* What is Blockchain Technology.

→ Yaa, when we search something on Google that data is retrieved From the Google Server. Means the data is centralized. But in case OF Block chain The data is not Centralized Means The data is Distributed among several Computers. means the Data is Decentralised or we can say that The data is Distributed so IF you become the Part OF that network you also have Copy OF that Data.

* Thaee TYPES OF Blockchain :-

- Public Blockchain :- A Public, or Permission-less blockchain network is one where anyone can participate without restrictions.

- Permissioned or Private blockchain :-

→ Oracle Blockchain PlatForm is a Permissioned blockchain.

- Federated or Consortium blockchain.

- A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of stake holders.

→ Meaning:-

- બ્લોકચેન નેટવર્ક જ્યાં સર્વસંમતિ પ્રક્રિયા (mining process) નોડ્સના પહેલાથી પસંદ કરેલ સમૂહ દ્વારા અથવા પહેલાથી પસંદ કરેલ સોફ્ટવેર હિતધારકો દ્વારા નજીકથી નિયંત્રિત થાય છે.

* Is Bitcoin & Blockchain the same thing?

→ No, Because Bitcoin is Crypto Currency. It's a Digital money, And the Technology behind Bitcoin & all the other crypto currencies, is Blockchain But it doesen't mean that Bitcoin & Blockchain are the same things. Because Blockchain has other Applications like Smart Contract & Decentralised Applications as well. That's why we can't say that,

Bitcoin & Blockchain are same Things. But we can say that, Bitcoin is a Blockchain.

→ Blockchain is Distributed, Secure, Transparent, Immutable, and accessible.

* Benefits of Blockchain:-

{ IIII TT RSVD }

- Trust
- Decentralized Structure
- Improved Security and Privacy.
- Reduced Costs
- Speed
- Visibility and traceability.
- Immutability
- individual Controls of data.
- Tokenization
- Innovation

* Disadvantages OF Blockchain :-

[HHHIIISSSD]

→ Slower Process
- High energy Consumption
- inEficient
- High cost
- interOperability
- Harder To Scale
- Data is immutable
- Self- maintenance
- Still Not mature
- integration

* Solidity Programming :- O.S.G Documentation

→ Solidity is the main Programming language For Writing Smart Contracts on an Ethereum blockchain network.

→ It's a Contract-Oriented language which means they organize code, Store data, and write all your Programming logic.

→ With Solidity you can create Contracts For uses such as Voting, CrowdFunding, blind auctions, and muti-Signature wallets.

→ It's Case Sensitive.

• NFT :-

→ NFT means Non-Fungible Tockens, OR we can say that "Non-Replaceable".

→ NFTS can be linked to "Real-World Objects".

→ NFTS represents digital rights to assets such as audios, videos, ART, DIGITAL Assets etc.

• The Process OF Creating an NFT :-

→ CReate the Artwork

→ Select a marketPlace

→ Create a Crypto Wallet

→ Connect The Wallet To a marketPlace.

→ Uplocid Your Artwork to the marketPlace

→ List Your NFT For SALE

* Uses :-
* Real Estate :-
* ART :-
* Luxury items :-
* logistics :-
* Domain name ownership :-
* Bitcoin mining :-

→ Bitcoin mining is the process of creating new bitcoins by solving extremely complicated math problems that verify transactions in the currency.

→ When a bitcoin is successfully mined, the miner receives a "pre determined amount of bitcoin".

→ Miner :- Computers that validate and process blockchain transactions.

* Bitcoin :-

→ Bitcoin is a Decentralized network of digital currency.

→ Transactions are made to and from 16 character encrypted address.

→ These addresses are mathematically secure so that no body but the owner of the address can transfer the funds that belong to it.

→ "Bitcoin has become a hot Commodity among speculators!!

"બિટકોઈન એક કોમોડિટી."

* MetaMask :-

→ MetaMask is a Software Cryptocurrency wallet used to interact with the Ethereum blockchain.

→ It allows users to access their Ethereum wallet through a browser Extension or mobile app.

→ which can then be used to interact with decentralized applications.

• Smart Contracts :-

→ Benefits of Smart Contracts :-

- Speed, efficiency and accuracy.
- Trust and transparency.
- Security → Program stored on a blockchain that run when predetermined
- Savings conditions are met.

→ Smart contract is that it's like a computer program that directly controls ~~computer~~ ~~program~~ digital assets. now the kind of direct control here is important right? it's not a computer program that makes a

—> Blockchain Technology relies on a decentralized method to store your data what this means is say For example you're watching this particular Video have you ever wondered where this video is actually stored on the internet it might be stored on one of google servers and your web browser may be google chrome, internet explorer or even your Youtube app will be requesting google Servers for it after this those servers provide this video to you so that you can view it but then there's a small problem with this method what if google one day goes down or there's some attack on google servers in that case all of our personal videos can also get deleted other than this Youtube has the sole right to take down or remove any of the videos they want as it is stored on their servers this causes a lot problems For Freedom of Speech and they might take down videos just because a certain part of the Society might not agree with the views now of course I can go on and on with the

Problems of such a centralized method or storing data but there are pros to it as well there are some good things with it as well things like you do not get glitches the security is entirely maintained by google and all of those things are there as well but then people wanted a decentralized method that's why they came out with the Blockchain technology and made sure it relied on a decentralized approach so that no one can take it down or stop it that's why there's a huge demand for blockchain developers in the market and you can see a lot of big companies opening up slots for blockchain developers on their teams so now that you've gotten interested in learning about this technology.

ENGINEERING Code:-

→ Actually the word Blockchain was being proposed by "Satoshi Nakamoto" in 2008.

→ Satoshi Nakamoto proposed you know in white papers about this particular blockchain.

→ A Blockchain is simply a block of transactions chain together is a chronological order.

→ Actually the Blockchain is a Record which have been connected to each other cryptographic, you know linking.

→ E.g :-

- A sends 5$ to B at 9:05 pm
- B sends 15$ to C at 9:06 pm
- D sends 200$ to E at 9:08 pm.

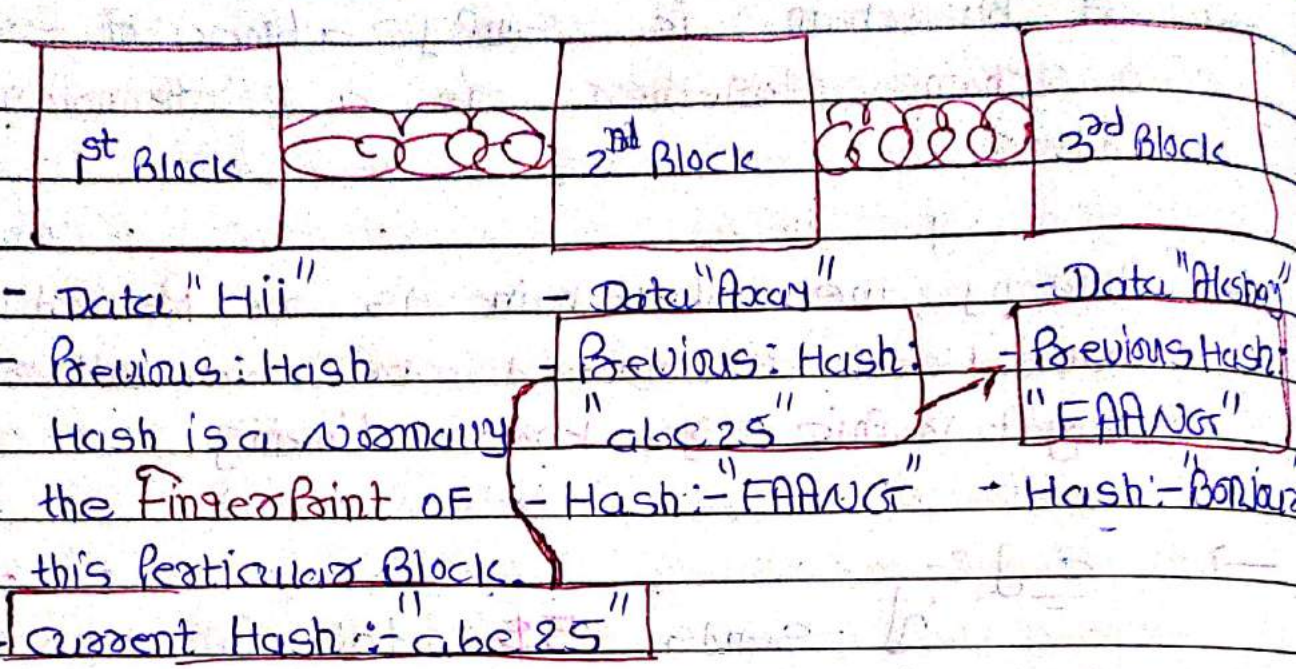
→ So Actualy they are in cronological order, They are in the order in which They happends so that is Blockchain.

→ Remember the First Block is Genesis always called "Block"

→ And It will always the first one.

* Cryptographic Linking Process :-

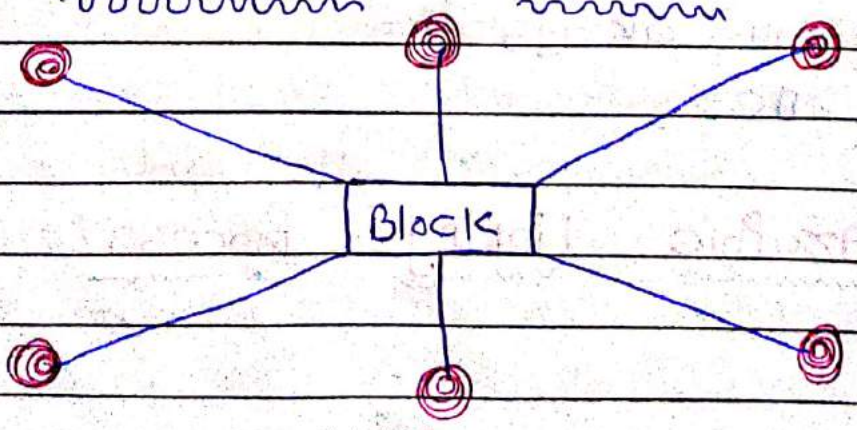
→



* Blockchain *

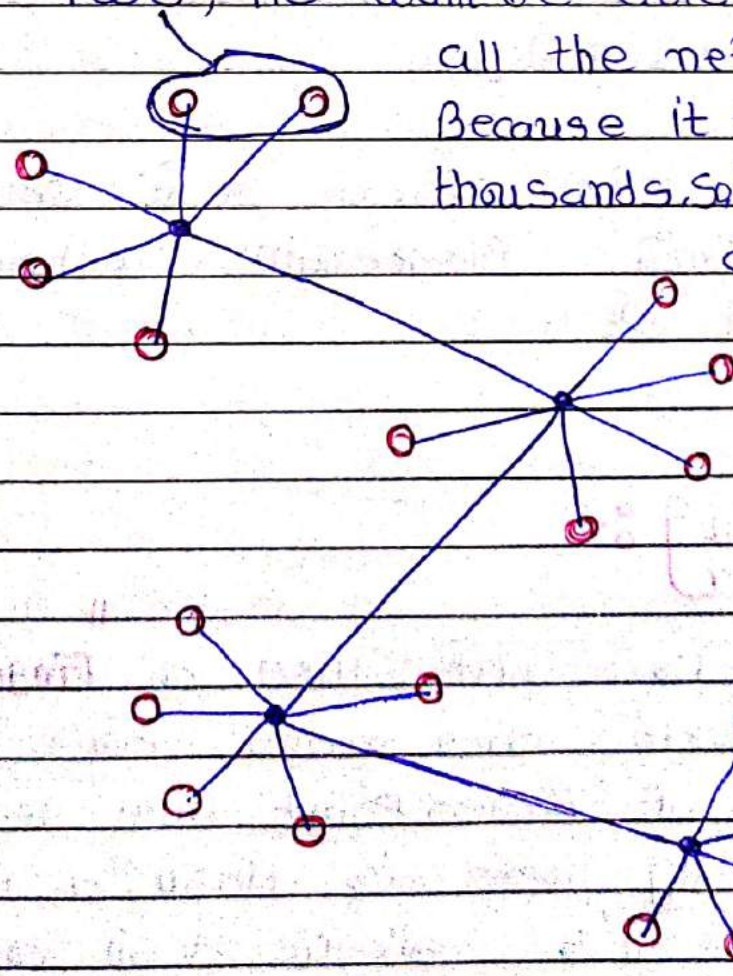
→ There are millions, Thousands, of Computers on which our Blocks are Being saved, Our data is Being saved and all of theme are connected to each another.

→ ## * Centralized System *



→ One Block is having its data and it will, every one will get will shared data From That Particular System So This one is centralized everyone is getting data From Server. * Decentralized System *

→ In case OF Decentralized it's not like that it's having data, each and every one having the same data, so even though hackers is Trying to Trick / Temper. To This Too, He Wont be able to Manipulate all the networks Because Because it there is millions thousands, so it impossible at very First instance to Perform this types OF attacks, So That's the Beauty OF Blockchain That's why it's very much secured and that's why we are



Shifting a From This world From you know.

Normal leaser Technique or Record keeping Technique to the Block chain Techiniques.

→ ડિજીટલ પાસપોર્ટ દ્વારા દુબઈ ઇંટરનેશનલ એરપોર્ટ પર બ્લોક ચેઈન સિક્યોરીટી મળશે.

→ ડિજીટલ પાસપોર્ટ તમામ Real estates ક્ષેત્રો સંપત્તિ થી જોડાયેલા transations Blockchain કે જરિયે હોંગે.

→ કિરાઈ સર્ટિફિકેટ ટેલિકોમ બિલ પણ Blockchain થી ભેગા કરી શકીશું.

→ MicroSoft, IBM, cisco અને crypto સહીત 46 કંપનિયો Blockchain Technology સે જુડ ચુકી હૈ.

- ## Hashing :-

→ Hashing is just like a "FingerPrint." like in real world each means are their indevedual sort of Finger Paint just like in world of Computing there is Hash, a like each File is having it's specific Hash and you know there is really small chance.

→ A hash is a function that converts an input of letters and numbers into an Encrypted output of fixed length.

→ SHA 256 → Secure Hash Algorithm 256 bits / 32 byte

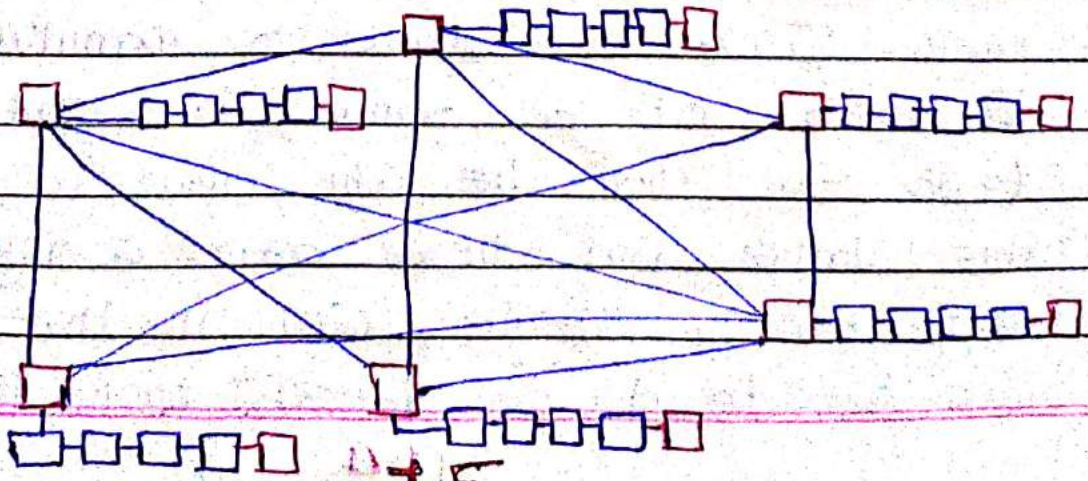
→ Websites :- "https://emn8ers.com"

* Characteristics of Hashing :-

- One way
- Deterministic
- Avalanche effect
- Fast computational
- Must withstands collisions

* Distributed P2P Network :-

→ Blockchain works on Distributed P2P Network.

