5)Registering Miners and Creating new blocks:

1.Miner Registration:

When a new miner joins the network, they must register themselves with the other nodes in the network. This involves broadcasting a message that includes the miner's public key and other identifying information. The steps involved in the miner registration process are as follows:

- The miner generates a public and private key pair to use for authentication and encryption purposes.
- The miner broadcasts a message to the network nodes announcing its presence and providing its public key and other identifying information.
- The network nodes receive the miner's message and verify the authenticity of the miner's public key using digital signatures.
- The network nodes add the miner to their list of known miners and allow them to participate in the network.

2.Validating Transactions:

Before a miner can create a new block, they must validate a set of pending transactions. This involves verifying that each transaction is valid, has sufficient funds, and has not already been spent. The steps involved in validating transactions are as follows:

- The miner receives a set of pending transactions from the network.
- The miner validates each transaction by verifying its digital signature, checking for sufficient funds, and ensuring that the transaction has not already been spent.
- If a transaction is found to be invalid, it is discarded and not included in the block.
- Once all transactions have been validated, the miner is ready to create a new block.

3.Creating a New Block:

To create a new block, a miner must follow the steps outlined below:

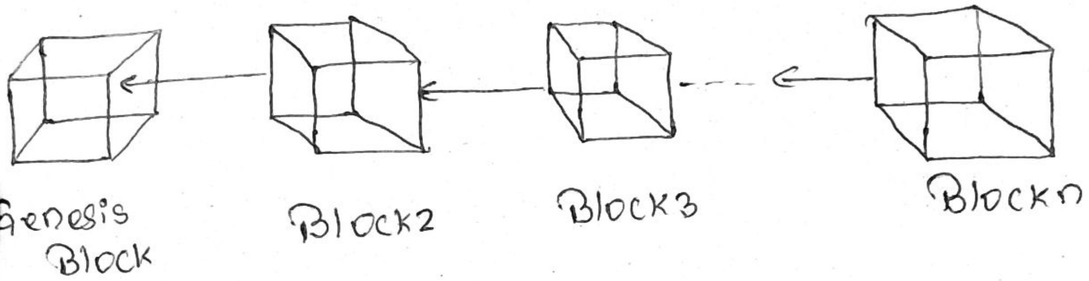
- The miner begins by creating a block header, which includes a reference to the previous block in the chain, timestamp, and a nonce (a random number).
- The miner adds the validated transactions to the block.
- The miner calculates a hash for the entire block by hashing the block header and the list of transactions using a cryptographic hash function like SHA-256.
- The miner must then solve a cryptographic puzzle by repeatedly hashing the block header with different nonce values until they find a solution that meets the network's difficulty target. This process is called mining, and it is designed to be computationally difficult to prevent malicious actors from creating fake blocks.
- Once the miner finds a valid solution, they broadcast the new block to the network.
- The network nodes receive the new block and validate it by checking that it meets the difficulty target, that the transactions are valid, and that the block references the correct previous block.
- If the block is valid, the network nodes add it to the blockchain and update their copy of the ledger to reflect the new transaction history.
- The miner who created the block is rewarded with a set amount of cryptocurrency as an incentive to continue mining and securing the network.

In summary, registering miners and creating new blocks in a blockchain involves several steps, including miner registration, transaction validation, and block creation. Each step must be performed correctly and securely to ensure the integrity of the blockchain network.

2. Genesis Block and sharing Block:-

Each Blockchain application needs a genesis block, which is the very first block of the blockchain.

→ The Genesis block is the first block is any block-chain based Protocol. It is ~~bias~~ basis on which additional blocks are added to form a chain of ~~→~~ blocks, hence the term blockchain.



→ Genesis Block is sometimes refers as Block 0.

→ Every block in a blockchain stores a reference to the Previous block.

→ In the Case of Genesis block, there is no Previous block for reference.

→ In terminal terms, it means that the Genesis block has it's "Previous hash" value set to 0. This means that no data was Processed before the Genesis block. All other blocks will have sequential numbers staring by 1, and will have a "previous hash" set to the hash of the previous block.

→ The hash of genesis block is added to all new transactions in a new block. This combination is used to create its unique hash.

Bitcoin Genesis Block

-> The most famous Genesis block was "Bitcoin Chain"

-> A coinbase transaction is the first transaction a miner places in a block constructed by them; it is a transaction rewarding the miner in Bitcoins for successfully creating a block to be relayed to network

Genesis Block Node :-

Without Genesis Block, it would be really difficult for the miners to trust a blockchain and to know when and how it started.

-> In theory, there is no real need for a Genesis Block. However, it is necessary to have a starting Point that everyone can trust.

Genesis Block - Block data.

The example taken here is the Bit Coin block Chain of the genesis block:

-> Number of transactions : 1

-> Transaction fee : $0.00

-> Block height : 0

-> Time stamp : 03/04/2023; 11:35.

-> Non ce : 208393

-> Block diffculty : 1

Block height:-

Block height of a block is the no.of blocks in the chain before that given blocks. Therefore the height of the Genesis block is 0 because no block was Placed before it.

