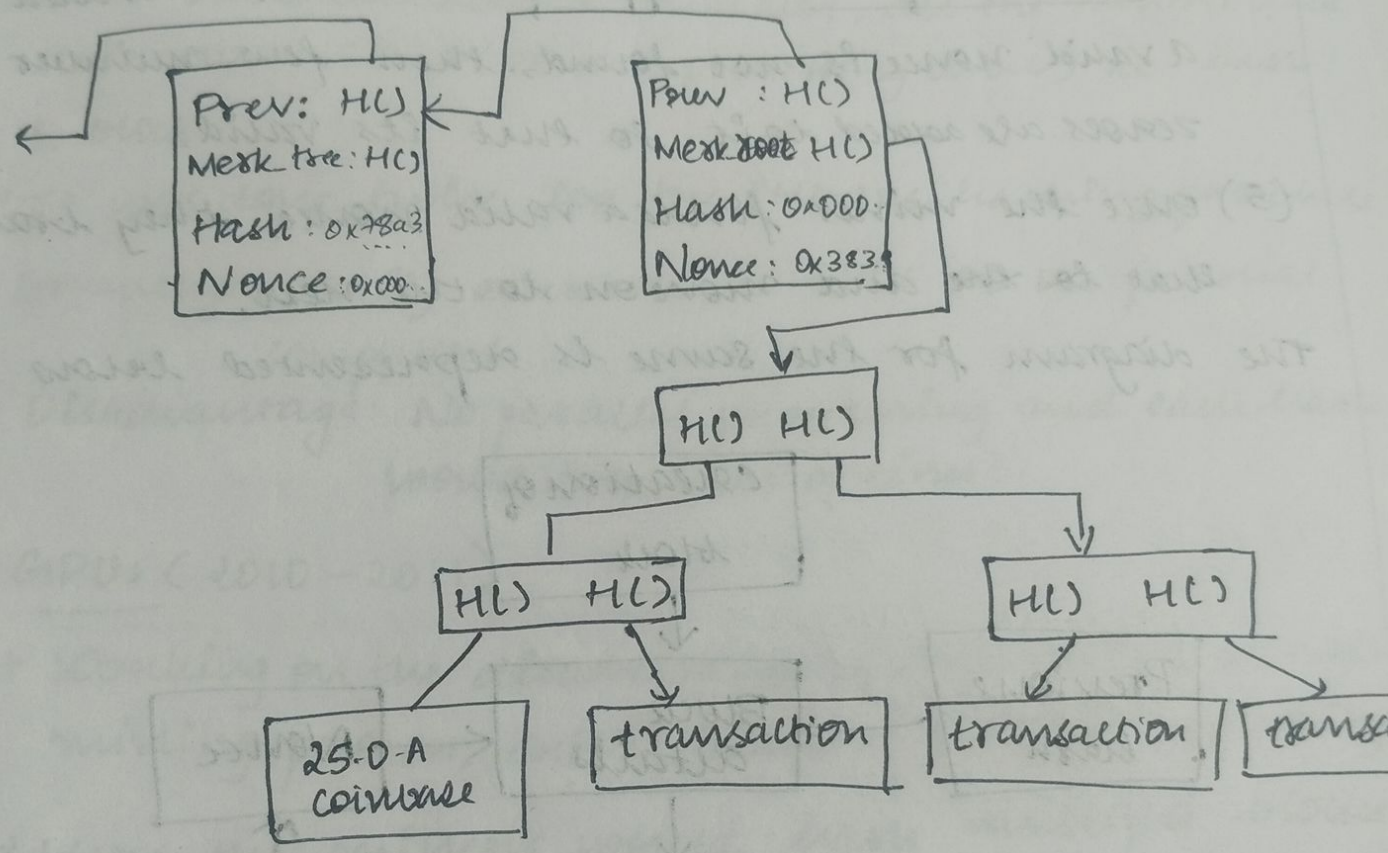
IAT-3

① Bitcoin mining is a process where miners find a valid block cryptographically using a by solving a puzzle. They use a nonce for the same

Nonce: It is a unique ID or number that is incremented each time a Bitcoin is spent or used.