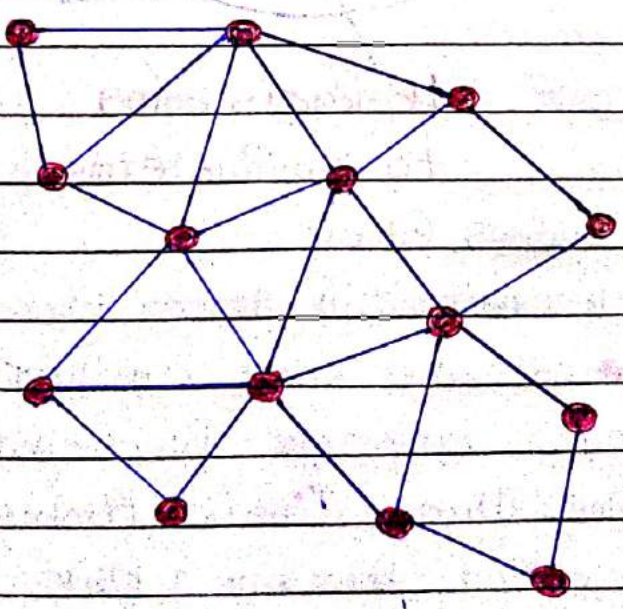


→ When some one will try to you know hack out your Record some what they have to do a like For Example They want to They manuplated this Record IF they manuplated this record It means The cryptographic link will be broken So that it will do it will created the Red signals It will give a red signal like damm There is Problem in our Blockchain it will Request another there is a Problem in our cryptographic link now all this links, all the cryptographic you know leaser will send him The File From their end them we will able to update it out So that's the reason why I told you like you know tough some one to hack all the system at a some time.

→ So, IF some one want to manuplate this value in that case what we have to do IF there is 1, 2, 3, 4, 5, 6 Computers out OF Six we have to make sure like more then 50% we have to manuplate 4 Devices at a some time and IF he able to do So then he will able to play with this value but here are 6 only Just Think For a while Gm in that case what we have to do we have to hack more then

4M devices, actually 51%. atleast 51%. Hackers have to hack then only we will able to manipulate this value so that's the Beauty of you know about it beautiful ledger Because it completely relaying on Destributed Peer2Peer Network how ever like whatever the records are being kept on Particular devices being shared by each and every devices so it's like even in Natural Calamities there are loat OF countries a ware netware calaminities are very much common.

→ This idea OF Blockchain was Termed in 2008 when there was also you know Serious Break down economic Background.



* Distributed *

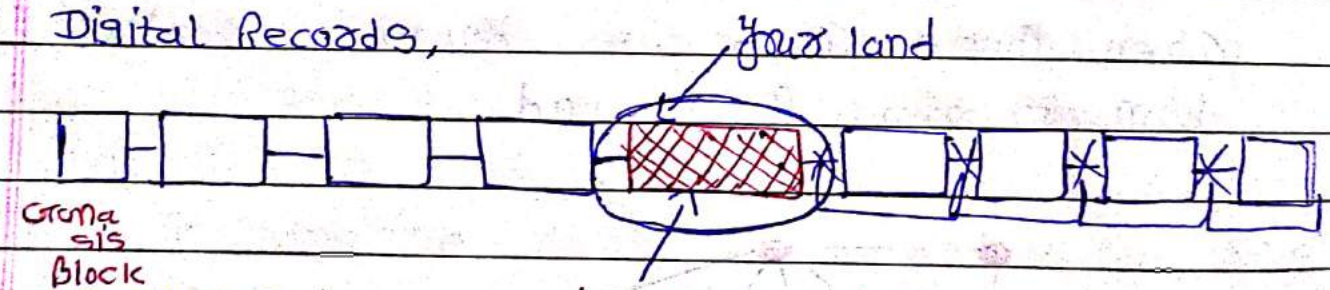
- Immutable Ledger :- (अपरिवर्तनीय)

→ Ledger is old way of gaining the records, older companies do what they keep their records.

→ Loats of Financial company do what they records of they write each and every thing.

→ For Ex:- I have money then I want to purchase the land so it dosen't like,

→ Digital Records,



Blockchain getting solutions, Block

→ Particular Block Chain will get to know like they will starts getting message from another Blockchain Blocks, you know another Blockchain immutable ledger saying like Dude there is a Problem on your 5th Block and again they will update it's out.

How to create your own cryptocurrency?

→ 1. Install Meta Mask
   a. create account and switch over to test net

2. Go over to Ropsten
   a. Receive the tokens after a while.

3. Go over to ConsenSys github account
   a. Check 'tokens': Ethereum tokens Contract' Repository.
   b. Contracts → eip 200 → Solidity Contracts.
   c. Import the contracts on remix.

4. Run and deploy your own cryptocurrency!!!

5. Check your transactions at: Ropsten.etherscan.io

- Merkle Root :-

→ So Merkle Root is 32 bytes actually. or we can say that is sizes of 32 bytes.

It represents the summery OF all the transaction data

→ The Advantage is whenever ~~we~~ transaction occure So rather then if you want to check whole transactions So rather then downloading the whole transaction process or whatever whole transaction is that you can just with the help OF merkle root you can get to know whether your transaction is successful or not. like rather than Downloading whole link OF data you can just download the merkle root Hash you can get to know about this with the help OF this 32 bites you know a data you can get to know whether your transaction occured or not.

- Advantages :-

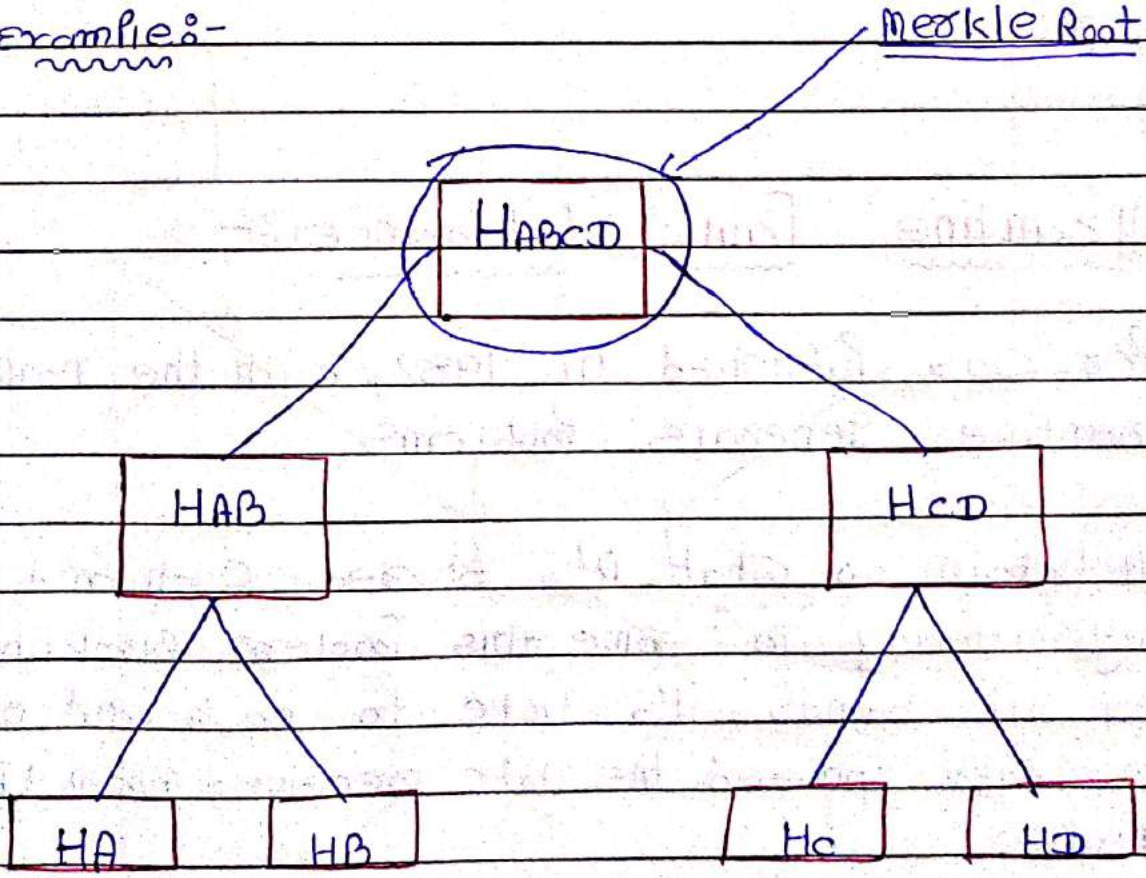
→ It is easy to check if transaction has been you know Tempered with or not.

→ It uses fewer Resources to generate Hash or it's uses Fewer Resource's to comply, or give out the result.

→ Easy to verify if it's specific transaction has been added to the block or not.

→ Tamper Proof.

* example:-



* Tree *

A merkle Tree allows for users to check that specific transaction has been included in Block without having to Down load the entire Blockchain, IF you want check whether your transaction occured or not you can do that you can use a protocal the name of that protocal is SPF (simplyFied Payment verification) with help of that protocal you can get to know whether your transaction occured or not

- Byzantine Fault tolerance :-

→ Paper was published in 1982, with the name of Byzantine Generals Problems,

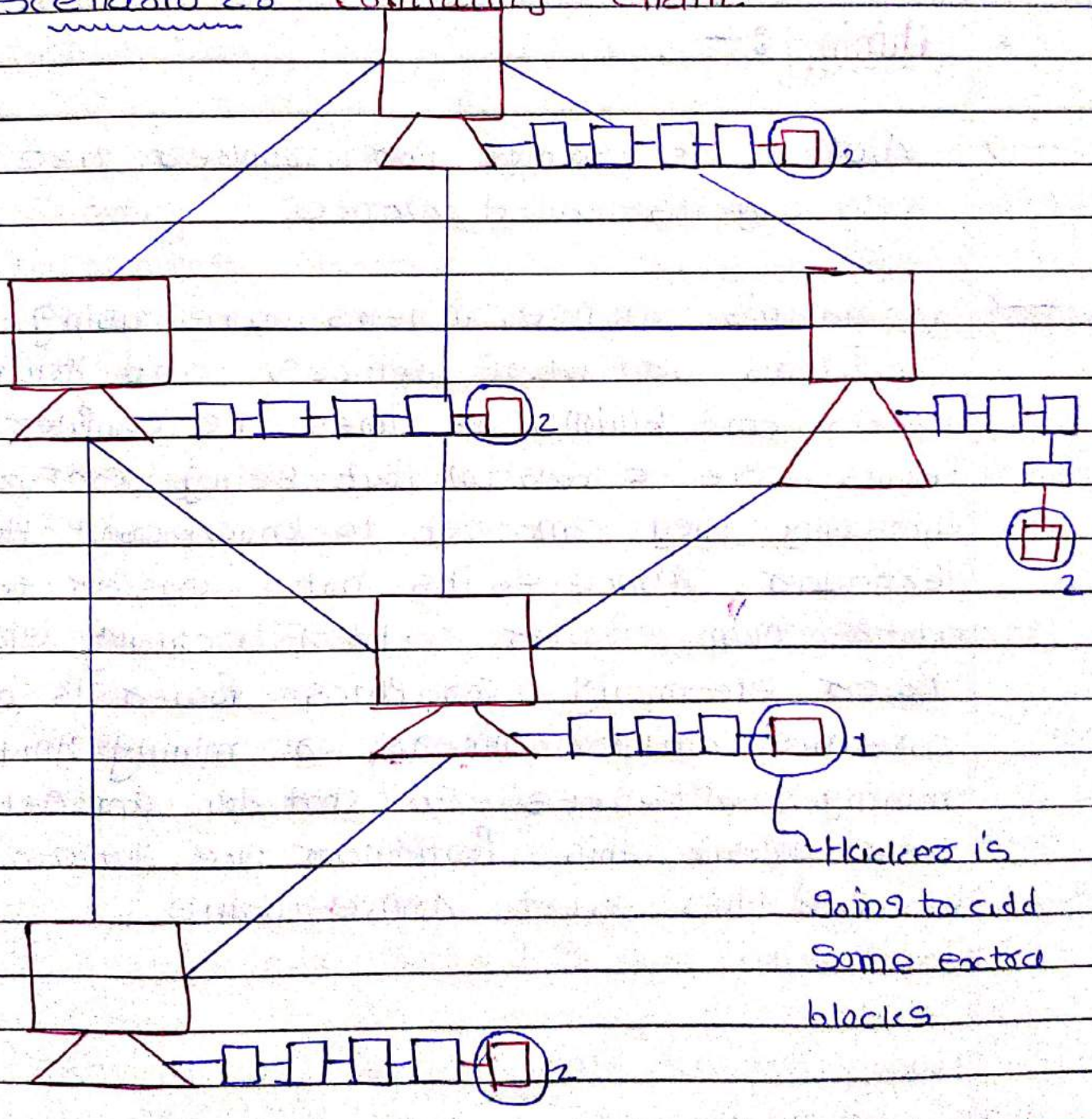
→ Blockchain do that it's shared each and every thing actually To solve this problem Blockchain does it sends it's vote to each and every one also shared the vote received from the other.

→ 1/3 mechanisum use.

• Consensus Protocol :-

→ Scenario 1 :- Attacker adding extra blocks

→ Scenario 2 :- Computing chain.



→ This whole scenario is also called PoW (Proof-of-Work) consensus protocol is relies on PoW and PoS (Proof-of-Stake) actually.

* **Mining:—**

→ Nonce is stands for number use once that's why it's called Nonce.

→ To find this Nonce, miners are using a lot of computers or lot of devices and you know millions and billions of times the computer computations are calculation that being conform then only they can get to know about this particular Nonce so it's not a easier task a lot of man power a lot of actually electronics power, electricity, graphics power is being consume while miners or mining you know mining softwares so that you can get to know about this particular like you can get to find this exact Nonce value.

Cryptocurrency :-

→ Cryptocurrency is a digital assets design to work as a medium of Exchange that uses strong cryptography to secure financial transition,

→ In Short, Cryptocurrency is an Alternative currency, It is not under control of any government organization, It's oppose them, it's don't realy on their guide line it is not dependent on their guideline actually.

→ Cryptocurrency is a type of alternative currency, which uses Decentralized control.

→ So your Bitcoin is a type of Cryptocurrency.

→ The Beauty of Cryptocurrency why Bitcoin gets so much booming responses that,

Ex:- 1 $ = 76 ₹, So if you have 70₹ and if you want to cash it out in dollers you will get 1 $ only so it's ocward.

→ So what is type of Problem what happend, the Satoshi nakamoto he created

the Bitcoin, what cost if in India The Value of Bitcoin is 6000$ approximately Then even in USA the Value will be Same.

→ IF you want to transacte From PayPal, Imps, NEFT, Paytm, PhonePay, whatever the digital wallet you have, IF you are using them you know charging something 1.8%, 2% of you total currency To transit your money From your wallet into your bank account.

→ But in case of Bitcoin you know there was no charging like whatever currency you have you will get it IF you are in India, IF you are having one Bitcoin even though in Us ~~same bitcoin~~ you will get the same bitcoin you can cash it out there is no brokerage charge or what so ever so that's why it is complatly decentralized and a with the help of Bitcoin, always Satoshi Nakamoto he tryes to decentralized the whole currency he tried to maintain a level of currency which can be used in almost all Part of the World so that's the Beauty of Cryptocurrency.

→ Under that crypto currency there are three sub division

1. Technology (Blockchain)

2. Protocol (Bitcoin, Ethereum)

3. Tokens

Our Blockchain is a type OF Technology OF Crypto currency

[www.coinmarketcap.com]

- Coins VS Tokens :-

→ Tokens needs one OF this PlatForms (Bitcoin, Ethereum, Solana, Polygones) to rely on or It requires PlatForm OF coin to exists.

→ Bitcoin is a type OF Protocol which work on a technology called blockchain.