Timestamps

Time stamps generally used to store the data and time of a given event. However, it is important to note that block timestamps are not exactly accurate, and they do not need to be. Block chain times are accurate only to within an hour (or) two.

Nonce:-

nonce is a random 32-bit number that miners use as a base for their hash calculations.

The term stands for nonce is number used once is commonly referred to as a cryptographic nonce.

Transaction fee:-

The blockchain fee is a cryptocurrency transaction fee that is Charged to users when performing crypto transactions.

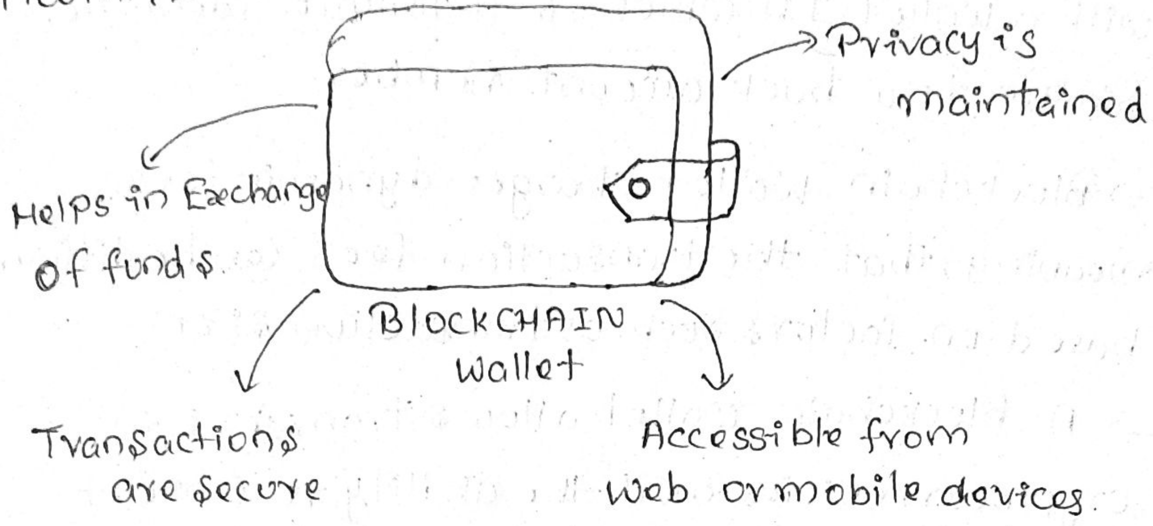
Block difficulty:-

The difficulty is a measure of how difficult it is to mine a bitcoin block.

The maximum block difficulty is 1

Blockchain Wallet:-

A Block chain Wallet is a cryptocurrency wallet that allows users to manage cryptocurrencies(like Bitcoin, Etherium, etc..,


Privacy is maintained
Helps in Exchange of funds.
BLOCKCHAIN Wallet
Transactions are secure
Accessible from web or mobile devices.

* It is very similar to the Process of sending or receiving money through PayPal (but uses cryptocurrency instead)

Examples of Blockchain Wallets

1. Electrum
2. Jaxx
3. Samurai
4. Bitcoin Paper wallet
5. ~~Bitcoin~~ Block chain.info

* Helps in Exchange of funds.

* Privacy is maintained.

* Transactions are secured.

* Accessible from web (or) mobile devices.

* Creating an e-wallet with blockchain wallet is free, and the account setup process is done online. Indivuals must Provide an email address and Password that will be used

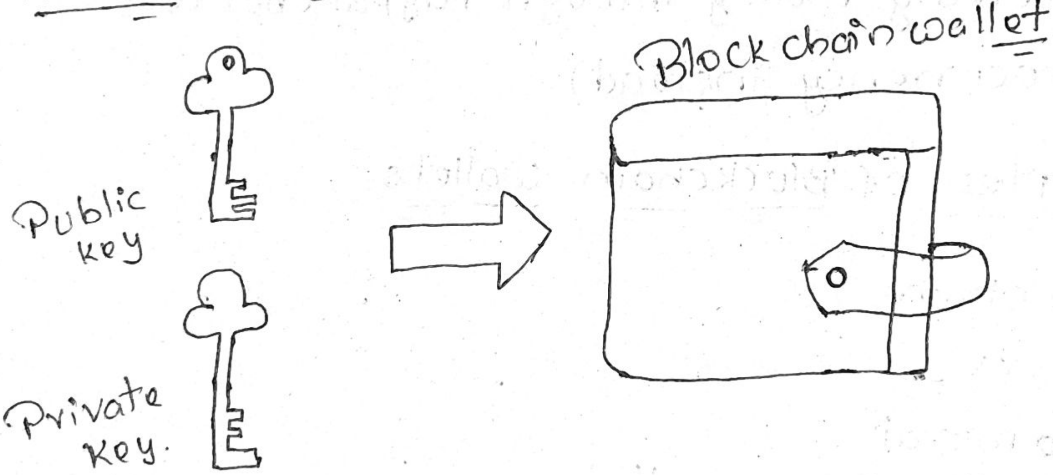
to manage the account, and the system will send an automated email requesting that the account be verified.

