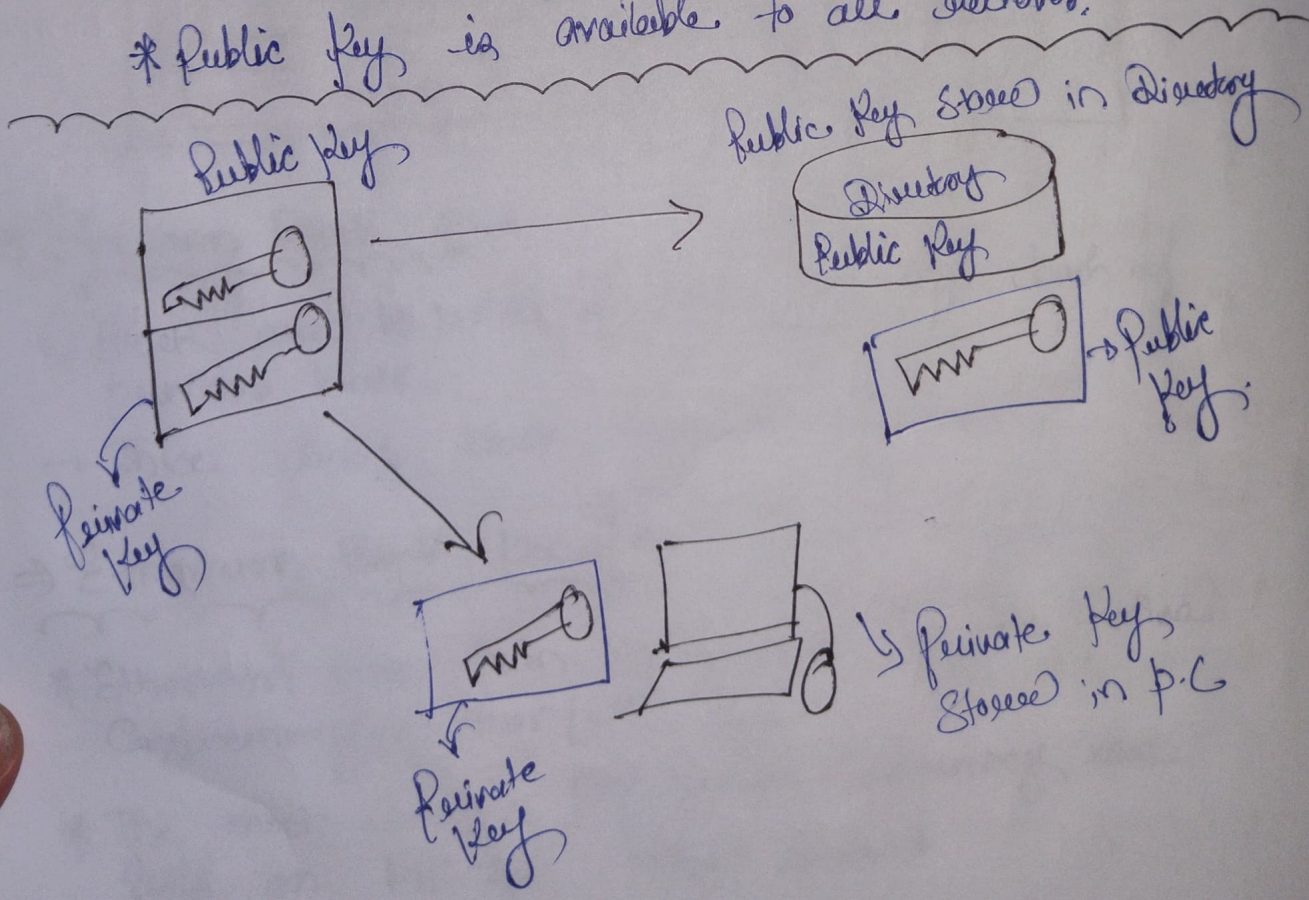
* Digital Signature & Hashing *

* 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