→ Coin is a crypto currency which operates independently of any other platform, like Bitcoin, Dogcoin., They don't rely on any one they don't dependent on anyone, They have even own set of Technology, They have even their own set of Blockchain.

→ Token is required a platform of coin to exists.

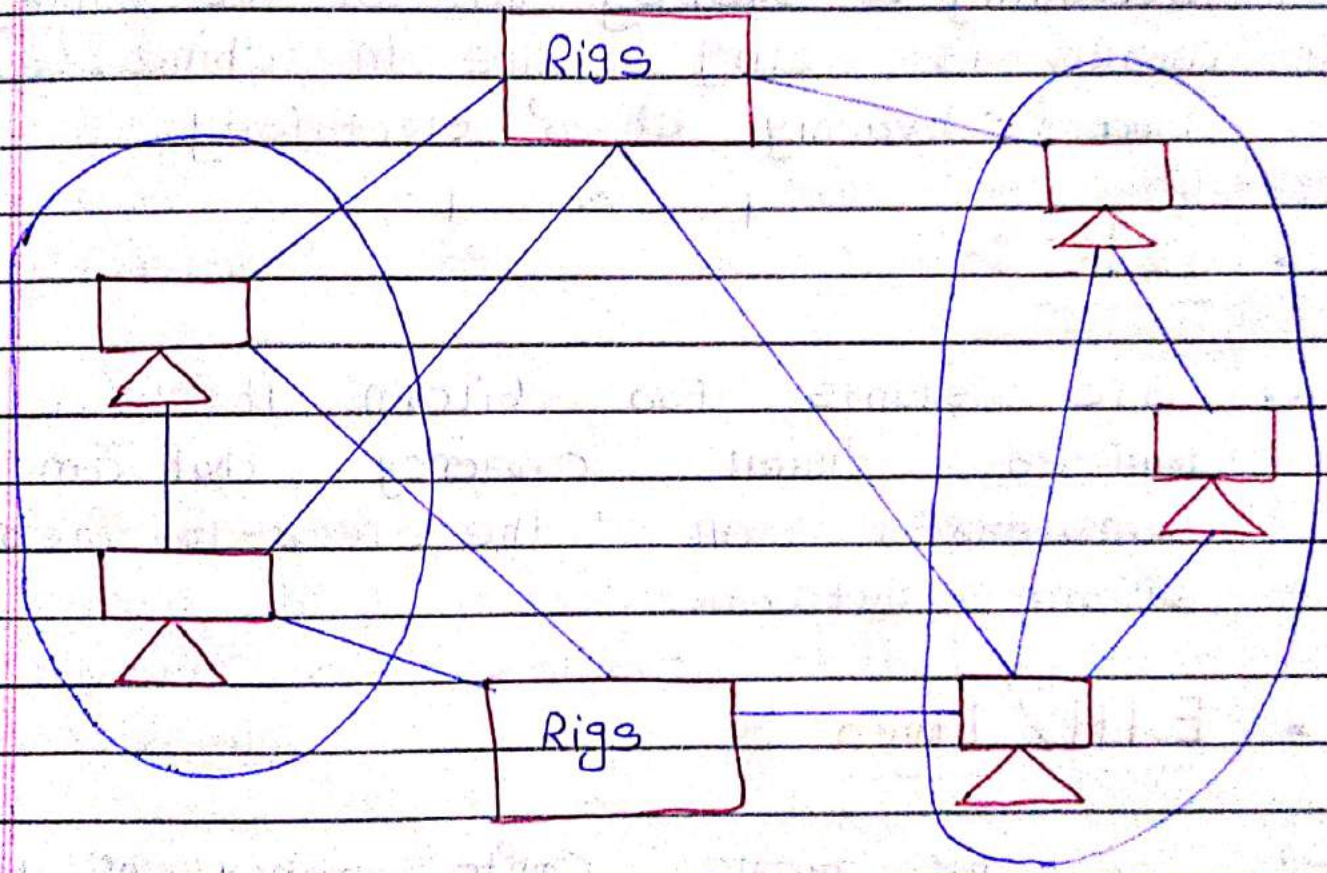
→ Smart contracts, They defines the token which run on the Top of the Protocols, This tokens are being defined by Smart contracts and they run on the Top of Protocal whereas is defined by Protocol it's self.

→ Remember Ethereum having a lotes of ~~coins~~ tokens but Bitcoin having don't any type of tokens.

→ Again Remember coin is a Unity it's a Protocal which have it's own set of Block chain, It's completely independent But Tokens need a coin, Token need a platform of coin to be an existantce so that's the defination

→ Blockchain.info websites.

* Mining Pool :-



→ BTC.com
→ AntPool.com
→ slushPool.com

→ Very First headache of all miner is to Deal with Electricity.

→ What miners do actually they started mining or they shift them selves they create their mining pool, country where the electricity is very much cheaper

→ According to survey 81% of the mining is work is being done in china. because china is having cheap electricity.

X

- **BTC :-**

→ BTC stands for bitcoin, it is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.

- **ETH / Ether :-**

→ Is the native cryptocurrency of the platform ethereum. Ethereum is a decentralized ledge technology (Blockchain)

- **DeFi :-**

→ Decentralized Finance (DeFi) is an emerging financial technology based on

blockchain. The system removes the control banks and institutions have on financial services, assets and money.

* NFT :-

→ NFT stands for non-fungible token. NFTs represent a digital asset on the blockchain which are unique and represents ownership by someone.

* Gas :-

→ Gas refers the fee, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain.

* Wallet Address :-

→ Your wallet address is a unique string of numbers and letters (also called a public key) that people can use to send you crypto currency.

* Smart Contract :-

→ Smart Contracts are simply Programs stored on a blockchain that run when predetermined conditions are met. They are self-executing code.

* Peer to Peer (P2P) :-

→ Something is called P2P where two decentralised individuals interact directly with each other, without intermediation by a third party.

* Altcoin :-

→ Altcoin simply means each and every cryptocurrency other than bitcoin.

* StableCoin :-

→ Stablecoins are cryptocurrencies where the price is designed to be pegged to a crypto currency, Fiat money, or exchange traded commodities it stays Stable.

→ Blockchain is changing the way we control over data. It is directly changing the dominant Application dilemma of control over the data by the central parties and puting the range in the hands of the people who are participating in the system.

→ over current world is dependent over trusted parties.

→ what if the trusted parties are not trust worthy
what if the referee in the Football match is biased.
what if the data hendle by the email providers or Social media applications get leaked or attacked.

→ The answers to all this questions comes with technology like Blockchain.

→ Blockchain started as an open source public solutions and the inclination now shifting towards interprise adaption.

→ Blockchain Technology is not the crypto currency, The digital currency is only one of the usecases for Blockchain Technology.

1. Distributed ledger Technology

Q What is DLT.

→ ~~DLT have been introduced in these people is used to keep~~

→ DLT have been used in Accounting in Asian history these people is used to keep record of transactions of items or Antities which are been traded across each other.

→ DLT became game changer back in 2009. with commencement of ~~ear~~ Bitcoin.

→ bitcoin introduced us a Peer to Peer bash ledger technology which can be utilized distrupt multiple markets.

→ "It is a "Database that is Shead accross mutiples Computers in the world" The Primary aim of DLT is to reduce the risk of Central Storage which we can see in different organization and government structures

→ Dlt is the umbrella term to describe any system that distributes data across multiple computers. 34

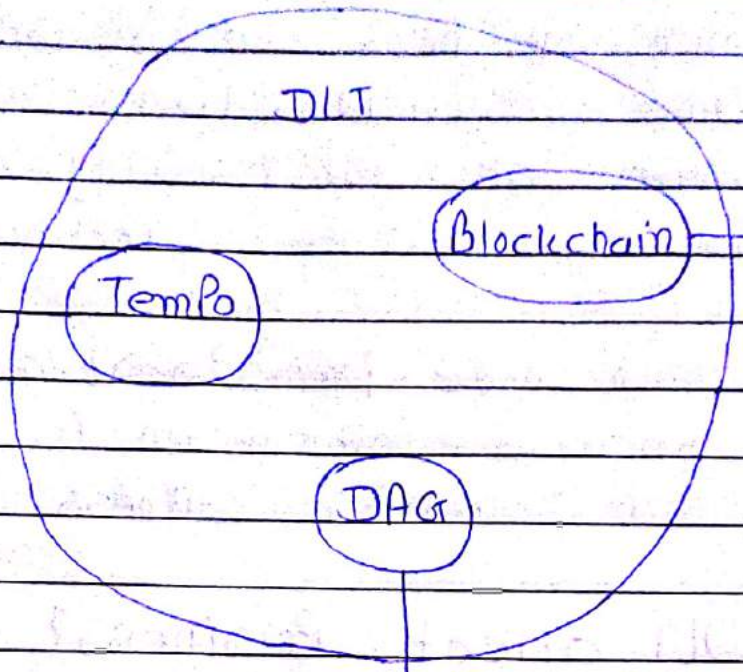
→ There are several types of DLTs like Blockchain, Tempo, DAG etc.

— Tempo is DLT which is based upon subsets of ledger by subsets we want to say that Tempo is based upon that conducting the transaction will only store those transaction.

- DAG is known as Directed a cyclic graph on the DAG we work Principle of only transations we don't have any concepts Blocks so we verify the transaction by making up the new transactions ahead of it.

→ All Blockchains are DLTs but all DLTs are not Blockchain. It's more of synonymous to Google and Search engine where Google is a specific type of Search engine.

→ Redix Quota and IoT are also some other different implementation of DLT's and all this are not Part of Blockchain.



- Benefits of DLT :-

- DLT have the potential to speedup the Transaction because they remove the central authorities or middle man.

- Apart from that DLT also have the potential to reduce the cost of Transactions to as fees by taken middle man is removed from the process.

- DLT is much more secure than the Tradition Technology because the Each node

of the network holds the record. Therefore creating the system that is more difficult to manipulate or successfully attack the compare to the central Technology.

- DLT is much more transparent way of handling records because information is shared between different nodes and its witness across world

• How DLT affect Business?

→ DLT creates a Permanent, decentralized, global, trustless ledger of records.

→ one of the primary example of disruption created by distributed LT is the Cryptocurrency whenever a new cryptocurrency is created the cryptocurrency is not their product its of like a market for distributed ledger technology they are creating the new economic system where the Tokens are the units of exchange and the DLT detects the rules of each participants in their economic system.

→ It is accessible any where in the world and do not require trusted 3rd Parties to carry out the transactions.

- Let's divide the effect of DLTs over business into 3 major Components :-

- Transforming internal Processes and Operations.
- Transforming Business Models.
- New opportunities

1. Transforming Internal Processes

→ The include the DLTs Potential along internal Processes and interactions within the busine ss value network. It can be in the form of :-

- Distributed Payments cutes out the middle man and their additional charges. Moreover they also reduce the Administrative Coust. For ex :- IF you are doing the clearing settelment of important exports using smartContracts. There you can remove the

middle man also reduce the fees, carried out by the middle man.

- **Asset Tracking**, DLT can Prominetly Audit stored the Audit Trail OF data, Therefore It can reduce the cost OFor maintaining Audit Sub trails. For example:- IF you are doing a tracking For the Ownership OF goods in supply chain, There you can maintain the Audit Trails Even Walmart is doing such a System at their end.

- **Data Sharing**:- This one is the major driving Force because we required exchange OF data without any Cost OF running Third Partie services we also need to maintain the security and integrity OF data For example:- IF we do a kyc OF Rubic records over DLT

- **Identity Management**:- there we required the reduce the redundancy Storing the users contains identities. We also required the to reduce the Cost OF doing Same Process multiple times. Example:- IF we run a background check or Academic credentials verification Process using DLT.

2. Transforming Business Models :-

→ This includes looking beyond the technology and including the value potential related to new types of customer interactions and innovation ideas for business models :-

Sectors :-

- Customer Engagements.
- Micro Transactions.
- Creating New Markets.

- If we create the economy with a integrate insentives for the participantes then the customer engage ment much more higher than the traeditional Technology.

- current processes only allow customers to do the full transaction they can not gone by micro properties or pay for what is actually consume at base end.

- CVM could be related to provizioning assests on the blockchain which can be related to theseal assests in the physical could this could be privously liquidated assets such as unused production capicities or as a secondary

market for raw ingredients, parts, goods or other services.

3. New Opportunities :-

→ DLT's might create new opportunities which are neither part of the core value chain nor the core business model:

→ Funding
→ Access to Data
→ Crowd Collaboration
→ Self Governed organizations (DAO)

* Realization of Challenge :-

- Digital disruption has pushed more than half of the Fortune 500 out of business since 2000, and adoption of DLT is likely to aggravate this trend.
- Adoption of new digital technologies brings pressure on profitability through competitors as everyone wants to deliver faster and better products.

- Some businesses runs thaough middle men and cutting them out would bechallenging.
- Risk of being decentaalized over token economies might Effect makct shaaes for businesses.
- Finally, innovator's dilemma.

Q Difference between DLT and Traditional Technology.

→ DLT	IT
- Follows Distributed Architecture.	- follows client-seaver Architecture.
- Permissioned oPeaations - Rubuic DLTs only aeed and waite cae available	- CRUD oPeaations aae available.
- Suppoat s built in integaity	- Additional component s aae neceSSaay tobuild integaity.
- Built in veaiFication oF data i's available.	- Additional Components aae neceSSaay to build veaiFication.

- Transparency of data is available.	- Indirect transparency of data is present.
- Control and Trust by the Participants.	- Control and Trust by a central server.

2. Introduction to Blockchain :-

* What is Blockchain ?

→ " Blockchain is the technology. Bitcoin is merely the first main stream mani-festation of its Potential".

→ Blockchain is a digitized, distributed database technology available over a Peer to Peer network or another words we can say it's a distributed ledger for all the records or transactions.

→ Blockchain says initialized Devised to Power Bitcoin, but it has much more significant use then releasing the Crypto currencies.

→ every blockchain which is available in the market is Primary built from three core technical functionalities.

1. Private key cryptography :- ECC
Example :- Bitcoin and Ethereum RSA
are working on ECC
Algorithms which is part
of ECDSA umbrella
ECC Algorithms states
a curve where mirror
points are chosen as a
key pair.

2. P2P Network :- • Torrent Network • System of Records
— P2P system is devised in such way that the
network participants do not need to trust cent
ralised server, they are connected and
create trust through the consensec.
(• Hashing, Hmac, Shake Algorithms)

3. Program (: The Blockchain Protocol) :-
→ Protocols are used to define How your
chain will operate, Ex :- The Bitcoin defines
that a new block will be added about every
10 minites, a reward will be destributed for confirm
ation of the blocks and the block size could not
go upto 1 MB. other Blockchain haves some diffe
rent Protocols, some Blockchain mights also include
Protocals For assets and date.

Real World Analogy for Blockchain :-

→ Transparent Bank Vaults.

- Traditional approach is that you go to the Bank with your Vaults key to access you positions only you have the access to you Vault through key and you can't see what is inside the other Vaults, now imagine a situation where all the banks are Transparent, you can see actual components of each wall but still you have only access to your own Vault same is the case with Public Blockchain where you can see everything happning in side the networks but you only have a access to your account, tokens and keys.

→ Bank account Statements.

- which are duplicated of hundred of computers. everyone records, everyone transaction you make thus no one can temper with your records. another example could be Book enology in a library, People come to the library, to borrow a book, if someone removes a page from the book, then the People landing a book after the cupoet can identify that the book has been tempered with and the pages missing from the book. and this example the book will

act like Blockchain every Page inside the book like a book and the text on each Page is like transactions, some other example could be a Google document or a SpreadSheet shared between mutiple users, where your work book is a blockchain, each work sheet is a block and linked with next work sheet and the dates in your workshit are like your transactions.

— A Street Soccer Game.

— Imagine a massive Vault system from a bank.
— The Vault is Filled with rows of deposit boxes
— Each deposit box is made up of glass, allowing everyone to visualize the contents of the deposit box, but only have access to their Vault.
— When a Person opens a new deposit box, he/she gets a key that is unique to that box.
— This is the Fundamental concept of Cryptocurrencies based on Blockchain. Anyone can see the contents of all over addresses.

• Why Blockchain is Web 3.0 ?

