Blockchain Transaction

Blockchain Transactions:

** Blockchains are a transaction-based system.**

Wallet helps to make a transactions:-

Wallet Address: A unique identifier for your wallet.
Private Key: A secret number that allows you to spend bitcoin from your wallet.
Public Key: Publicly shareable key that connot be used to spend bitcoin.

private key ---->(Eliptical curve multiplication algorithms) ----> Public Key ---->(RIPEMD(SHA256)) ----> Public key hash-----> (Base58check) -------> Wallet Address.

Wallet types:-

Non-deterministic Wallet: (random wallets) A wallet where private keys are generated from random numbers.

Deterministic Wallet: A wallet where addresses, private keys, and public keys can be traced back to their original seed words.

Hierarchical Deterministic Wallet: An advanced type of deterministic wallet that contains keys derived in a tree structure.

Generating private key:-

Private Key: A 256-bit random number between 1 and 2^256.

Entropy: Lack of order or predictability. The degree of disorder or randomness in the system.

Signing a Transaction:-

Signature: establish proof of ownership for each transaction on the blockchain.

made by **Mohamed Abdel Nasser** :)