The procedure for finding a valid block using nonce is as follows:

(1) The miner creates a new block that contains

- The previous hash
- The details of all transactions in the form of a merkel tree
- A hash value for the particular block
- A target and - A nonce for the same.

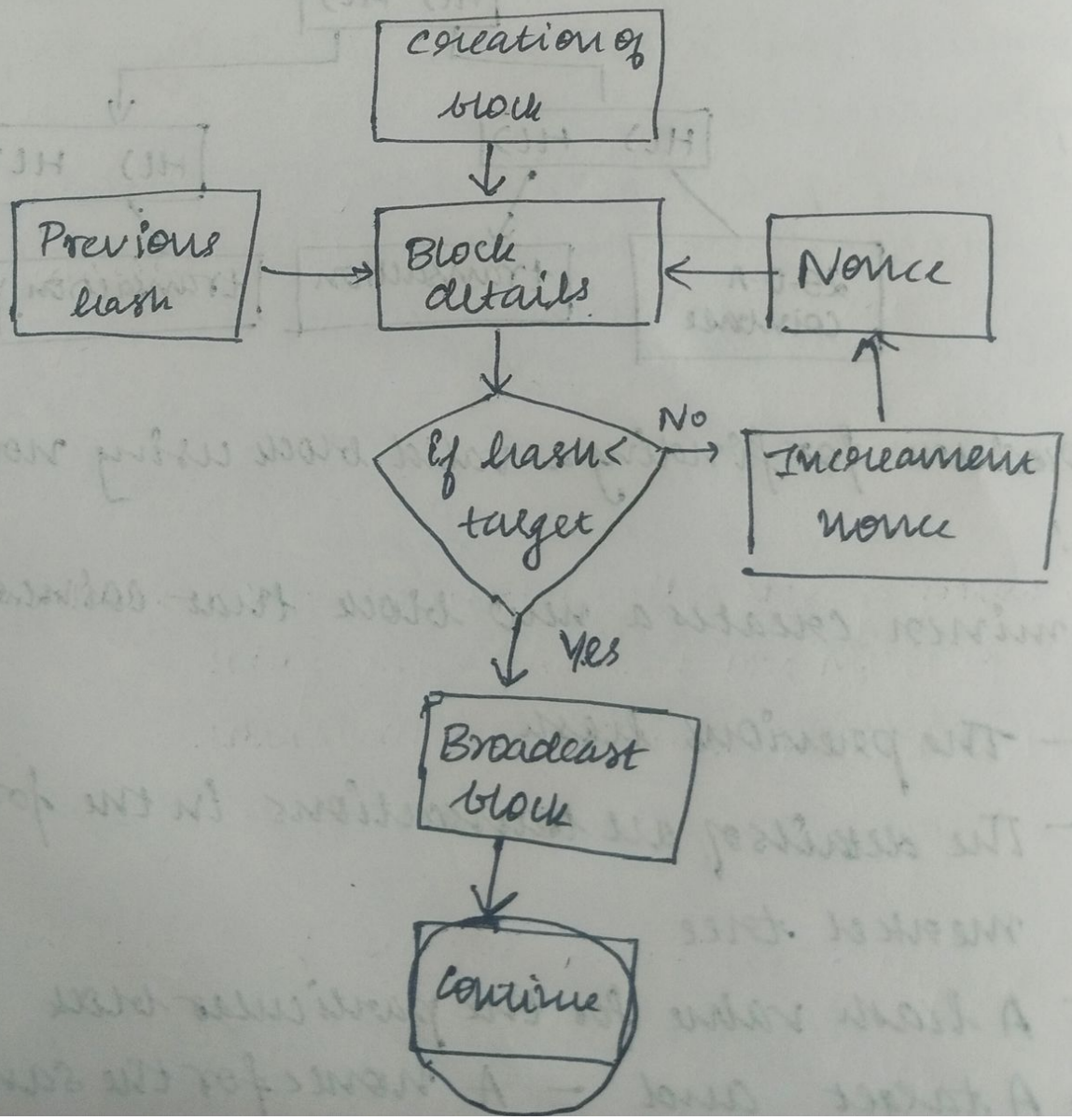
(2) Now, miner checks if the hash value is lesser than the target or not.
If yes, the block is valid, hence else it is not valid.