→ The initial distruption started back in 1994 when the internet came into being This was called as Web 1.0 by the year 2000, Tech giants like Google, facebook, amazon emerged and let to the 2nd distruption known as Web 2.0 This distruption still had a Problem of centralized control now new technology like Blockchain is Trying to Put the Power back in the hands of the uses Why is Blockchain known as Web 3.0 first of all there is no central Point of control in Blockchain as compared to the traditional services, if you are going to use email services your bond to trust Google and microsoft to make sure that your emails remains Private, if you are going to use Storage Services your Puting your trust in Google or Dropbox to keep your data safe.

→ We have seen how the confidentiality of data and hacks have been Significant cause of consone for this central organization by using Blockchain we are removing the trust from the central Authorities and third

parties and making sure the data is protected and made available through consenses of the participants.

→ The second reason for disruption is the account of ownership once the data is over Blockchain is immutable and any body can verify the and ordead the data.

→ Blockchain can also store data with digital signature which provides the ownership of data.

→ if some other person toys to upload the same data in the future then varifie's can see the History of the data and state the ownership of rights. this can help to reduce land and pattent disputes.

→ As Blockchain is based upon secured and proven cryptographic Algorithms the chances of hacks and data breaches are eager more over protocols like consences and permission base services almost make blockchain principle.

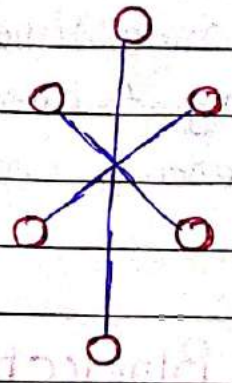
→ This security parameters also form a reason

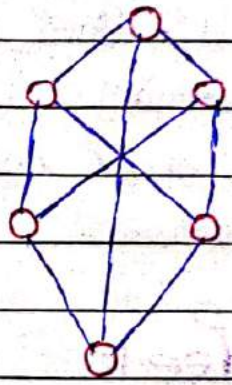
for calling Blockchain as Web 3.0.

→ Most of the attacks over Blockchain till now have been due to some implementation issues For example one of the crypto ~~currency~~ exchange servers hacked where the private key of the user who are being stored at a central server attackers where able to perform transfer of crypto currencies using those private keys, more over the ownership of data helps in the diduction of Tests and data frauds.

→ The fourth reasone is uninterupted service Blockchain is available through Peer to Peer network so any body who is connecting to the Blockchain has node running with them on every nodes stores the complete data associated with blockchain, For example you have 100 nodes connected to a blockchain network, now lets take a sample that 5 of those nodes goes down but you still have 95 nodes which will Provide the data and Guranties the availabilety of Services This are the reasons why blockchain is called Web 3.0.

→ No Central Point of control.
→ Ownership of Data.
→ Reduction in Hacks and Data Breaches.
→ Uninterrupted Service.



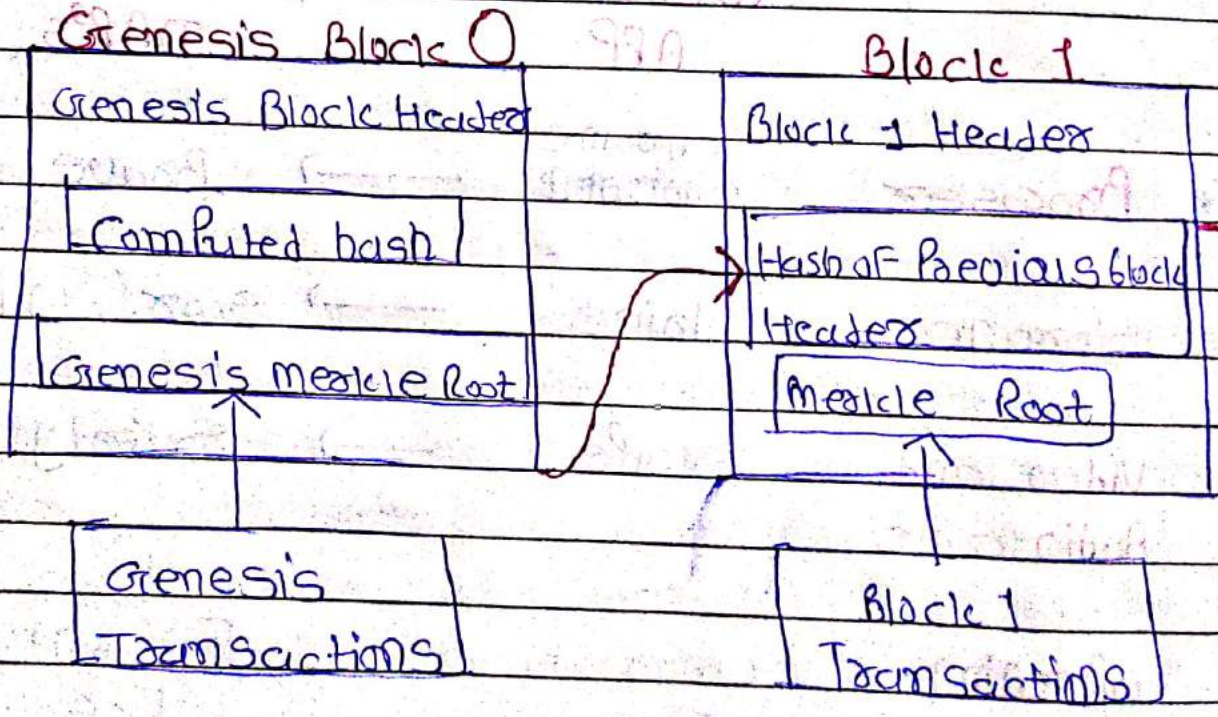


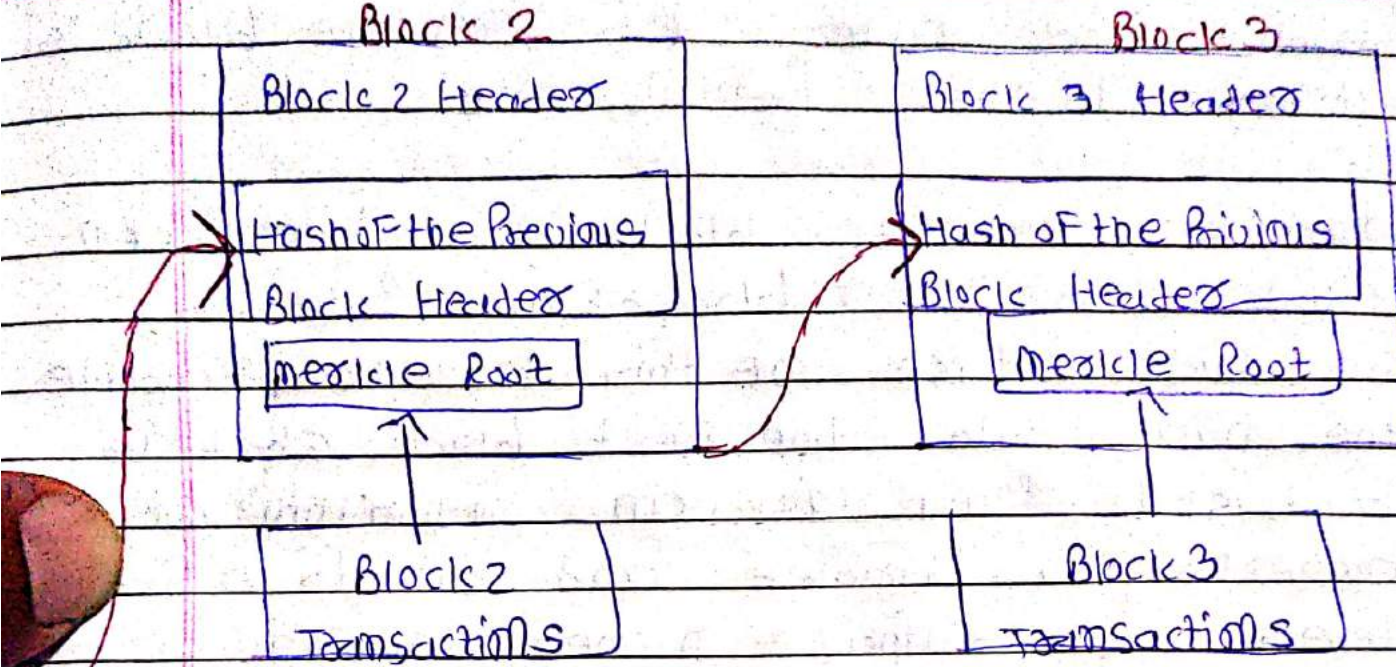
	Web2.0 APP	→	Web3.0 DAPPs
* Browser	~~Chrome~~ Chrome	→	Brave
* Storage	Daive	→	Storj, IPFS
* Video and Audio calls	Skype	→	Exposty
* Operating System	android, IOS	→	Essentia.one, Eos
* Social Network	Facebook, Twitter	→	Steemit, Akasha

* Messaging — Whatsapp → Status
* Remote Job — Upwork, Freelance → Ethlance

→ All the services mentioned here are currently running and trying to change the Echosystem in a way, we interact and shared the data

* Peek inside Blockchain :-





→ Whenever a blockchain is getting started, you have a block zero, which is also known as a Genesis block. This Genesis block holds all the parameters related to blockchain behavior.

→ Genesis block will define what your blockchain will do in its running time. This will set your block time, block size, hashing algorithm and also design your cryptocurrencies.

→ Genesis block is a special kind of block which is not linked with any previous block. You can see in the diagram how

each block after the genesis block is linked to the previous one.

→ once the genesis block zero has been filed with the blockchain protocols, we take a hash of this block and include the hash into the next block. What is a hash? Hash is an algorithm which converts a variable and data to a fixed length of alpha numeric string.

→ For example, a hashing algorithm SHA two five six generates a fixed length of 256 bits of hash and input of 1kB or 1GB both will lead to 256 bits of fixed length hash. As you can see in the diagram, we have linking established from one block to another. This linking shows that the hash of the previous block has been stored in the next block. Apart from the hash, we also have market note and transactions. All the transactions inside the blockchain are grouped under blocks.

→ For example, in bitcoin blockchain, after every ten minutes, a new block is opened up

and the network waits for all the transactions coming in the for that ten minute period and stores them under the block. Apart from transactions, blockchains also stores a merkel route, which is a single source of truth for all the transactions.

Blockchain Characteristics:-

→ We know that every block is connected to the next incorporating the hash of the previous block. This linking of block forms the chain. After the addition of block into the chain, the validation and the confirmation of the blocks are carried out by the miners. In elementary terms, we can say that the miners inside the block chain are doing some logical calculations or playing a game trying to validate and confirm the blocks over the blockchain.

→ The miner who wins the game gets the rewarded some reward and all the miners shift to the validation to the next block.

→ For example miners receive 12.5 bitcoins in Bitcoin blockchain and two Ethers in Ethers in Ethereum blockchain.

→ Blocks are created in chronological order by using different cryptographic algorithm which means that's nearly impossible to delete and modify data over the block chain.

→ The immutability of the blockchain is also maintained using consensus algorithm, which makes sure that all the transactions inside the blockchain are validated and only added once the consensus has been achieved. This consensus is carried out by the node, as we mentioned that all the blocks inside the blockchain are added in a chronological order.

→ This means each block has a time step associated with it. So we have a complete history of th blocks maintained. If my blockchain is running on 1,00,00th block, then I can still trace my blockchain back to the first block and see how everything originated. This is also true

For Bitcoin blockchain, there we can track back to see how Satoshi Nakamoto originated the entire Bitcoin blockchain back in 2009. Let's summarize that blockchain is. Blockchain in general is a distributed storage of information which is distributed and available over a Peer To Peer network. Blockchain is based upon Cryptographic algorithm and runs Consensus algorithms for Security and immutability.

→ Every new block added inside the blockchain is linked to the previous block using the block hash. All the blocks are present in chronological order and every participant over the network can view all the transactions.

→ If we want to define blockchain, in other words, we can say that "blockchain is a digitized, distributed, consensus based, secure storage of information protected from revision and tempering over a peer to peer network. That's how, in a single definition, we can summarize Blockchain."

History of Blockchain :-

Bitcoin Beginnings :-

→ The First known attempt at crypto currency is occured in Netherlands in the late 1980's in the middle of the night the Petrol stations present in the Remote area who are being waited for cash and the operations who are in happy about the situations but the Petrol stations had to stay open over night so that the Trucks could refuel.

→ Some one in Netherland had a bright idea of Puting money into the Smart cards So the electronic cash was borns, Trucks drivers change given this cards instead of the money and the stations who are more safer from the robberies.

→ David chaum and american crypto graphers who was already investigating electronic cash came to know about Netherland situations and decided to move to the country, in the late 1980 coming with CCI organization, he started Digicash, which was the First internet money invention unfortunatly due to some mistakes his company Filed for bankruptcy around in 1998

→ apart from digital currencies other ways to safeguard information these also being introduced. a structured similar to that of blockchain has been appeared in mentioned in a research paper which was published in 1991 by haber and stornetta, with a topic how to time stamp a digital document, according to that paper a client sends a document for time stamping to a time stamping server, and the server signs a document with a correct time stamp also The Server could link the document to the previous document.

→ The pointers pointed to a specific data and not the location of the document, so the data is become change the pointer should become in valid, it insure no one could tamper with a data that had once being pass through the server.

→ learning and improving the previous mistakes Satoshi nakamoto published white paper bitcoin peer-to-peer electronic cash system. The paper claimed had a solution to the double spending problem in digital currency, using peer-to-peer network, The main aim of the paper

was to build Peer-to-Peer version of digital currency that would enable People to spend it directly without it going in a Financial Institution. It was a huge innovation that allows the users to Transact directly relying on the third Parties.

→ In the year 2009, the digital cryptocurrency bitcoin was made available by satoshi, he release the concept of Genesis's block with 50 coin which letter became Part of the Bitcoin Peer to Peer Network. Bitcoin also bought the idea of blockchain, around 2014 attention shifted Form bitcoin to blockchain.

→ The World realize that the blockchain can be Seperated Form the currency and can be applied to various other use cases.

