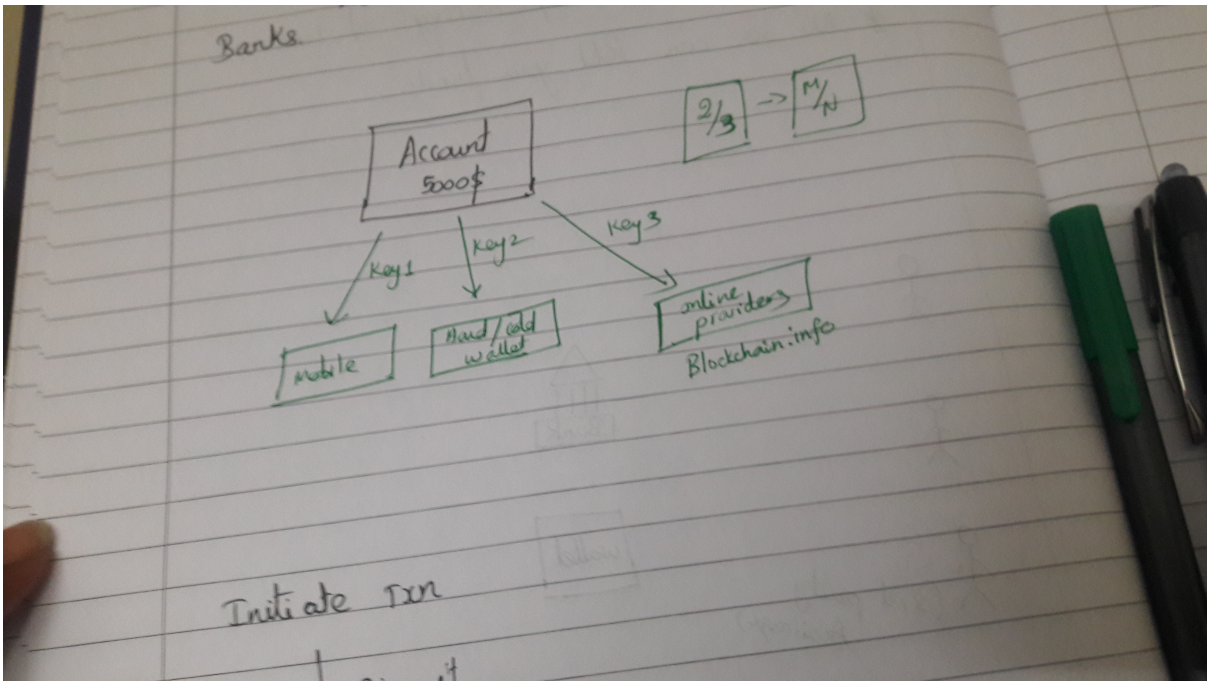
Multi sig wallet

Enables trust layer in transactions



THANGARAJ M

Moving Funds without Intermediaries

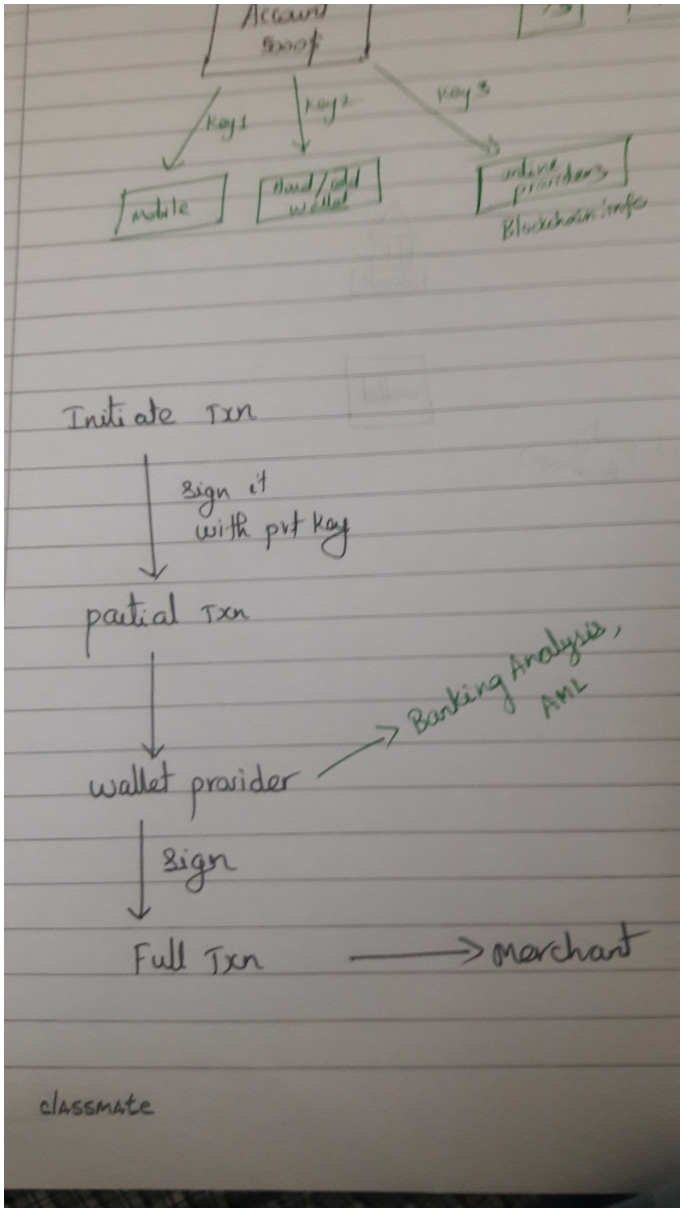
Multi sig wallet works on M-N Model

M -> Private keys required to sign

N -> Total number of Private Keys

A Transaction between two Entities in Traditional way includes lot of Intermediaries to Validate the Transactions and they are charging to process the Transactions.

Once a transaction is Initiated from Sender, it is partially signed with the private key and it requests the wallet provider to validate and sign the Transactions.



Master card could be your Multi sig provider or even blockchain.info could be your Multi sig Provider. which uses AI and Banking Analysis to find whether the Transaction is legitimate to not.
and The Transaction gets signed with the second key. Now Transaction is fully Signed and we can move funds without the involvement of any Intermediaries.
There is no Single point of failure.
and no one owns your funds.

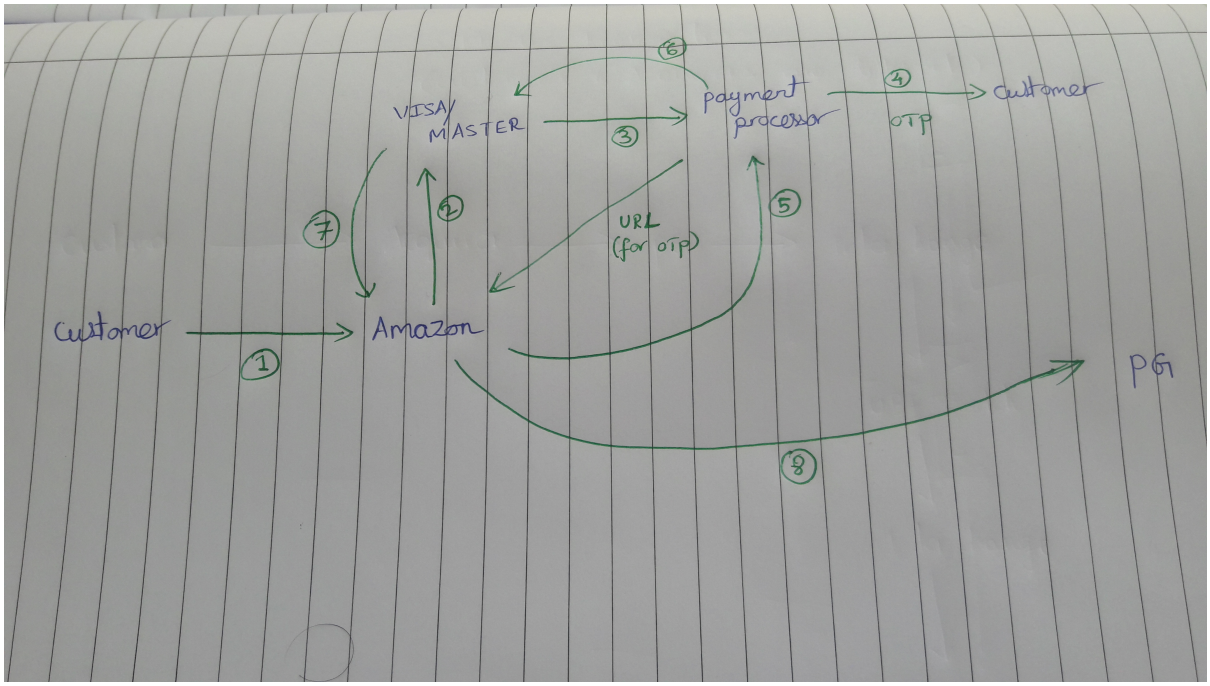
Advantages of having a Multi sig Transactions :

- Benefits on Fraud Protection
- Tracking of Transactions
- No one can hold/move your Funds

Cashaa is working on Multi sig Model

Involves Banking Analysis, AML Models and AI

- It can also be used for more advanced scenarios such as an address shared by multiple people, where a majority vote is required to use the funds.
- 2-of-3: Any two out of three parties can approve the transaction. This is commonly used for escrow purposes, where the two counterparties to an agreement engage a third party to act as an arbitrator in the event of dispute.
- Public key encryption, also known as asymmetric cryptography, is a key underlying technology of blockchains. Participants in the chain generate their own pairs of private keys and public addresses. They keep the private keys secret, but freely distribute the associated addresses. A blockchain transaction which performs an action for a particular address (e.g. spending its funds) must be signed by the corresponding private key. All participants on the chain can then verify these signatures, using public addresses only, without needing to see each others' private keys.



Traditional Model vs Multi Sig