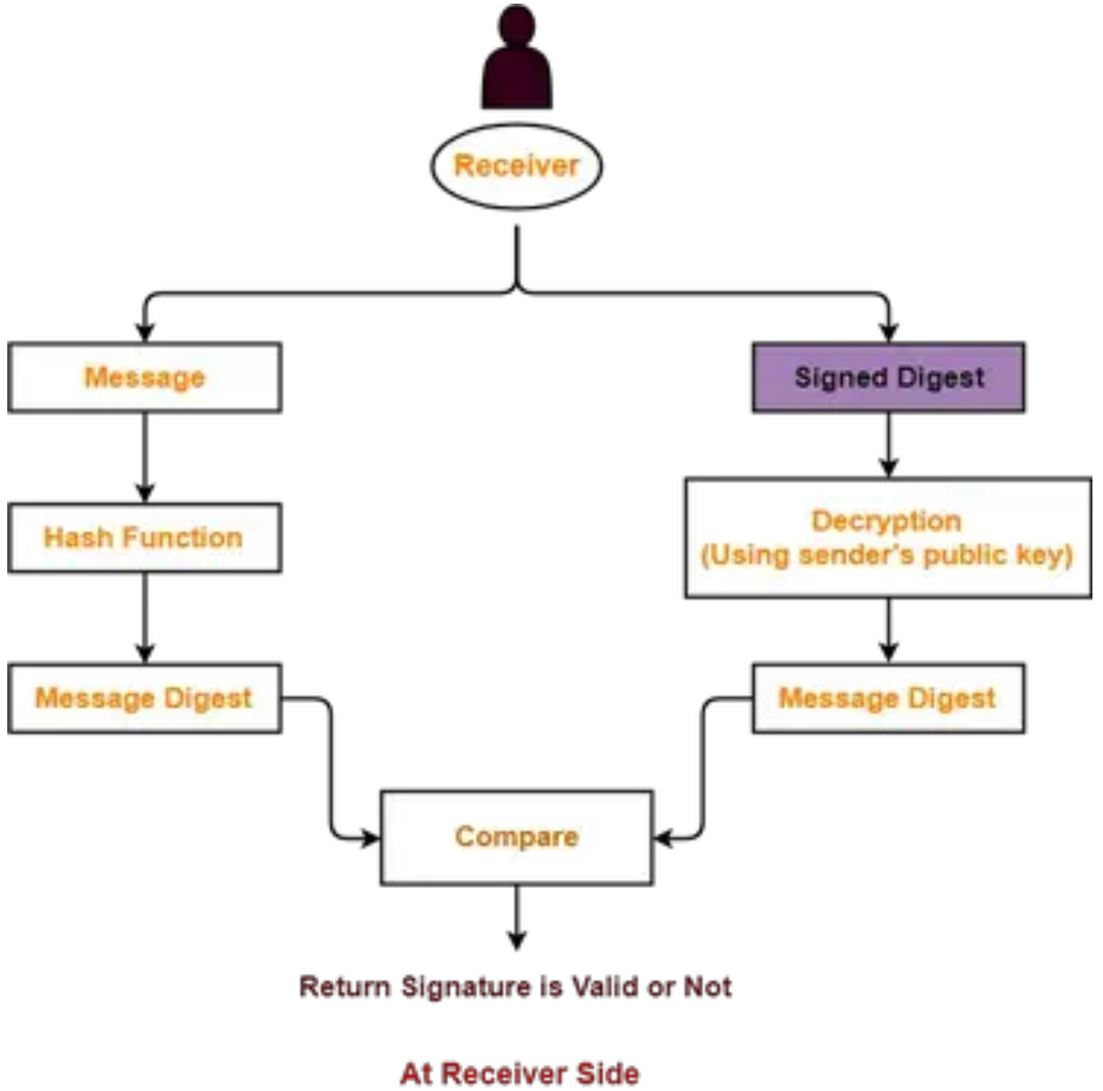
- **Encryption:** A sender encrypts data using the recipient's public key.
- **Decryption:** The recipient decrypts the data using their private key.

Digital Signatures:

- **Signing:** The sender creates a digital signature using their private key.
- **Verification:** The recipient verifies the signature using the sender's public key.