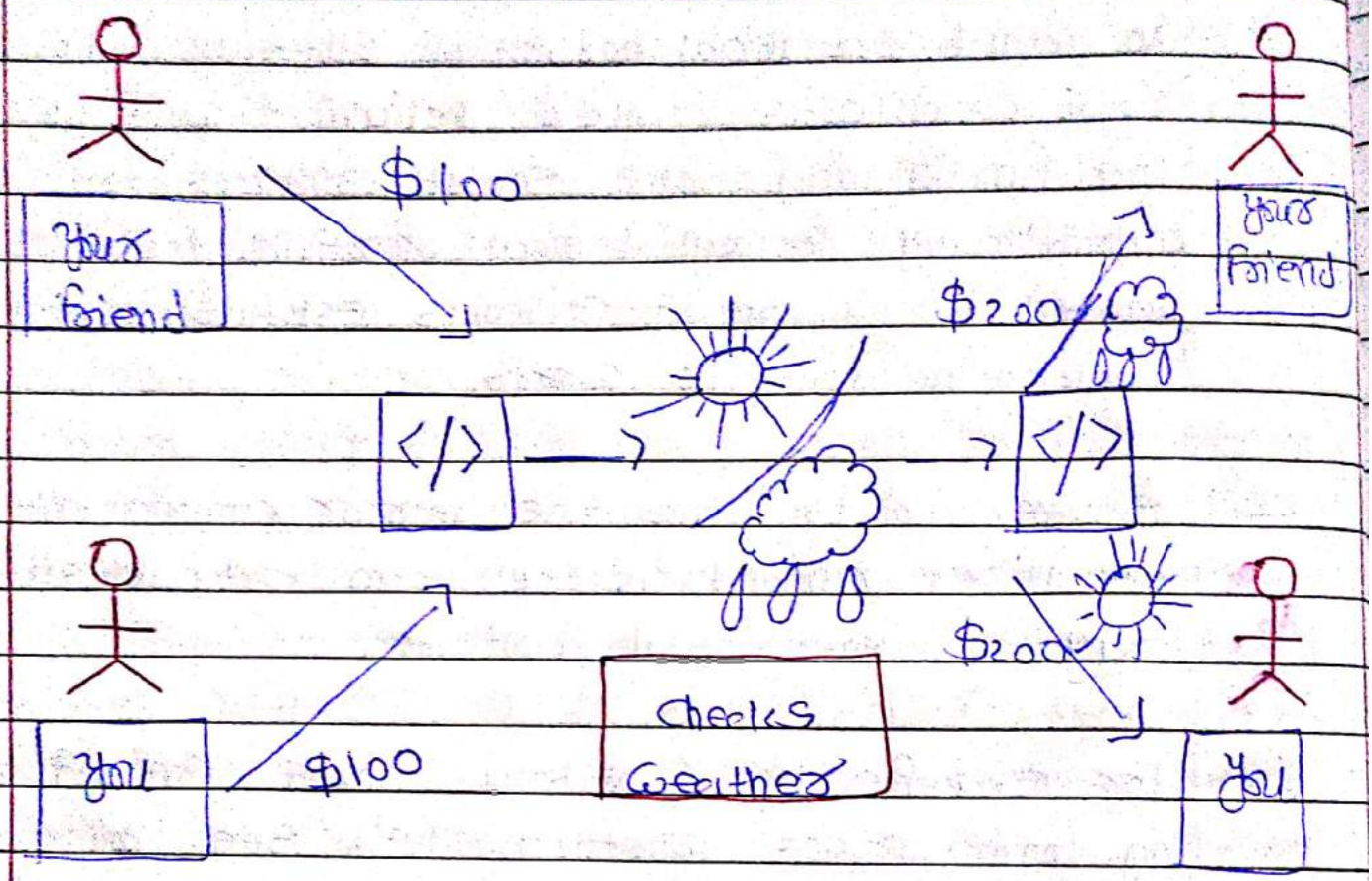
* Rise of Smart Contracts :-

→ Soon a Developer name Vitalik Butarin, who was the initial contributors to the Bitcoin Codebase, became Frustrated the limitations of the Bitcoin in the year 2013, He decided to start his own

chain by learning and fixing the limitations of Bitcoin, he launch the initial version of Ethereum in the year 2015 which was called Helium. It was started the functionality of the smart contracts that can automatically perform logical operations this was basted on a set of criteria's establish over the blockchain in the words,

→ Smart contracts are the mirror commitment for the legal contract as they can act in a similar way as your legal contracts,

→ For example you created a smart contract to bet on tommorrows whether. let's see you and your friend are going to bet with this contract both of you will predict and upload your gas through the smart contract with the beting coment over the blockchain where it becomes immutable the digital currency send to the contract will be permenantly held itill the next day onces the corresponding day arrives the smart contracts check whether you have win the prediction of whether bet or not if your prediction is correct then the smart contract will automatically disperse the winning money to your account



* Time line *

1990s origin — the concept of distributed computing has been around since 1990

2009 Satoshi Nakamoto created Bitcoin — 2009

& introduced the concept of a block chain to incorporate a decentralized ledger maintained by enonymous consensus

2011-2012

Cryptocurrency (Bitcoin) transfer and digital payments system, where top industries started making their financial transaction using Bitcoin and the other popular currency

2013-2014

The deployment of crypto currency in application

Transactions ($) related to cash

2012-2013

Financial markets and applications using blockchain beyond cash transactions small but disrupted applications came into being like upload of kyc documents or kyc processes over the blockchain

in 2015, the Smart Contract (ethereum VM) Chese introduced with ethereum blockchain, and that opens up the vast innovative and effective way of creating Decentralized applications on top of the Blockchain

2014-2015

In the same year other blockchain also came to the series which chose more towards the permissioned blockchain network solutions, like Hyperledger and R3 model.

2015-2016

Application

Market Consolidation and further sub-development

2016-2017

How Blockchain Works?

→ Let's imagine that there are ten People inside a room and they decide to create their currency for any exchange between them. Apart from transacting they also need to have of transparency for all the transactions taking place.

→ They need to be aware about the flow of the funds between them so that disputes regarding the same can be resolved in the future. That is why they decide to appoint one Person to keep a list of all the transactions which are taking place between the members of the group.

→ Let's call this Person Dave. You can see in the image that Dave kept a record of all the transactions happing in the room in a notebook.

→ All the transactions from the beginning were noted down. For example, Alice gave three coins to Carol. Carol gave five coins to Chuck. Chuck gave three coins to Eve, and finally Eve transferred one coin to Bob. These recorded

down in a note book, This notebook acts as a source of transparency and verification for the group. Once, out of the group of ten people, there is one person let's call him chucle, who decided to steal money from the group.

→ To accomplish that, he changed the entries present in the notebook one night, he got hold of the notebook and modified his entry to somebody else.

→ For example, he burned the entry number three in the notebook from chucle gave three coins to Eve to cook gave three coins to Eve. Thus making sure his account is not deducted for the transaction.

→ Dave notices that someone has messed up with the notebook and he decided to protect the entries. He created a program called a hash function. How does a hash function work? "A hash function converts a variable length of data to an alpha numeric string of a fixed length"

→ A hash Function always generates the same size of data for any input size. For example, Sha Two Five Six is a known hash Function which is being used in bitcoin and ethereum. Be it 1 input data or 1GB of input data. SHA 256 hash Function will always generate 256 bits of output hash We can see the example of hash Function in action as, Example like Attack, can't Attack and can Attack have a Fixed length has through the SHA 256 has Function. Even a single bit of changes in data will lead to a different hash result,

→ In other words, We can say the hash acts like a digital signature for the data. If the data change, the hash will also Change.

→ Dave added the records of hash inside the notebook in such a way that after each transaction he has of the transaction. The new notebook entries look like, a'

→ When Alice gave ten coins to Carol, a hash of the same is denoted below the transaction. The same happens for the rest of the transaction s or any other future transactions. If check

tries again to change the entries inside the notebook, then the has For those entries will be different and they could be able to verify the modification entries. Although the hash Function has been Put into effect, Chuck somehow learned about the hash Function and decided to manipulate the entries again. He took the notebook on night and changed the transactions as well as the hash OF the transactions, For examples you can see in the image he changed the transaction, as well as the hash OF the transactions, For example, you can See in the image he changed the transaction. Carol gave Five coins to Chuck. To Carol gave eight coins to Chuck So that his account has more coins. He also recalculated the hash OF the other transactions and modified those in the notebook as well.

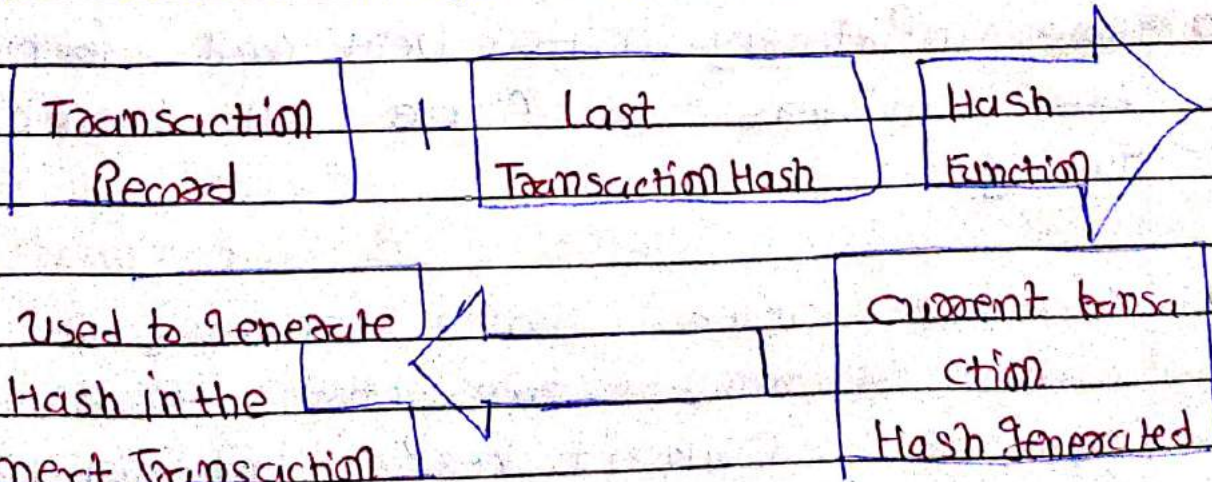
→ By changing the hash, he made sure that if Somebody tries to verify the transactions by using the hash function, then the transaction gets validated. Dave noticed again that Some body has Fiddled with the notebook, Frustated with the attackers.

→ he decided to complicate the records in such a way that each hash is generated by combining it with the previous hash. So each transaction record is added with the last hash transaction and pass through the hash function. The resultant hash is the current transaction hash.

→ It will be used to generate the hash for the next transaction in the notebook. Each entry in the journal depends upon the previous entry.

→ If the attacker tries to change any record in the notebook, then he needs to replace all the entries inside the note book.

→



→ Chuck wanted more money, and he spent the whole night counting all the hashes.

→ Finally changing all the hash entries accordingly. He replaced all the hashes with the corresponding cheat hashes.

→ Dave did not want to give up. He decided to add a random number after each account. This number is called "nonce" nonce should be chosen so that the generated hash ends in two zeros.

- Now, to forget transaction s, chuck would need to spend hours cracking once for each line.
- more importantly, it's very hard for even the computers to figure out the nonce quickly.
- Sometime after, Dave realized that there were too many transaction records and that he couldn't keep the diary like this forever, After reaching 10,000 transactions, he converted them to a one-page spread sheet. Dave checked that all transactions

are right.

- Dave shared his spreadsheet with over 10,000 computers located globally.
- These computers are called nodes. Every time a new transaction occurs. It has to be validated by the nodes.
- Once every node has received / checked a transaction there is a sort of electonic Vote, as some nodes may think the transaction is valid and others believe it is a fraud.
- Now, if Chuck changes one entry, all the other Computers will have the original entries. They would not allow fraud entries to occur.

Summarising :-

- This spreadsheet created in the example is called a block
- The whole chain of blocks is collectively called Blockchain. Every node holds a copy of the Blockchain. Once a block reaches a certain

number of approved transactions, then a new block is formed.

- The Bitcoin Blockchain updates itself every ten minutes.
- As soon as the spreadsheet or ledger or register is updated, it can no longer be changed. Thus, it's impossible to forget it.

* Wallets, Digital Signatures and Protocols:-

* Wallets :-

- A blockchain wallet is similar to a digital wallet that allows participants to manage their cryptocurrencies.
- A wallets lets the users generate the private key and public address.
- The Private key is used to send the transactions and Public address is used to receive the transaction.

- No visible records of identity about who did what with whom, only the address of a wallet is visible in the transactions.

- Types of Blockchain wallets are :-

- Paper wallet :- Private keys stored on a piece of paper

- Web wallet :- Present on internet; can be accessed through URL

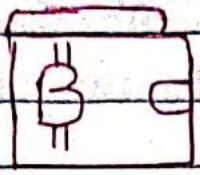
- Mobile wallet :- Application on mobile device.

- Desktop wallet :- Software application.

- Hardware wallet :- Hardware device used for storing the private keys

- Physical wallet :- In the form of a smart card

→ Blockchain wallets consist of two major things:-



→ can hold multiple addresses

Private key

→ Acts as Digital signature

→ Used to sign and send the transactions

Public Address

→ Used to receive the transactions

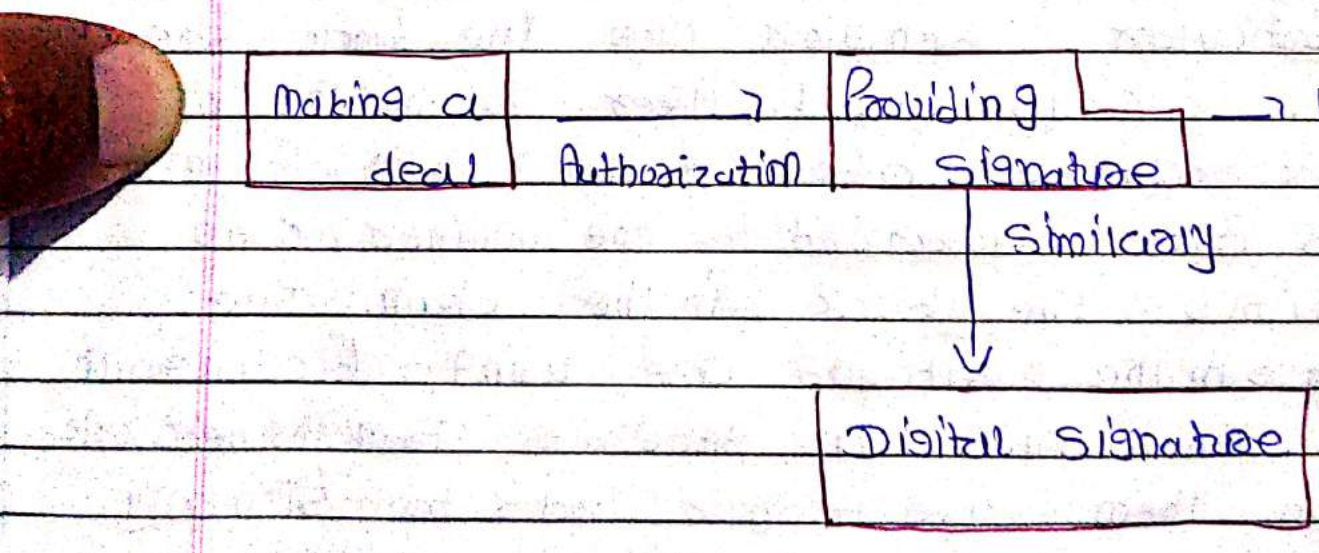
→ Make sure you never give your Private key to any one.

→ wallets help you to interact with Blockchain.

Digital Signatures :-

→ DS verify whether you are authorise to interact with blockchain or not.

- Digital Signatures similar to real signatures are a way to prove that somebody is who they say they are.
- Digital Signatures use cryptography which is more secure than handwritten signatures.



- The Private key is used to sign messages digitally.
- The recipient can verify using the Sender's Public key.

- Every transaction that is executed on the blockchain is digitally signed by the Sender using their Private key.

- SSL is an example of a digital signature.

* Protocols :-

→ You might have seen that every blockchain has some different Functionalities. Bitcoin has a particular behavior like the block size will always be 1. After 10 minutes, a new block will be added to the chain with 12.5 BTC awarded to the miner who confirms the block in the chain. The keys in the bitcoin are using Ecc algorithms, which you can generate from the network and then use your keys to sign any transaction over the bitcoin blockchain.

→ Similarly, Ethereum blockchain has some other Functionalities like Smart contracts, which are mirrored to the legal agreements between two or more parties. Smart contracts gets executed on top of the Ethereum

blockchain using the Ethereum virtual machine.

→ other blockchain platforms like Hyperledger offer enterprise related behavior and use new protocols such as Gossip protocol to distribute information between different nodes.