(3) If it is not valid, the nonce is incremented.

(4) Exhaustion of nonce: suppose if all 2^{32} are searched and a valid nonce is not found, then few number of zeroes are added to it so that its valid.

(5) Once the miner finds a valid nonce, they broadcast that ~~to the~~ and move on to the next.

The diagram for the same is represented below



(2) The evolution of Bitcoin mining from CPU mining till ASIC is a appreciable growth as it concentrates on lesser power consumption and more process take place quickly.

The evolution is as follows:-

(i) CPUs (2009-2010)

→ When Blockchain started initially, all the miners used their own CPU's (central processing unit) to hash a block.

→ It was done twice for the SHA-256 hashing procedure.

→ Advantage: Easily accessable as CPUs are on personal computers.

→ Disadvantage: No parallel processing and each hash would take a lot of time.

(ii) GPUs (2010-2011)

→ Working on the disadvantage of CPUs in the Bitcoin mining process, GPUs allowed parallel processing

→ Here the miners would hash multiple blocks at once, hence increasing their efficiency.

→ Advantage: Due to multiprocessing & parallel processing systems, the tasks of hashing could be done at a faster pace compared to CPU's

→ Disadvantage: There was a huge power consumption when the use of GPUs were employed.

(iii) FPGAs (2011-12)

→ Field Gate Programmable arrays are more advantageous than GPUs.

→ Here more amount of hashing could be done in comparison to GPUs and CPUs.

→ The efficiency had increased tremendously.

→ Advantages: Faster computations compared to GPUs at lower power consumption compared to CPU's & GPU's.

→ Disadvantage: The initial expenditure for FPGAs is extremely high and the maintenance too.

(iv) ASIC: (2013 - present)

→ Systematic Integrate circuits are the present way of Bitcoin mining.

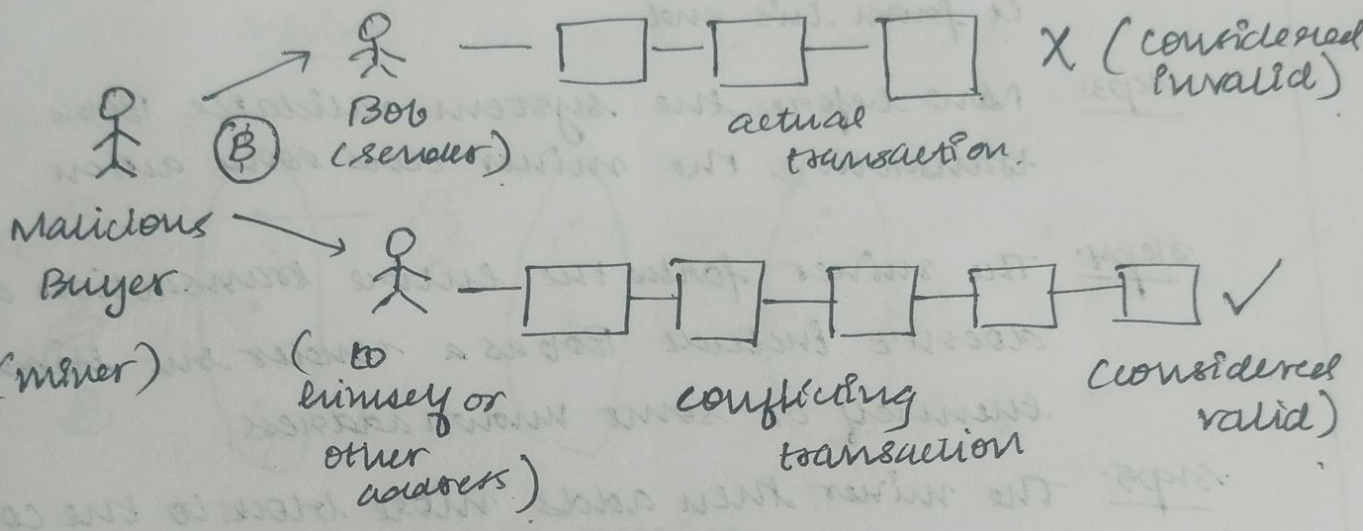
→ It solves on all the disadvantages that were seen so far such as parallel processing, power consumption and expenditure.