-> Once the wallet is created, the user is provided with a wallet ID, which is a unique identifier similar to a back account number.

-> Blockchain wallet charges dynamic fees, meaning, that the transaction fees can be different based on factors such as transaction size.

-> A blockchain wallet allows transfers in cryptocurrenicies and the ability to convert them back into a user's local currency.

How do Blockchain wallets work



Block chain wallets follows using Public key and Private key both together

-> Public key is similar to the email address of a Person basically, whenever your wallet is generated Public key is generated you can share that Publickey with anyone inorder to receive funds.

→ Private key is top secret it's similar to your Passwoord it should not get hacked or you should not disclose it to anyone and you use this private key to spend your funds.

→ With Blockchain wallet, no one will be able to send cryptocoins (emails) through your Public key (e-mail address,) until they know your Private key (Passwoord).

Features of Blockchain wallet

→ Easy to use

→ security.

→ Instant transactions

→ Currency Conversion.

Types of Block chain wallet

There are two types of Blockchain wallet based on Private keys.

1. Hot wallet

2. Cold wallet.

Hot wallet

Hot wallets are like normal wallets which we carry for day to day transactions.

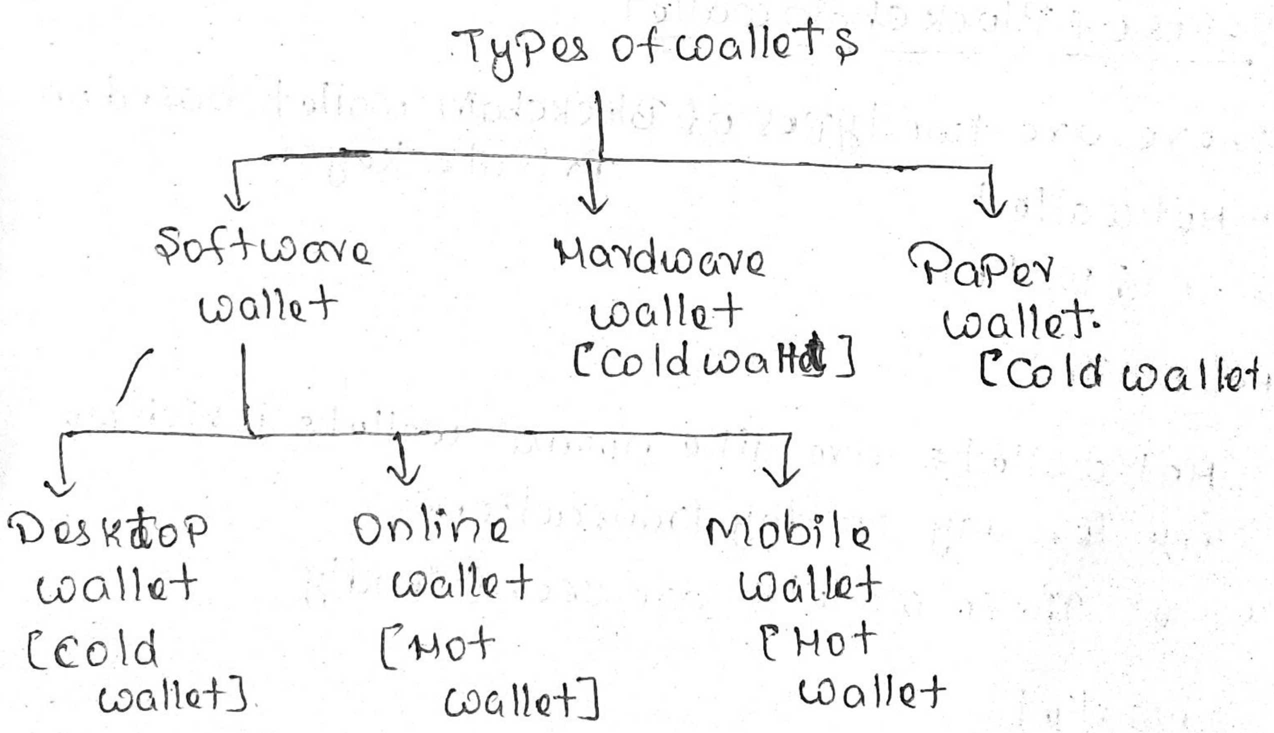
Note: These wallets are user friendly.

Cold wallet

Cold wallets are similar to a vault, where cryptocurrencies are stored with a high level of security.

Hot wallets	Cold wallets
→They are the online wallets through which cryptocurrencies can be transferred quickly.	→ They are digital offline wallets where the transactions are signed offline and later disclosed online
→Private keys are stored in the cloud for fast transfer	→ Private keys are stored in a hardware or a paper document
→ It is easy to access, but has a risk of unrecoverable theft when hacked	→ This method of transaction helps in protecting the wallet from unauthorized access and other vulnerabilities.

→ Furtherlly, types of wallets.


Types of wallets
Software wallet
Hardware wallet [Cold wallet]
Paper wallet. [Cold wallet
Desktop wallet [Cold wallet]
Online wallet [Hot wallet]
Mobile wallet [Hot wallet