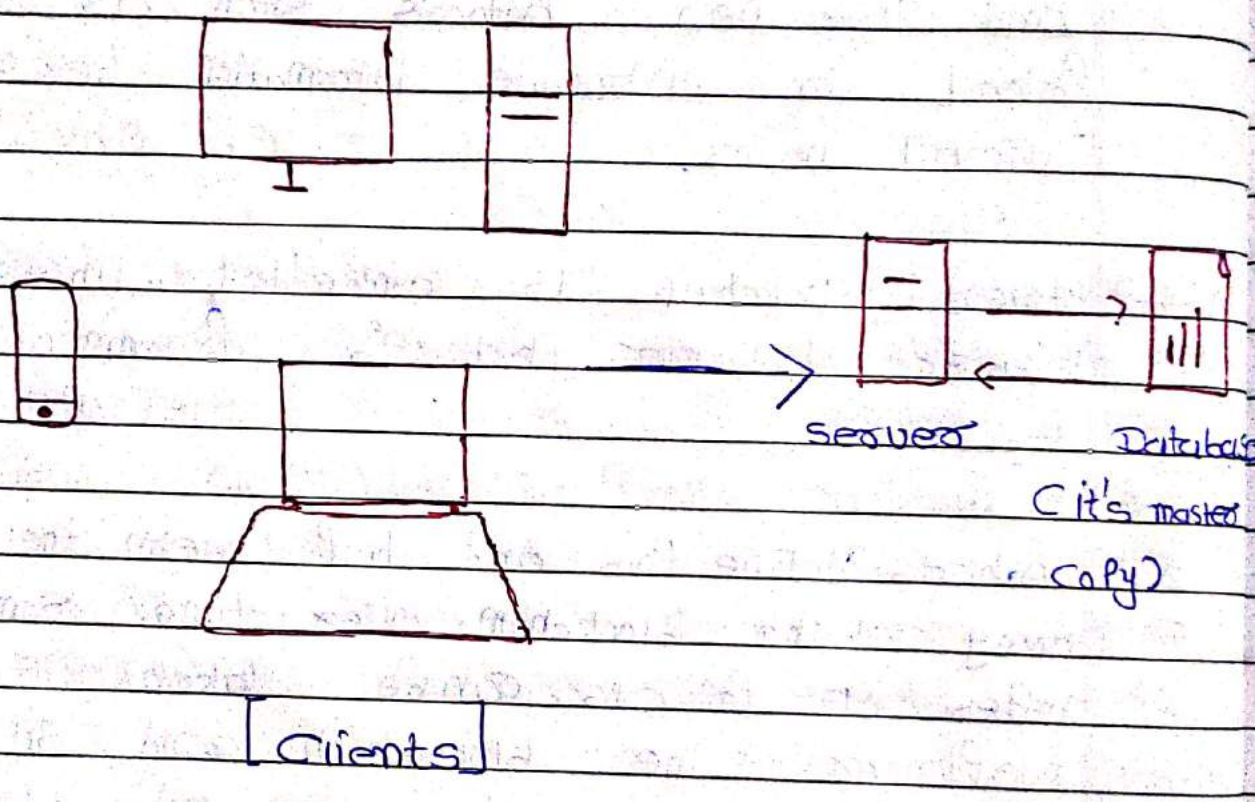
→ Every blockchain is embedded with some specific behavior that is programmed into it.

→ Protocols define this and help govern the functioning of the blockchain over time. Some examples of protocols can be taken from the pioneer of the blockchain world, Bitcoin behaviors like block time, block size, block difficulty, block reward difficulty, half an interval difficulty adjustment, or use of the specific hashing algorithm are an excellent example of the blockchain protocols.

* Benefits over Traditional Technologies:-

→

* Traditional Technology *



* Benefits of the Blockchain:-

— Decentralized Control:-

• Blockchain allows multiple parties that do not trust each other to share information without requiring a central control.

- It eliminates the risks of centralized control. With a centralized database, anybody with sufficient access to the system can destroy or corrupt the data within.

- Cost savings are also provided; usually billions of dollars are spent on safeguarding central repositories from hackers.

- Blockchain provides a sine shared system of record simultaneously for everyone who is connected to the network.

- The trust is established by the cryptographic protocols running behind the Blockchain Technology.

- All the parties must agree to make a change in Blockchain which is nearly impossible.

Integrity and Transparency :-

— Blockchain technology distinguishes it from traditional database Technology as it publicly verifiable, which is enabled by integrity and

Transparency.

- Every user can be sure that the data they are retrieving is uncorrupted and unaltered since the moment it was recorded.

- Every user can verify data appended over the Blockchain.

- Blockchain grows like ever-expanding archives of their history while also providing a real-time portrait.

- Merkle tree ensures the integrity of the data by hashing the transactions to a single root.

* Confidentiality :-

- The Blockchain is an openly distributed ledger, yet a private system can be established to maintain confidentiality.

- Data confidentiality in Blockchains ensure that individuals or organizations who are preve

nied from accessing data are not authorized to access it.

- Permissioned Blockchains have emerged as an alternative to Public ones to address enterprise needs for having known and identifiable Participants.

- Solutions like Hyperledger Fabric Blockchain and Block Stream offers rich sets of permissions to maintain confidentiality in the system.

* Enhanced Security :-

- Transactions are encrypted and linked to the Previous transactions.

- Information is Stored across a network of computers instead of in a single Server.

- Blockchain Prevents fraud and unauthorized activity.

- Cryptography Protocols make sure that the data is thoroughly Secure.

- Safeguard from DoS attacks as the data is present on all the nodes connected to the network.

- Cryptographic fingerprint is unique for each block.

* Faster Processing :-

- Traditional Banking Process takes days to settle, But the Blockchain has reduced that time nearly to minutes or even seconds.

- Everyone has access to the same information, and it becomes easier to trust each other without the need for numerous intermediaries.

- Moreover, tracking of Products could be made efficient by uploading the data on Blockchain.

- Digital assets and the trustless system makes sure that the data is protected and Transacted efficiently.

Bitcoin vs Blockchain :-

- **Bitcoin :-**

- Bitcoin is a crypto currency, created and held digitally on Pc or in a virtual wallet.
- It is decentralized, so, no person, institution or bank controls the currency.
- An implementation of Blockchain.
- It was started in 2009 to get rid of third-Party Payment Processing intermediaries.
- The Blockchain is the underPinning technology that maintains the Bitcoin transaction ledger.
- In Simple words "It's gold for nerds."

* Blockchain :-

- A Blockchain in the core is a distributed data base of records.
- Each transaction in the Public ledger is verified by consensus.
- Transactions are encrypted and cannot be replicated or altered.
- Currently, the most famous Blockchain application is the Bitcoin Blockchain.
- Blockchain can easily transfer everything from Property rights to stocks and currencies without having to go through an intermediary.
- In simple words "Blockchain is the tech. and Bitcoin is merely the first mainstream manifestation of its Potential."

- Bitcoin is a mirage :-
- Blockchain Holds Promise :-

→ Walmart → Blockchain

Tracking of Products

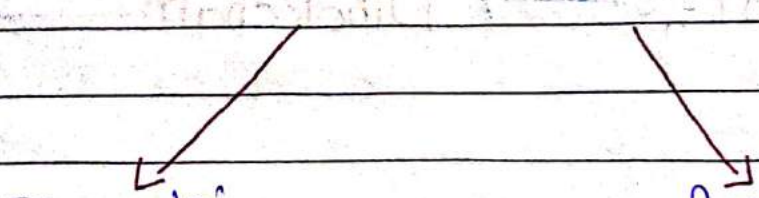
Tracking of Products days to 2 seconds.

- Key Concepts of Blockchain :-

→ • Keys :-

Pailvate key	Algorithm → Transformation	Rublic key	Hash → functions	Address

* • Key Generation Algorithms •

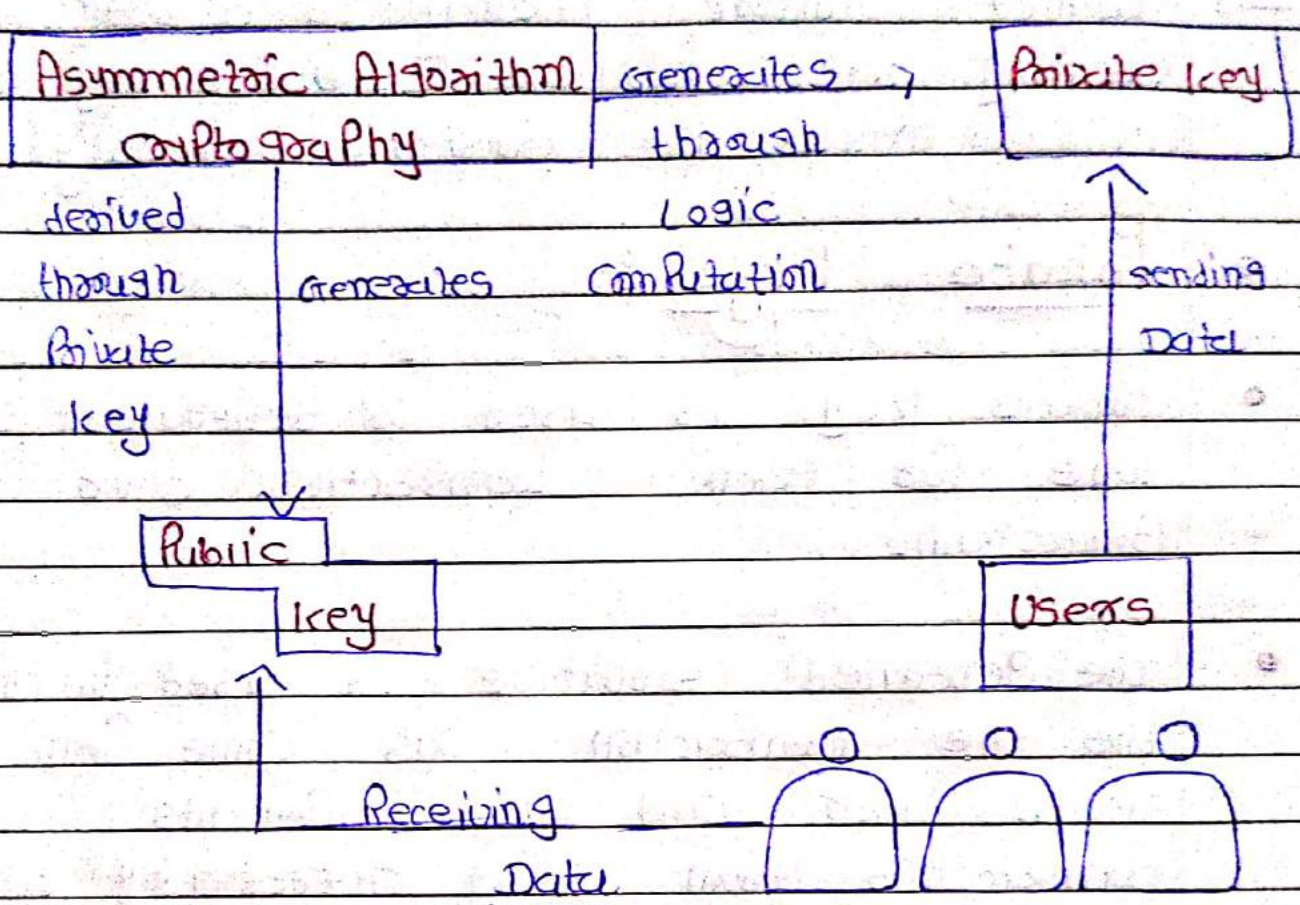


→ Symmetric cryptography Algorithm → Generates → key → shared → users → Use the key → Encryption Decryption of Data

* Example :-

→ AES Algorithm → Used in → TLS services

→ RC4 Algorithm → Used in → Wireless Encryption services



- Example :-

- RSA Algorithm Used with → Access of servers in cloud computing

- Ecc Algorithm Used with → Blockchain

→ Wallet import Format is a way of encoding a Private ECDSA key so as to make it easier to copy.

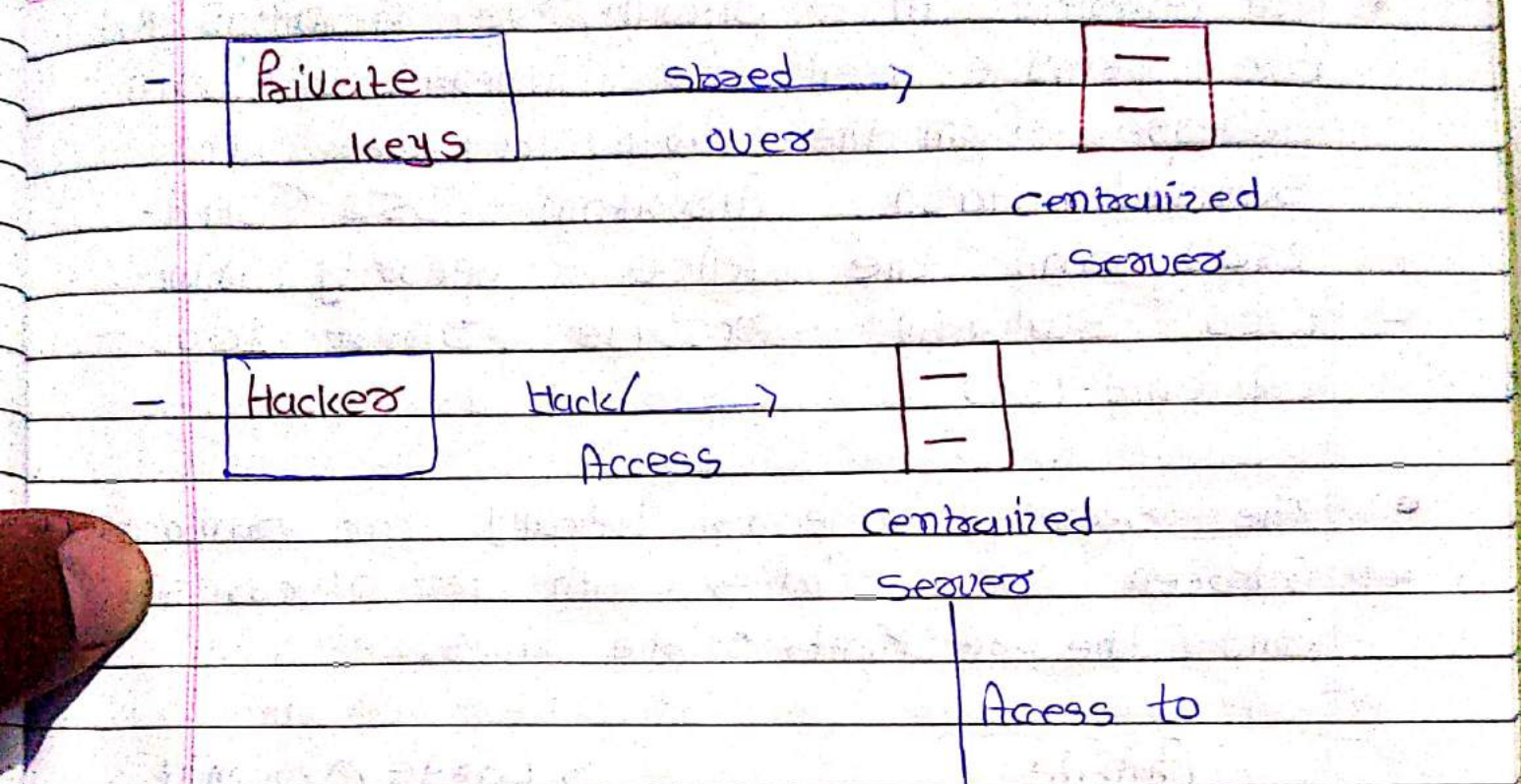
- **Private keys :-**

- Private key is used to generate a signature for each transaction over the Blockchain.

- The generated signature is used to confirm the the transaction has come from a specific user, and also prevents the transactions from being altered by any malign entity.

- In simple words - "Private keys are used to sign the crypto currencies you send to others"

- If someone obtains your Private keys, they would be able to send your crypto currencies to themselves, which has happened in most of the hacks around the world.



- **Address :-**

- A crypto currency address in a core is a representation of the Public key.

- one-way cryptographic hash functions are used to derived address from the Public key.

- For example in Bitcoin, the algorithm that are being used for generate a bitcoin address from the public key are the Secured Hash Algorithm 256 (SHA-256) and the RACE integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)

- The address appears typically in a transaction Between Two Parties, with the address signifying the recipient of the funds.

Private key → Large, randomly generated numbers

Public key → Generated from Private key

Address → Generated from Public key

Transactions :-

- Transactions are records of data in chronological order.
- Transactions are stored in a Merkle tree inside the Block.
- The transactions, when submitted, are picked up by Blockchain network and is inserted transactions on that network that have not been confirmed yet.
- Miners on the network select transactions from this Pool add them to their 'Block'.
- Transactions also contain metadata information which can be utilized to store data over the Blockchain.

What are Blocks :-

- A Block is a container data structure which contains a set of confirmed transactions.