→ Advantages: Even countries with cheap power are able to setup ASICs for Bitcoin mining as it uses lowest and can run on minimal power consumption.

→ Disadvantages: If all the ASICs are setup in countries with less expenditure then it will impact the global availability.

(3) The attack name in the above scenario where a malicious miner sends a transaction to Bob and receives some goods or service in exchange for it is called Double spending attack.

Diagram:



Explanation:

→ The attack describes the Double spending attack.

→ Double spending attack occurs when a malicious miner sends someone a cryptocurrency (Bitcoin) to one user in exchange for some goods.

→ Here, the transaction is confirmed by Miner.

→ The malicious miner, then forks the entire transaction that was the original one, and adds more blocks to make it authentic. and spends the same cryptocurrency

→ The system considers the longest transaction as valid and considers the shorter (original) invalid.

→ In the ~~exp~~ example of Bob, the series of events have taken place.

Step1: The miner sends Bob a bitcoin in exchange for some goods or service

Step2: Bob takes the Bitcoin and the miner confirms it from his end.

Step3: Now before the system validates Bob's transaction, the miner does some action.

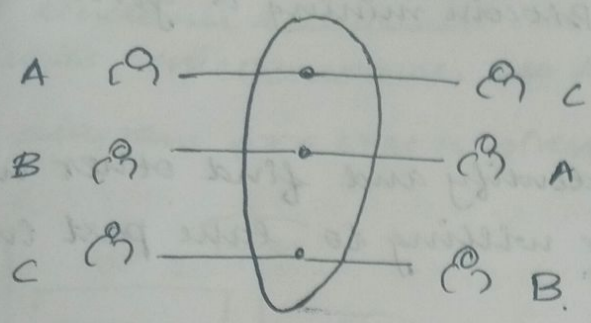
Step4: The miner forks the entire transaction and doesn't include Bob as a sender but ~~himself~~ themself or some known address.

Step5: The miner then adds more blocks to the confir transaction and broadcasts it to the network

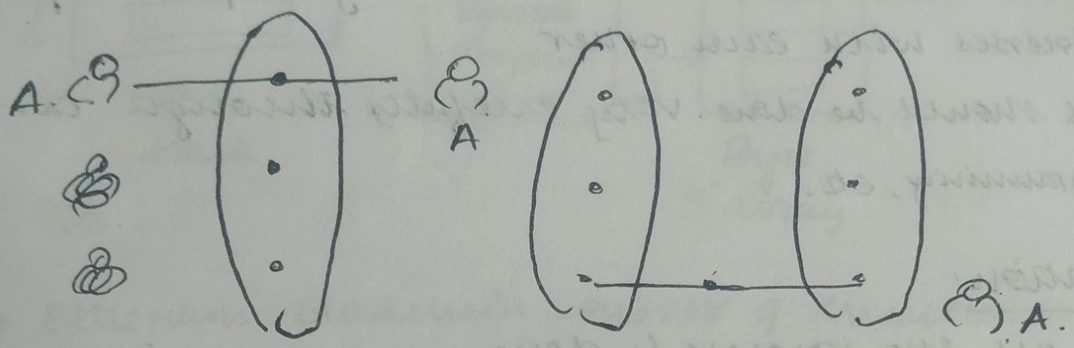
Step6: Finally the system validates the conflicti transaction as it has more no. of blocks and the transaction done to Bob is not counted

Therefore, this attack was a double spending atta

(4)



Mixing.



Multistage mixing

The Mixing process in Bitcoin mining is where a set of users combine all their inputs into a single transaction and their outputs are unpredictable.

