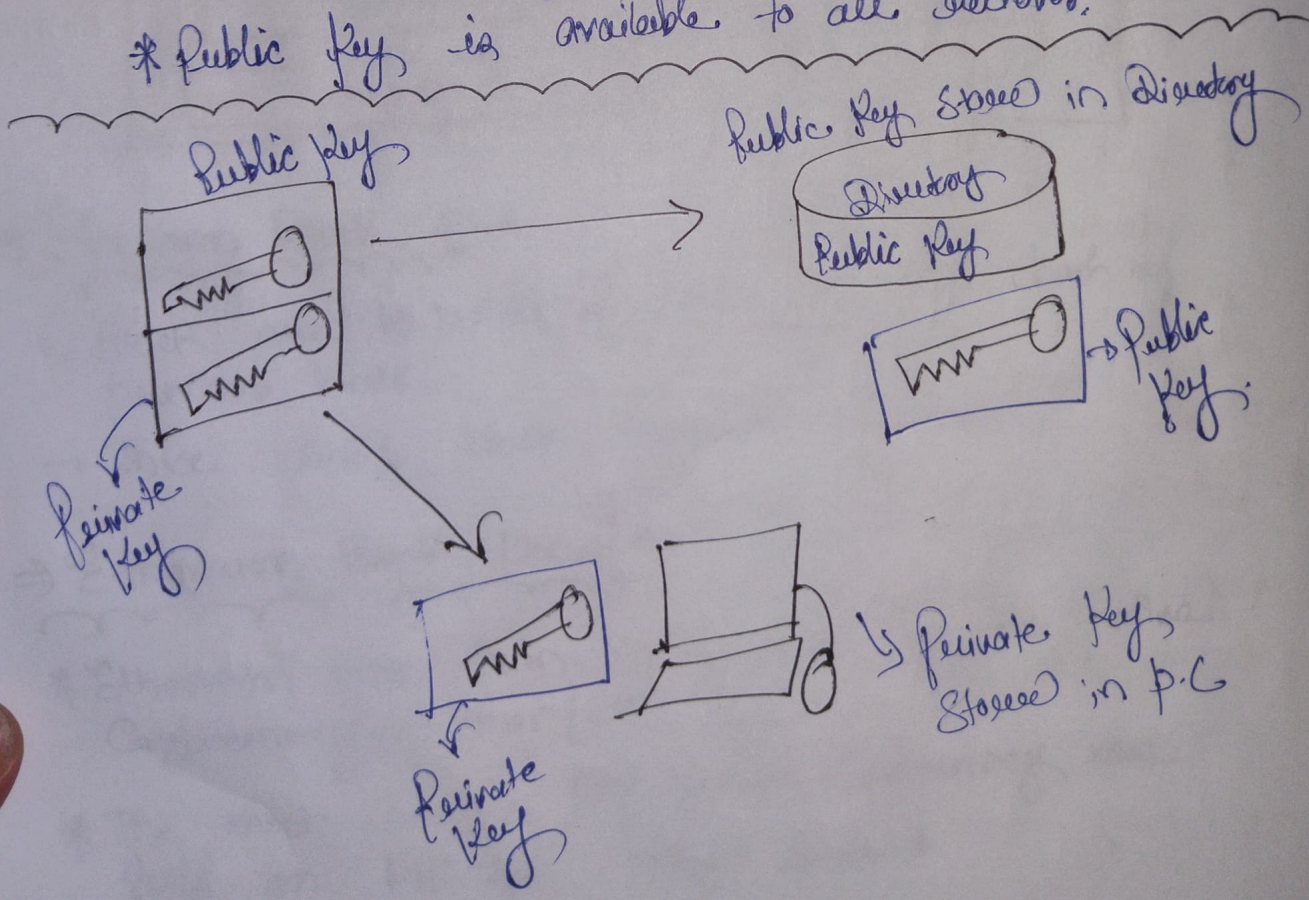
* Digital Signature & Hashing *

* Digital Signature & Hashing → Forms devised level of Security in Blockchain & Cryptography

⇒ Digital Signature :-

* Mathematical Concept to authenticate sender of E-document.
* It is attachment to any E-document that contains identity of owner
* It is used to provide Authenticity, Integrity & Confidentiality.
* Private key is accesible only to signer.
* It is used to generate signature that is attached to msg.
* Public key is available to all reciever.



* Application of Digital Signature :-

① E-mail ② Data storage ③ E-fund transfer
④ Software distribution ⑤ Smart cards.

⇒ Authentication ⇒ Fraud prevention.
⇒ Integrity of data

* Disadvantage of Digital Signature :-

① Expiry ② Public distrust.
② Difficult to understand

⇒ Hashing :-

↳ Mathematical function that takes input string of any length and convert output string of fixed length.

* Fixed value output is called Hash Value.
* It is Cryptographically secure and useful.

* Properties of Hash function :-

① Deterministic :- A hash function must be deterministic which means for any given input, a hash function always give same result.

② Avalanche Effect :- Small change in input string huge impact on output.

③ Fixed length Mapping :- length of Input & Output should be same.

* Application of Hashing in Blockchain :-

(1) Creating Immutable records
(2) Helps in Solving Complex Mathematical puzzles which help to add new block
(3) Helps to Verify identity of users in blockchain.