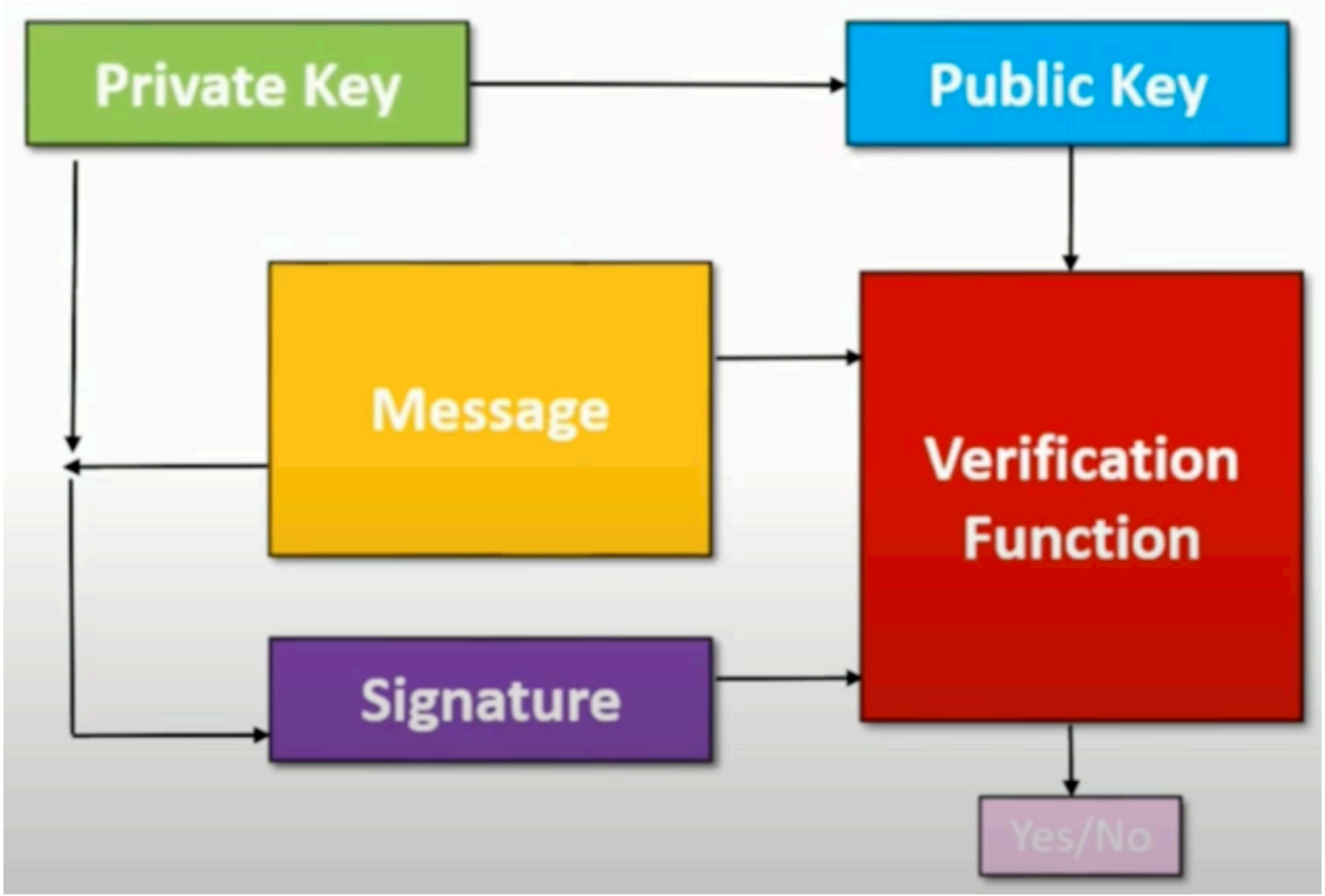
Digital Signature





Cryptography in Blockchain

- Let’s say a hacker writes some false transactions in the Mempool and mines a block. How to verify whether the transactions are legitimate or not?
- A wallet has to be created first with which a private key is provided. The private key should be kept secret with the user.
- A public key is then created using the private key which is openly available to everyone.
- The private key is then used to encrypt the hashed transaction and create a digital signature.
- The transaction data along with the digital signature is then verified using the public key of the user.
- In case the verification fails, the other nodes reject the new block added and the blockchain is recovered.
- Google search tools.superdatascience -> Public and Private keys.