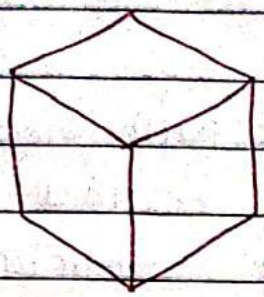
- A Block could contain different information, and a chain of these Blocks evolves into a Blockchain as long as it links one and the other.

- The Blocks are stored on the hard drives of many miners spread across the globe on a Peer to Peer network.

- In the Bitcoin algorithm, a Block is created every [10 minutes] All the transactions happening over the network within 10 minutes interval are clamched into that Block and added to the chain.

→ Memory Pool ⟶ miners ⟶ Validation ⟶ Block

→



• Blocks •

mostly contains →
- Transactions
- Time Stamps
- Block Identifier
- Nonce Value
- Previous Block Hash
- other Additional information.

• Block Header + Nonce → Twice Sha256

Block Hash

* Structure of Blocks :-

→ All Blocks in the Blockchain are composed of a header, identifiers and a long list of transactions. The structure of a Block is as follows.

- Block Header.
- Block Identifiers.
- Merkle Trees.

Metadata information

- Timestamp
- Protocol information
- Nonce
- Difficulty
- Previous Block Hash.

Hash Binary Tree → used to store & verify transactions.

Hash associated with Block

* An Example of Bitcoin Blockchain *

Field	Desciption	Size
Magic No	Value always 0XD9BEF9	4 bytes
Blocksize	number of bytes following up to end of Block	4 bytes
Block header	Consists of items	80 bytes
Transaction Counter	Positive integer VI = Variant	1-9 bytes
Transactions	The list of transactions.	Transaction counter-many Transactions

* **Block Header :-**

→ The header contains metadata about a Block. These three different set of Metadata.

- The Previous Block hash, in a Blockchain, every Block is inherited from the last Block Because we use the Previous Block's hash to create the new Block's Hash.

- mining competition for the network. for every Block to be Part of the Blockchain, it needs to be given a valid hash. This contains the values for the time-stamp, the the difficulty.

- Markel tree root. This is a data structure to summarise the transactions inside the Block.

- **Block Identifier :-**

→ To identify a Block, we need to have a Cryptographic Hash, a digital signature. This is created by hashing the Block header Twice with the SHA256 Algorithm in case of Bitcoin Blockchain. You can use different hash functions for your Blockchain.

→ Every block uses the last Block's hash to construct its hash.

→ Another way to identify a specific Block is the Block Height. This is the position of the Block in the Blockchain.

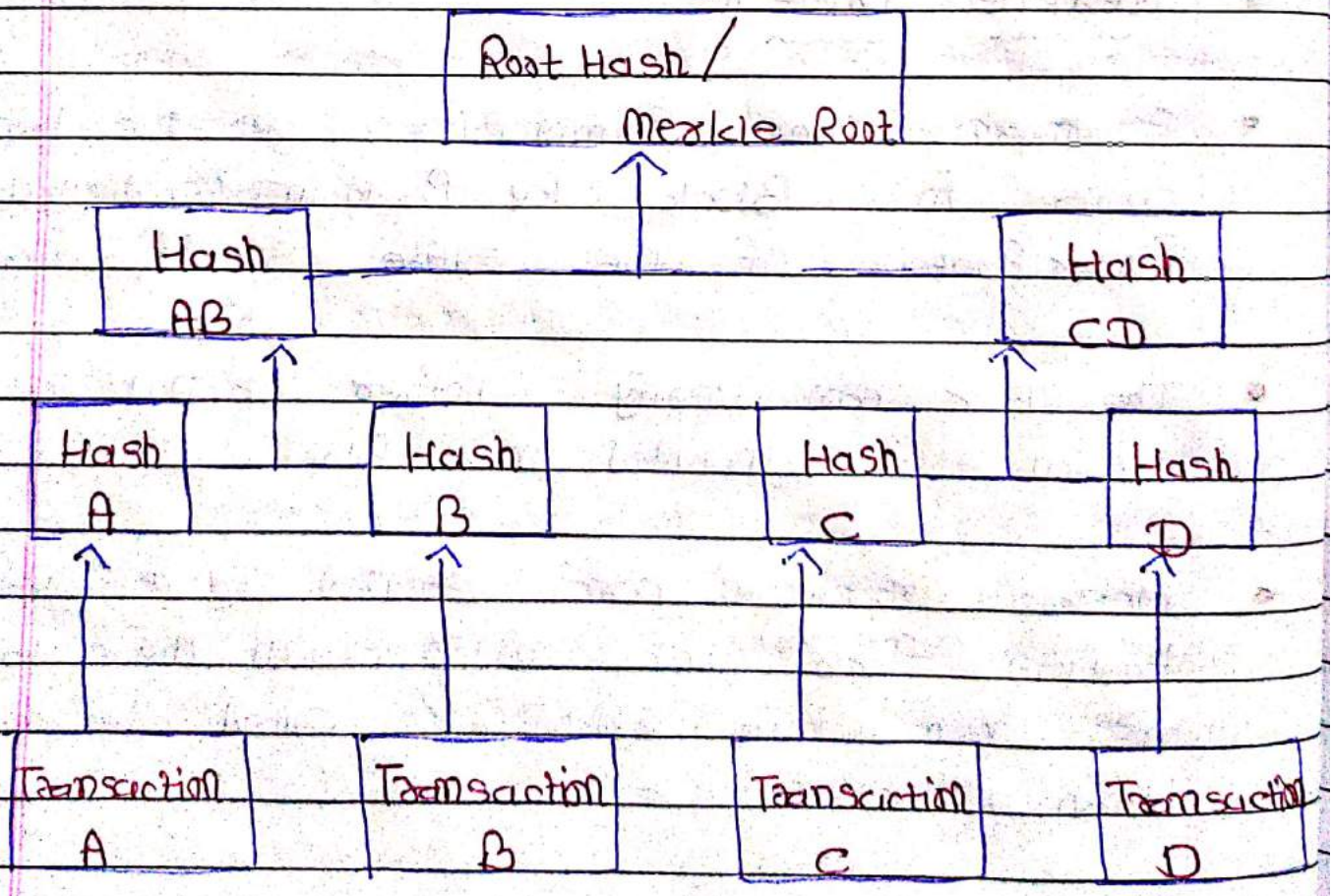
→ for example if we say the Block is the 7312 position This means that there are 7311 Blocks Before this one.

* Merkle Tree :-

- A Merkle tree Summarizes all the transactions in a Block by Producing a digital finger Prints of the entire set of transactions.
- The user can verify whether or Not a transaction is included in a Block.
- Merkle Trees are Created by Repeatedly Hashing Pairs of Nodes until there is only one hash left which is called the root Hash.

- Each leaf node is a hash of transactional data, and each non-leaf node is a hash of its previous hashes.
- Merkle trees are binary and therefore require an even number of leaf nodes.
- If a single detail in any of therefore require an even number of leaf nodes.

Merkle Tree



* HD Private key :-

→ Hierarchical deterministic is a type of deterministic cryptocurrency wallet derived from a known seed, which allows for the generation of child keys from the parent key.

→ The child key is generated from a known seed. There is a relationship between the child and parent keys that is invisible to anyone without that seed.

→ The BIP 32 Protocol can generate a nearly infinite number of child keys from a deterministicality - generate seed from its parent.

→ You can recreate those same child keys as long as you have the seed.

→ The child key can operate independently, and the parent key can monitor and control each child key.

Mnemonics Seed :-

→ A mnemonic seed is used to substitute either a 12, 18 or 24-word phrase for the private keys which can easily be memorized by human mind compared to hex encoded format.

→ Mnemonic word phrases are tied with the private keys and support wallet restoration.

→ This provides additional security for the user, as well as a convenient solution to recover a wallet.

→ BIP 39 introduced the mnemonic wallet implementation.

→ The English wordlist for BIP 39 contains 2048 words, so to crack 12-word phrase it could require figuring out $2048^{12} = 2^{132}$ possible combinations under a shield of 128-bit security.

Smart Contracts :-

- Smart contracts are the digital contracts signed between two parties and stored over the immutable ledger.

Smart contracts help you exchange money, property shares, or anythings of value in a transparent, conflict-free way while avoiding the services of a middleman.

Contracts can be encoded on any Blockchain, But Ethereum is mostly used since it gives unlimited Processing Capability.

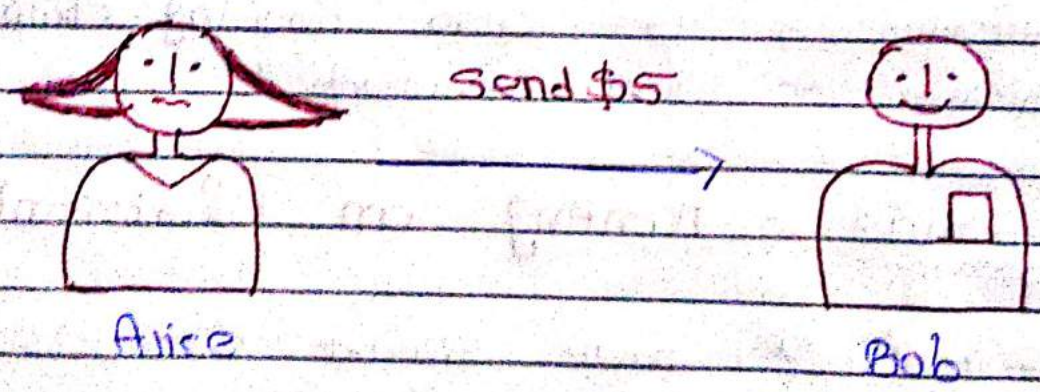
HyperLedger is also Providing chain codes which are very similar to smart contracts.

Example :- Renting an Apartment.

—→ If you have smart contracts for Renting a house, You don't require a Property dealers in the middle The house owner can share their home over the smart contracts and the lenders can rent the house, By depositing money on the smart contract

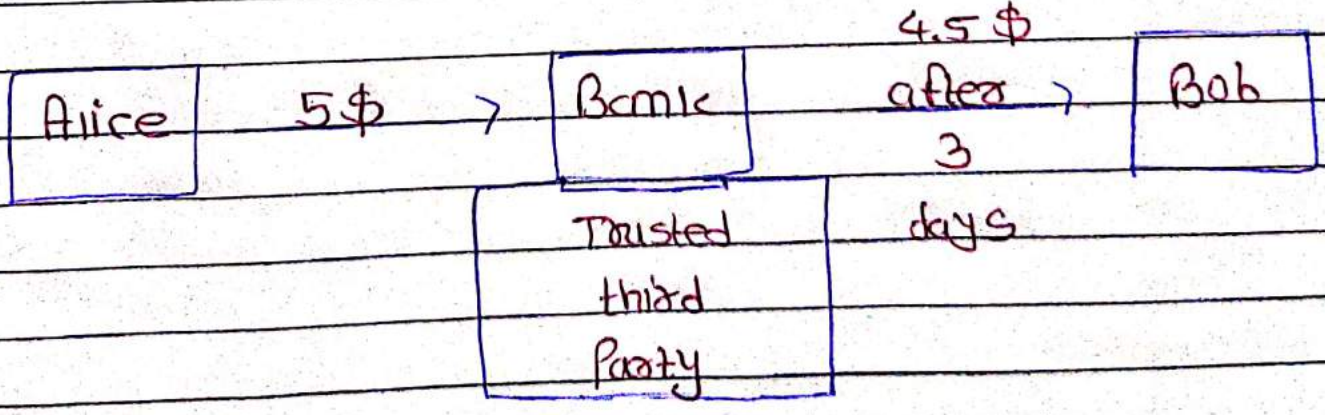
Present Solution with Example

- How Blockchain transaction works?
- Alice in the US wants to send $5 to Bob in Australia
- She can make use of net banking or any other payment services like PayPal.
- The 3rd Party service can take 3-4 days for cross-border transaction and charges a cut let's say $0.5.
- Moreover, Alice cannot see the whole process of her transaction execution.



* Problems with Present solution:-

- The transaction costs are high with 3rd parties involved.
- The time taken for the process is also slow.
- Imagine a scenario where Alice needs to transfer a large sum of money for some medical operations. This will take time and charge massive cost over the transaction.
- can we do the same things removing the present problems?



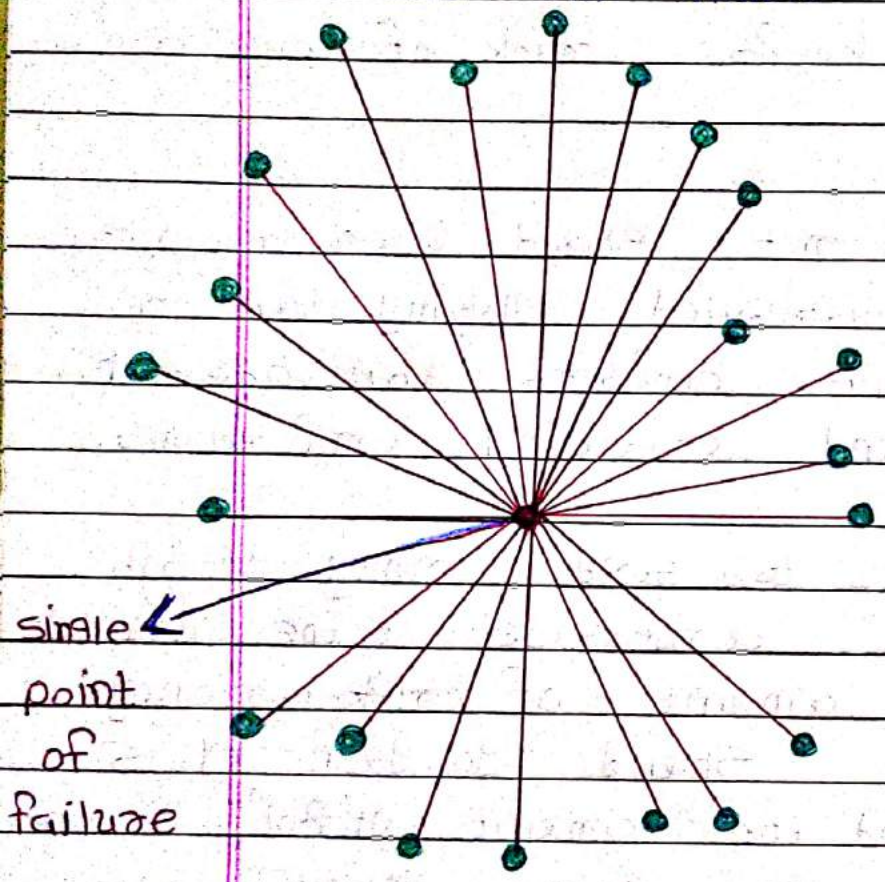
Blockchain for the Save :-

- Blockchain uses a ledger, a digital file/ database that keeps track of all transactions.
- Ledger file is not stored over a central server. It is distributed globally via a network of private computers that are both storing data and executing computations.
- If Alice wants to send money to Bob, she broadcasts a message to the network that says the amount of crypto currency in her account should go down by 5 Tokens/5 $, and the amount of Bob's account should go up by the same quantity.
- Each node connected in the network will receive the message and apply the requested transaction to their copy of the ledger, this updating the account balances.

— Fewer intermediaries.
— Faster Process.
— Transparency.

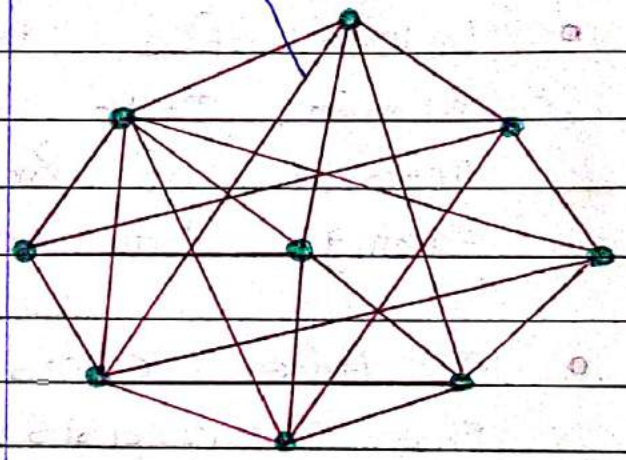
* Transaction Distribution *

- All transactions are distributed in Blocks and all nodes hold all transactions.



single point of failure

- centralized



Availability is built in

- Distributed ledger
Shared ledger

* Consensus Mechanisms :-

- Blockchain are decentralized systems which consist of different participants who act depending on incentives they receive and information that is available to them.

