# Blockchain Application and Architecture

## CIA - IA

Manish Bhart
1947235

1.) Account based coin transfer description :

Create 30 coins & credited to Bob
Asserted by miners

Transfer 15 coins from Bob to Alice
Signed (Bob)

Transfer 5 coins from Bob to caral
Signed (Bob)

Transfer 10 coins from Alice to Jim
Signed (Alice)

Transfer 6 coins from Jim to Caral
Signed (Jim)

Transfer 8 coins from caral to John
Signed (caral)

Transfer 5 coins from John to Bob
Signed (John)

Transfer 10 coins from Bob to Caral
(Signed Bob)

Transfer 3 coins from caral to John
(Signed Carol)

Transfer 8 coins from caral to Alice
Signed Caral

## Transaction based ledger:-

1) Input : ϕ
Output : 30.0 → Bob

2) Input : 1[0]
Output: 15.0 → Alice, 15.0 → Bob, Signed(Bob)

3) Input : 2[1]
Output: 5.0 → Caral, 10.0 → Bob, Signed(Bob)

4) Input : 2[0]
Output: 10.0 → Jim, 5.0 → Alice, Signed(Alice)

5) Input : 4[0]
Output: 11.0 caral, 4.0 → Jim, Signed(Jim)

6) Input : 5[0]
Output: 8.0 → John, 3.0 → caral, . Signed(Caral)

7) Input : 6[0]
Output: 15.0 → Bob, 5.0 → John, Signed(John)

8) Input : 7[0]
Output: 13.0 → caral, 5.0 → Bob, Signed(Bob)

9.) Input: 8[0]
Output: 6.0 → john, 10.0 → carol, Signed(carol)

10.) Input: 9[1]
Output: 13.0 → Alice, 2.0 → carol, Signed(carol)

③ A cryptography wallet is a piece of software that keeps track of the secret keys used to digitally sign cryptocurrency transactions for distributed ledgers. Because ~~to~~ those keys are the only way to prove ownership of digital assets and to execute transactions the transfer them or change them in some way - they are a critical piece of the cryptocurrency ecosystem.

Crypto wallets keep track of encryption keys used to digitally sign transactions, it also stores the address on a blockchain where a particular .. asset resides. If they (owners loses . that address, they essentially lose control over the digital money or assets.

(2.) Bitcoin doesnot use the account model. the account model works on ~~ac~~ BALANCE. But Bitcoin works on transactions. In account model, if alice receives 25 coins in first transaction and then transfers 17 coins to Bob in second transaction, she would have 8 bitcoins left in her account

Thus it works based on balance. Downside of this model is that if anyone has to confirm it ~~his balan~~ the transaction is valid, will have to keep track of these account balance.

But in case of transaction ledger, it keeps tracks of trans-actions not the account balance. Looking up the transactions output is easy since it uses hash pointers. To ensure whether coins are not been spent, we need to scan the blockchain between the referenced transaction and the latest block; we need not go through whole blockchain from beginning.

- This bitcoin script which is used in transaction based ledger helps to prevent the double spent attack.