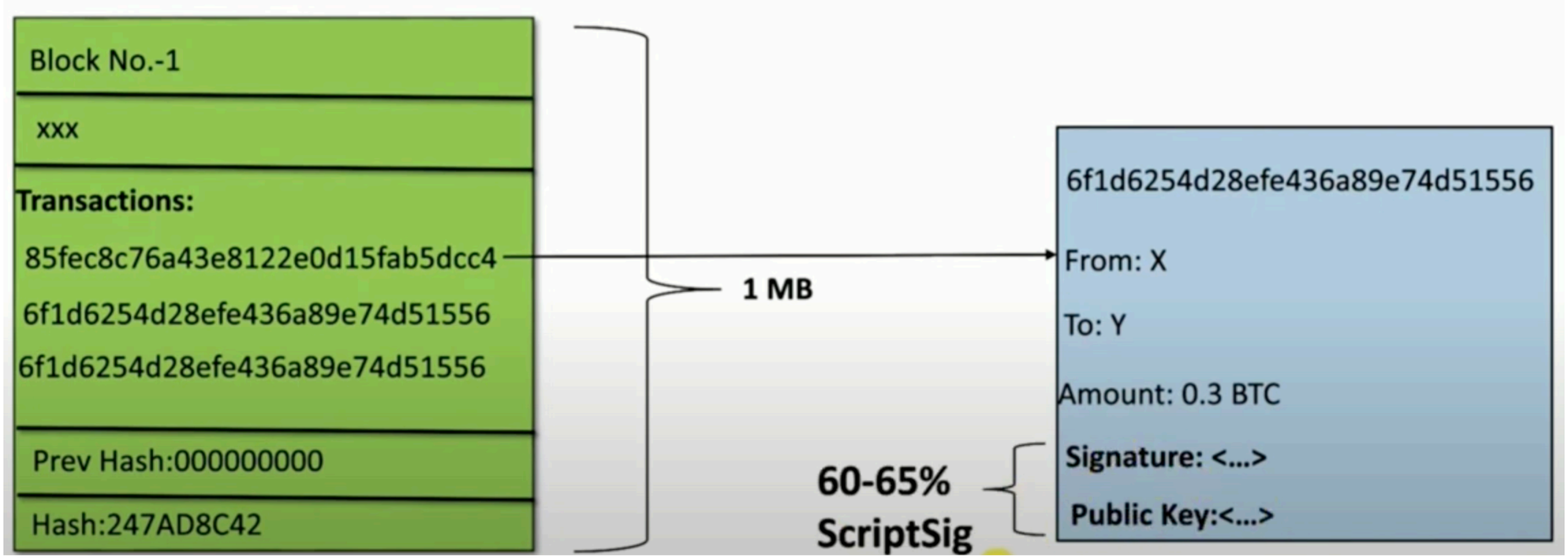

Private Key
Public Key
Message
Verification Function
Signature
Yes/No

Segregated Witness

- Let's say we limit the size of the block to 1 MB. If only 3 transactions were stored in 1MB, then 15 transactions will be stored in a block if we increase the block size to 5MB.
- Miners pick transactions from Mempool and then places them in block after mining. If more transactions are picked at a time, less time will be needed to process the transactions.
- If less transactions in a block, processing time of transactions is more.
- However, a block will larger size will consume more bandwidth on the network when it is propagated to other nodes.
- In bitcoin blockchain, optimal blocksize was 1 MB.

Segregated Witness

- However, after 2017, the users increased significantly and therefore the transactions also increased. 1MB block was not optimal then.
- Whenever a transaction is stored, its digital signature and public key are also stored with it for verification. It consumes most of the space.



Segregated Witness

- The witness of a valid transaction - digital signature and public key (also called ScriptSig) are segregated from the block and sent separately.
- As a result, more transactions can be picked up and placed in the block.
- ScriptSig is the part of a transaction which contains the required signatures and the script which unlocks a UTXO for spending.

Ethereum

- Founded by Vitalik Buterin in 2013
- A Blockchain where programs are run. It is an open-source blockchain based platform.
- It provides ethers (ETH) by which transactions can be made.
- All the systems in the network are called nodes/clients. A node is a computer that runs the Ethereum client software and is connected to other nodes on the network.
- These nodes work together to verify transactions and verify the common blockchain database known as a ledger.
- There are three types of nodes - Full Node, Light Node, Archive Node.

