**Week 3**

**3.1 Creating a web based wallet**

* 20 bytes is 40 hex characters.
* In solana, we use EDDSA to get a 32-byte public key and a 32-byte private key. We use the 32-byte public key and convert it to base58 and say that this is the public address of the wallet.
* In Ethereum, we use ECDSA.
* generateKeypair() 🡪 64-byte public key 🡪 using the Keccak-256 algo 🡪 32-byte string 🡪 last 20 bytes 0x(20 bytes)
* RPC – Remote Procedure Call. tRPC, gRPC, jsonRPC. Basically, you call a function using an API call.
* Web3 coins also uses these RPC servers.
* No one makes their own RPC servers, but rather delegates it to some companies.
* You use an RPC provider which basically talks to the node in the blockchain to get a particular wallet balance etc. These RPC servers sit very close to the blockchain.
* Like dollar has pennies and rupees has paisays, Ethereum has Wei. We store in Wei because of precision inaccuracies. So integers are stored eventually for Weis. 1 ETH = 10 ^ 18 Wei.
* In case of Solana, it is Lamports. 1 SOL = 10 ^ 9 Lamports.
* You would need to install some polyfills which bip39 libraries use. They are no available in the normal JS environment.