The features of mixing are as follows:-

- Decentralized system: mixing in Bitcoin mining is decentralised and doesn't depend on 3rd party servic
- Individual signatures: Each user that takes part in this must validate their signatures individuall
- ~~Either~~ Fees: some mixing procedures charge fees for the same, the concept is either all or little

preserves

The process of mixing in Bitcoin mining is given below:

(i) Find the pool of users:

The users have to identify and find other users that will agree & are willing to take part in this mixing procedures.

(ii) Exchange input/output address:

The various users have to exchange input/output addresses with each other.

This should be done very carefully through car programming, etc.

(iii) validation:

once all the process is done, each user is supposed to validate their output by validating and giving appropriate signatures.

→ Challenges:

There are several challenges the users participating in this might face:-

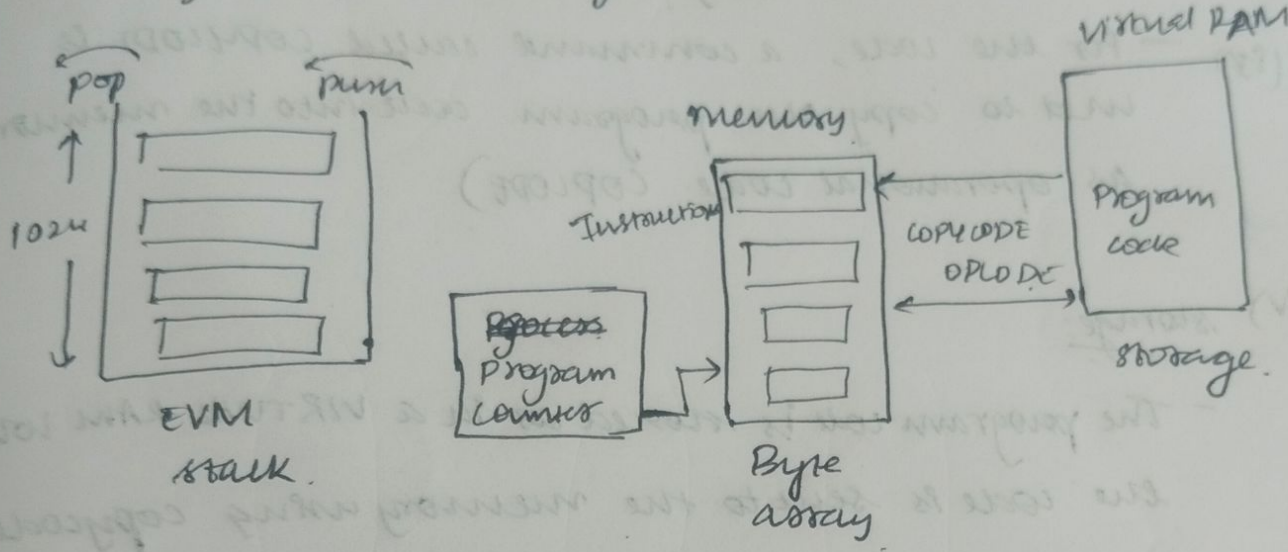
(i) One user not committing to the rules and regulations

(ii) The data integrity and privacy.

(iii) One user just ~~left~~ leaving in between making the entire pool invalid.

(5) The ethereum blockchain consists of various elements such as smart contracts, the block, EVM, etc.

The diagram for a EVM is given below.



→ The Ethereum blockchain consists of smart contracts which are for a valid agreement between ~~the~~ ~~users~~ two users.

→ The EVM is a Ethereum virtual machine, where the code is processed quickly.

→ The main components are:-

(i) EVM stack:- It is a typical stack that ~~can~~ contains input and output operations ~~to~~ for the code.

- It pushes or pops stuff based on the operation.
- It can execute 1024 instructions.

(ii) Program counter:

- The program counter keeps a track of the program and executes it one by one.

(iii) Memory:

- For memory, the EVM uses a Byte array code to store easily.

(iii) - For the code, a command called COPYCODE is used to copy the program code into the memory as operational code (OPCODE)

(iv) Storage:

- The program code is stored in a VIRTUAL RAM where the code is sent to the memory using copycode.