Week 2: Public Key Cryptography

How banks do Auth

username → HDFC → Rs 20,000 transfer
PWD

Blockchain Auth

Public-Private Key pair

Asymmetric cryptography

Publickey → Blockchain → Money

~~Solana~~
solscan.io
explorer.solana.com

Private key

PAGE NO.:

Bits and Bytes

Bit → Smallest unit → 0 and 1

Byte → 8 Bits

0 → 255

Uint8Array

32 Bytes → Private Key

255^{32}

Strings represented in Binary

ASCII

65 ⇒ A

97 ⇒ a

Hex

1 character = 4 bits

0-9 and A-F

Base 64

64 different chars

(6 Bits) = 1 character

Base 58

58 characters

Hashing v/s Encryption

hello $\xrightarrow{\text{Hashing algo}}$ asdf !

Encryption → Both ways

Key

Symetric

hello $\xrightarrow[\text{key}]{\text{Encryption}}$ akiuui $\xrightarrow[\text{key}]{\text{Decryption}}$ hello

Asymetric

hello $\xrightarrow[\text{Private key}]{\text{Encry}}$ asdf..... $\xrightarrow[\text{Public key}]{\text{Decryption}}$ hello.

Signature

PAGE NO.:

~~Q & A~~

Public key & Private Key

Salt ⇒ Post Hashing.
(for same pwd in database)

Graf ⇒ Fees, Incentive.
SOL, ETH

#2.2 Web Based wallet

Public Key.
Private Key.

01011001 01011000 $\xrightarrow{\text{ASCII}}$ XY
$\xrightarrow{\text{Hex}}$ 5958

solscan.io

→ code of conversion

Encodings

== Base 64.

Asymetric Encryption : Public key cryptography

Private Key ⟷ Public key

RSA ⇒ Prime nos multiple
ECC - ETH & BTC
EDDSA -
ECDSA -

PAGE NO.:

Common eliptic curve

1) secp256k1 - BTC and ETH
2) ed25519 - SOL

Hashing - SHA-256
MD5

Symmetric - AES

$x^2 = y^3$

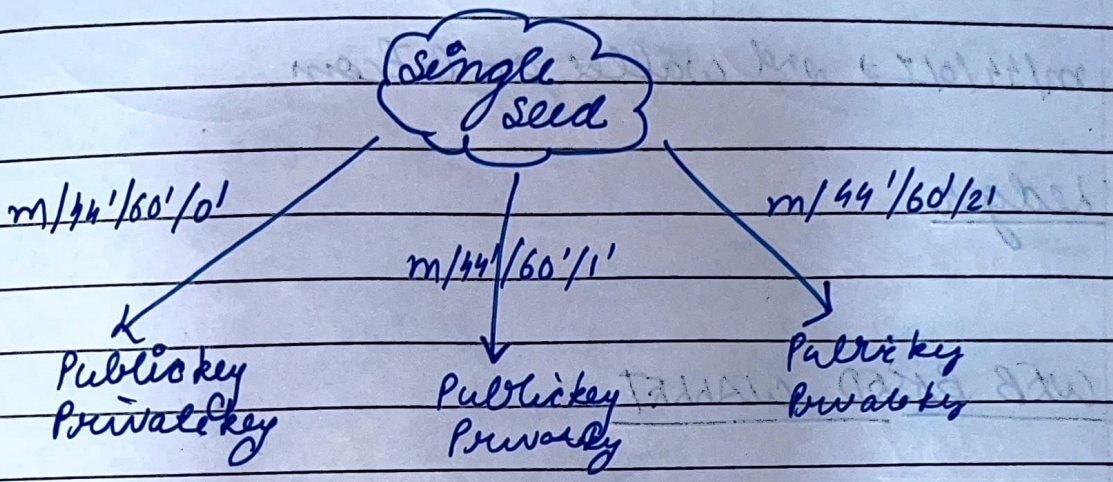
Creating a public/private keypair

1) Create
2) Define
3) Convert
4) Sign
5) Verify

You → sign
Minor → Hash

Hierachical Deterministic (HD) wallet

Tree of key pairs from a single seed



BIP-32 → Recovery

crypto steel

How to create a wallet

Mnemonics → human readable string of words
(seed)

seed phrase

Interportability

BIP44

// bitcoin addresses, eth addresses, sol addresses

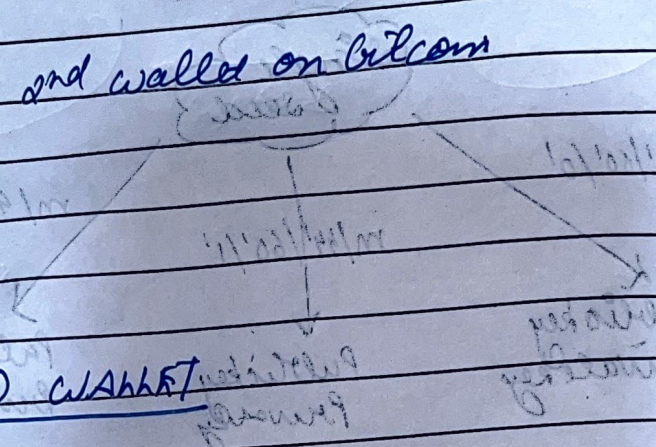
m/44/0/0 ⇒ 1st wallet on bitcoin

m/44/501/0 ⇒ 1st wallet on solana

m/44/60/0 ⇒ 1st wallet on ETH

m/44/0/1 ⇒ 2nd wallet on bitcoin

Ledger



WEB BASED WALLET

Assignment left.