* Relation between Hashing and Digital Signature :-

* The process of generating digital Signature have 2 Key Step → (1) Hashing &
(2) Signing
* Every transaction are Signed using unique Hash

Mining and Validation:-

→ mining transactions are validated digitally on bitcoin network

→ Bitcoin mining is used to secure and verify transactions to the rest of the Network

→ Consider a Network of gaint block chain model

* every person who want to access data in the block chain are called Miners
* In a bitcoin data transformation each user mines into the block chain structure and client yourself
* The mining processes is mainly designed for bitcoin formation structure
* Now, Bitcoin is made with standard money maintaining with some proper data module.
* Consider an example of different different currency of dollor, Ruppee, euros, Dhenams.
* each currency will have some value to convert that dollor value to Bitcoin.
* Now to accenses different data of currencies across the world we need mining processes
* This mining is done in atmost security and least complexity.

validations-

→ validation is a part like security mechanism

→ It validates data based on the rules and etheristics of currency modulations

→ validation acts as interface b/w

* Ethereum & Bitcoin Block * [Unit-2]

*Bitcoin Block :-

* A block is a place in blockchain where information is stored and encrypted
* Blocks are identified by long numbers that include encrypted transaction information
* Block and its information must be verified by the network before new block can be created.

*Bitcoin per Block :-

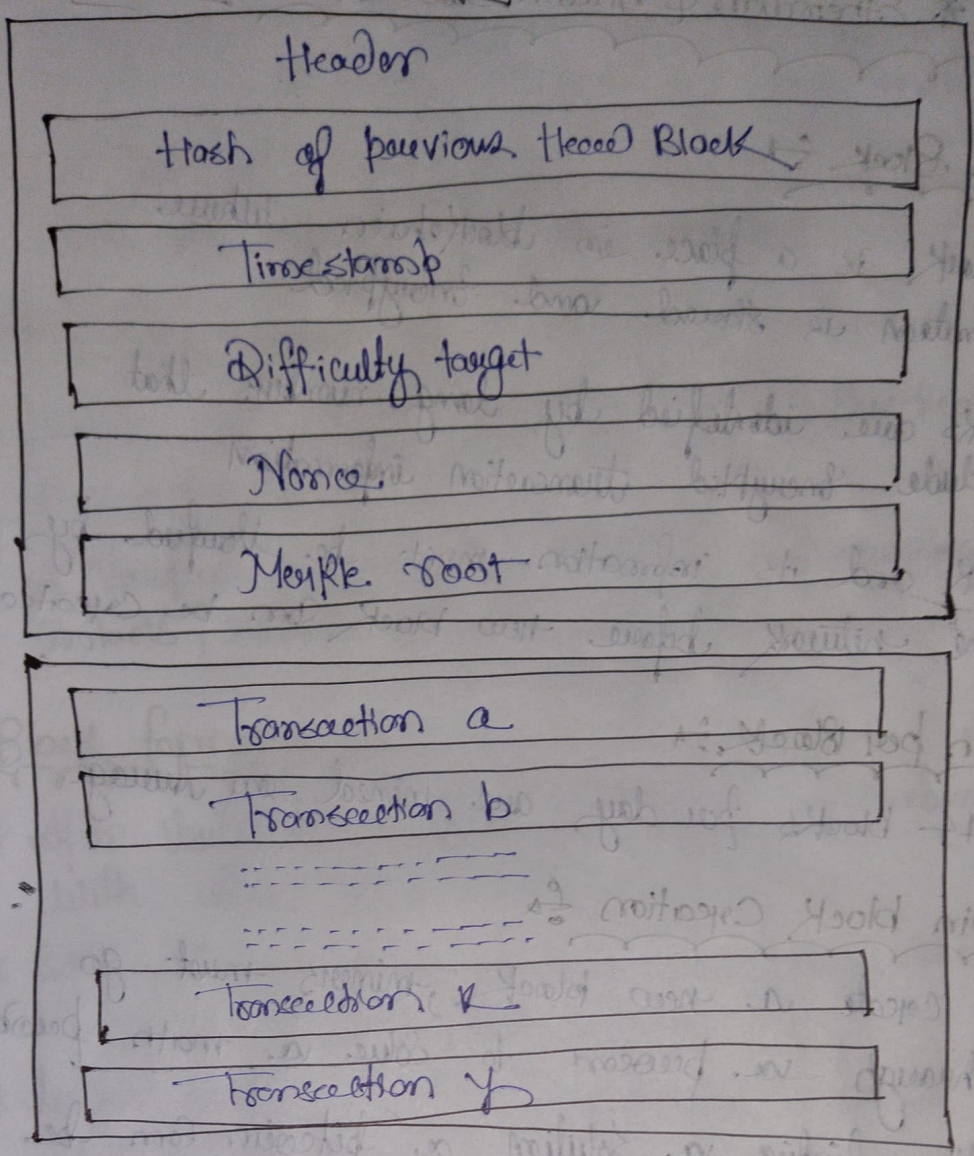
↳ 144 blocks per day are mined on Average.

*Bitcoin block Creation

* To create a new block, miners must go through a process to solve a math problem.
* After finding a solution, a bitcoin can be added to blockchain by consensus.
* Miner who will find the solution will be rewarded for new block.

*Bitcoin Block Structure

* Block is made of header containing metadata.
* It also contains long list of transaction.
* Header is 80 byte
* Average transaction is 250 bytes.



* Ethereum Block :-

↳ Block are batch of transaction with hash of previous block

→ This links block together in chain.

⇒ Ethereum Block use :-

* Ethereum Blockchain is powered by its native Cryptocurrency - Ether (ETH).

* The most common ETH-based cryptocurrency are build on ERC-20 token standards

* Working :-

* Both in Ethereum blockchain and bitcoin block chain, there is expected block time and average block time.
* In bitcoin expected time is 10-min, while in Ethereum it is 10 to 19 second.
* New Ethereum block is created every 14 second.
* Ethereum is more future proof than any protocol.

* Block and its role :-

* Each block stores previous hash, so its impossible to reverse and tamper data.
* Ethereum use proof-of-work as consensus Algorithm.
* Ethereum store several Important data.