Full Node

- Stores and maintains recent block data (i.e., the last 128 blocks) on disk.
- It serves blockchain data upon request and helps support the network by participating in block validation and by verifying all blocks and states.
- Recommended hardware requirements to run a Full node: A fast CPU with 4+ cores, 16 GB+ of RAM, A fast SSD drive with at least 1 TB of space (storage capacity will grow over time), 25 MBit/s bandwidth

Light Node

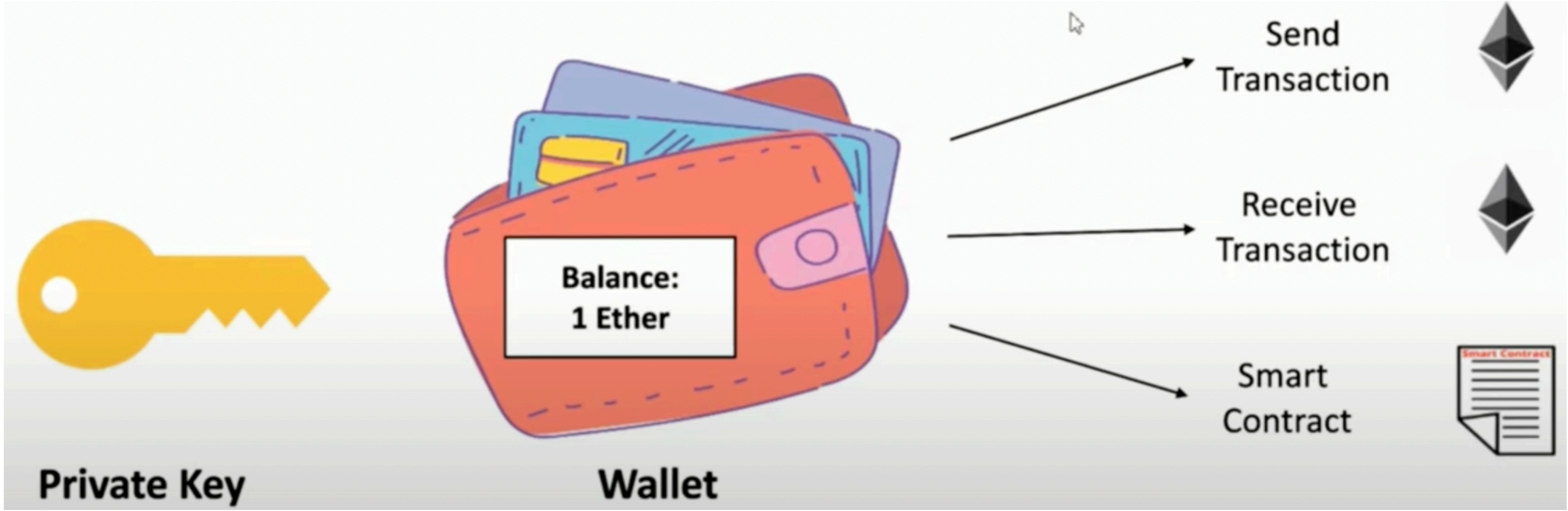
- Do not have high computational resources
- Only perform transactions
- Stores only the block header (index of blocks). Requests Full node for detailed information.
- For low capacity devices which cannot afford to store the gigabytes of data.

Archive Node

- Store everything kept in the full node and build an archive of historical data.
- Requires terabytes if diskspace
- This type of node is useful when querying historical blockchain data that is not accessible on Full nodes.
- For example, you'll want to access an Archive node if you need block data before the last 128 blocks.
- Also, Archive nodes aren't required to participate in block validation.

Ethereum Account

- An Ethereum account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.
- There are two types of accounts - Externally Owned Account (EOA) and Contract Account (CA).
- EOA is created once a wallet is created. A private key is used to access and open the wallet. EOA is used to send and receive transactions and interact with smart contracts.



Ethereum Account

- Smart Contracts are deployed on a block of Ethereum. For that, contract accounts are created.
- When A and B come into a contract, their contract accounts are created. They are provided with a unique address through which they can access the block where the contract is written.
- Contract account is controlled by the code written in the block and no human intervention is needed.
- A wallet is created free of cost (no gas required). However, whenever a contract account is created, some gas cost is needed.
- ETH balance is required to fulfil the contract.

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