- When a new transaction gets broadcasted on the network nodes connected to the network have the option to either include that transaction to their copy of ledger or to ignored it. When the majority of the nodes which comprise the network decide on a single state, the consensus is achieved.

→ Let's dive into 2 Generals Problem and understand the consensus better.

* Two Generals Problem :-

- This Problems describes a scheme where two generals are attacking a fevent enemy. General 1 is considered the leader and the other general is referred as the follower.

- Each General's army on its own does not have the strength to defeat the enemy army; thus they need to collaborate and attack at the same time.

- For them to collaborate and agree on a time, General 1 needs to send a messages across the enemy's territory that will provide the time of the attack to the other General. However, there is a probability that the messanger will get captured by the enemies, and thus the message won't be delivered. This will result in General 1 attacking while General 2 and his army hold their ground.

- Even if the first transmission goes through, General 2 has acknowledge that he has received the news, So he sends a messenger back, thus repeating the previous scenario where the messager can get caught. This extends to infinite messanger exchange, and therefore, the generals are unable to reach an agreement.

Byzantine Generals Problem :-

→ A more generalized version of the Two Generals Problem describes more than two generals agreeing on the time of the attack. Additionally, one or more generals can be the traitors, meaning that they can lie about their attack choice.

→ To reach a consensus here, the commander and all the lieutenants must agree on the same decision.

→ Let's change the scenario to a Commanding General and Lieutenants based approach, so when General issues an order, every loyal lieutenant will follow the same to attack.

→ If the commander is a traitor the consensus is still achieved. As a result, all lieutenants take the majority vote over the default value.

→ This implies that the algorithm can reach a consensus as long as 2/3 of the actors are honest. if the traitors are more than 1/3, the consensus is not reached, the armies do not coordinate their attack, and the enemy wins.

* Explanation with Example :-

- Take an example; every lieutenant needs to convey orders within 10 minutes. In other words, 10 minutes are required for communicating a message for an attack.

- Moreover, the passing of messages is related to appending the message and then sending them to the next lieutenant.

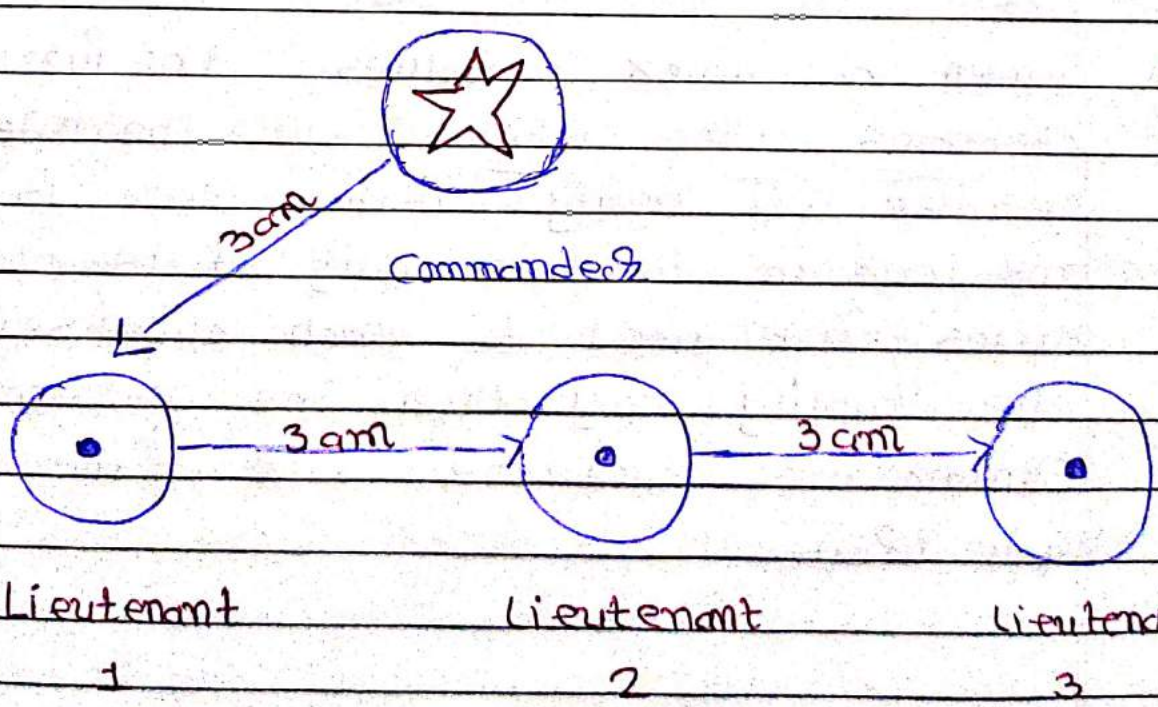
- Example :-
- General - Attack at 3 am.
- Lieutenant 1 - Attack at 3am, Attack at 3 am.
- Lieutenant 2 - Attack at 3am, Attack at 3 am, Attack at 5 am.
- As you can see if the lieutenant 2 is a traitor, then the 3rd lieutenant can verify that the incoming message is not in synchronization.

- Moreover, if Lieutenant 2 decides to change all the previous messages too, then each message would take 10 minutes thus Lieutenant 2 will be Goofing for 30 mins.

- But Lieutenant 3 expects the message to come in 10 minutes, thus again giving in that Lieutenant 2 is a traitor.

- If the commander is a traitor, then he might send different orders to different Lieutenants, which will come into Consensus but since the messages don't follow the structure of Paxos in the same attack time, the default option of retreat will come to action.

→



How does it relate to Blockchain?

- Blockchain are decentralized ledgers which are not controlled by a central authority. Due to the value stored in these ledgers bad actors have substantial economic incentives to try and cause fouls.

- Proof-of-work is a Probabilistic Solution to the Byzantine Generals Problem as described in depth by Satoshi Nakamoto.

- It follows the longest chain rule where miners shift to the chain which is being more worked upon.

- When a miner solves the puzzle and confirms the Block, all the nodes in the network will verify if the Block is valid and add it to their copy of the chain. The nodes first need to reach a consensus on the validity, only then the network will synchronize, and the state of the Blockchain will update.

Conflict Example in Mining.

- Multiple miners work on mining the Blocks.
- Suppose two miners can confirm a Block within a fraction of seconds.
- Other miners start working in for the next Blocks.
- Bitcoin and ethereum identify the longest chain Based on total work is done/difficulty.
- Node prefers the first-seen valid chain with the most work measured in terms equivalent to the sum of the difficulty of all the Blocks.

Longest chain Rule :-

- In Public Blockchains like Bitcoin, conflicts are being resolved by the longest chain rule.
- Let's say a miner received the first Block 4 then he will start building the next Block on top of that Block 4.

- Node, in a few seconds that miners see another Block 2, so that miner will keep an eye on that new Block.
- if the next Block 3 is being detected from other nodes in Blockchain then that miner will keep on eg disregard the 4 and will accept the new longest chain which is 1→3→5 and so on.
- Conventional wisdom states that it is therefore wise to wait for six Blocks to confirm a transaction.

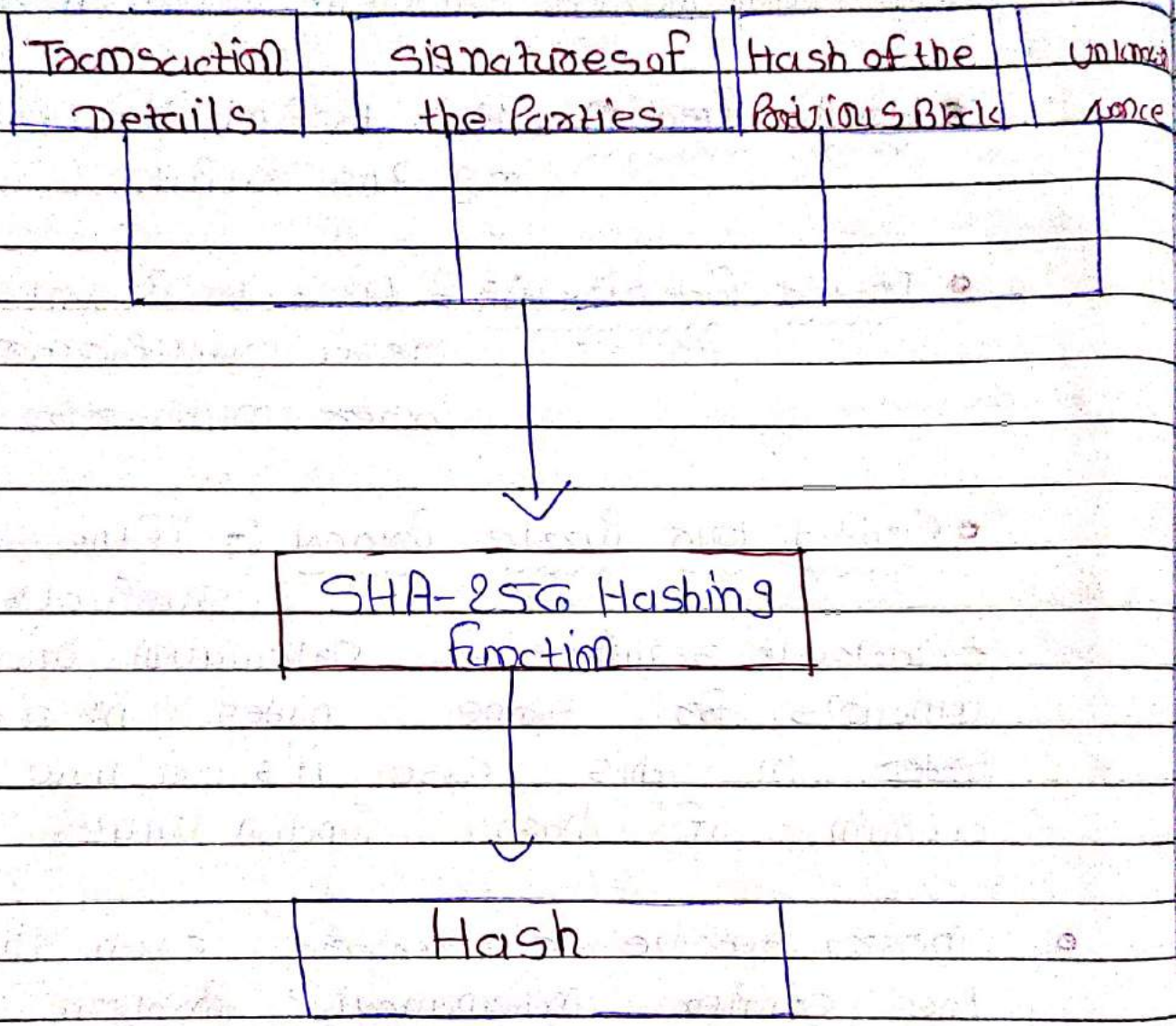
* Top 5 Consensus :-

1. Proof of work :-

→ PoW is the consensus algorithm where miners compete to solve a difficult Mathematical Problem Based on a cryptographic hash algorithm. This Proof Proves that a miner spends a lot of time and resources to solve the Problem. When a Block is 'solved' the transactions contained are considered confirmed.

→ By Mathematical Problem we mean.

- Hash function - How to find the input knowing the output.
- Integer factorization - How to present a number as a multiplication of two other numbers.
- Guided tour Puzzle Protocol :- If the servers suspects a Dos attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it's a 'how to find a chain of hash function values Problem.
- Miners receive a reward when they solve the complex Matematical Problem.
- For example in Bitcoin miners receive 12.5 Bitcoins for solving the Puzzle.
- Miners can also receive transaction fees in addition to rewards.



✱ PoW Example :-

- Example Bitcoin :-

→ In Bitcoin, a Block is being mined every 10 minutes. The difficulty is adjusted such that it never deviates much from this limit. if the difficulty stays the same, while

the computer Power increases gradually, it will take less and less time to mine a Block.

→ To make sure this doesn't happen over Blockchain, the Proof OF Work target is a dynamic Parameter. In the Bitcoin Blockchain, the target gets adjusted every 2016 Blocks. Computing the amount of time it took to mine 2016 Blocks. It should take 20160 minutes (2016 * 10 minutes = 14 days). The difficulty is adjusted depending on the time it took to mine those blocks.

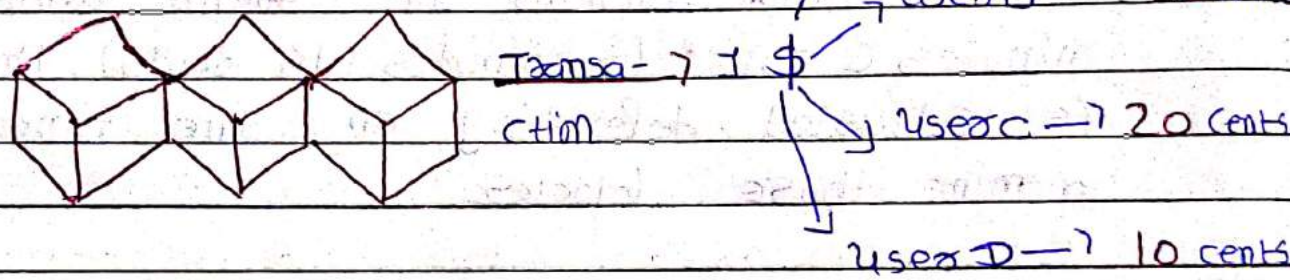
2. Proof of Stake :-

→ Proof-of-Stake is a different algorithm to validates transactions and achieve the distributed consensus.

→ Proof-of-Work algorithm rewards miners who solve complex mathematical Problems with the end goal of validating transactions and creating new Blocks. On the other hand, in the Proof-of-Stake algorithm, the creator of a new Block is chosen in a deterministic way, depending on its wealth/stack in the Blockchain.

→ No block reward.

→ All the digital currencies are created at the start of the chain, and their number never changes. Miners only take the transaction fees. That is why in the Pos system miners are also called forgers.



1. Anyone who holds the native currency can become a validator.

2. The chance of mining and earning rewards are based on how much of the stake they have in the Blockchain

3. The chosen validator is rewarded by a part or the whole of the transaction fee.

- Proof of stack Example :-

- Example Neo :-

→ NEO is a Smart Contract development often referred to as "China's Ethereum." The network aims to be the center of a creative economy where digital assets can be securely traded with little overhead.

→ Staking NEO lets, you generate GAS, the Platform's internal currency. The more NEO you have staked, the more GAS you'll earn with each Payment. NEO rewards stockholders with an anual return of 4-6%.

* Delegated Proof of Stake :-

→ People in a particular Blockchain ecosystem vote for witnesses to safeguard their computer network.

→ Let's imagine a record system where only the top 100 witness are Paid for their service, and only top 20 earn

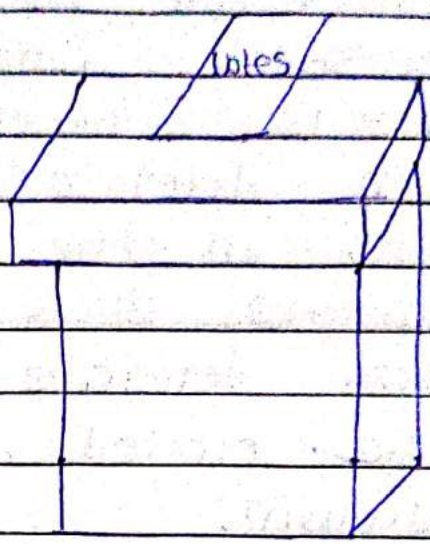
a regular salary. As it creates a healthy competition, many wants become a witness thus providing hunderds of backup witnesses.

→ The vote strength of a person is determined by how many tokens they hold. People who have more tokens will influence the network more than people who have less tokens.

→ If a witness starts acting like a schmuck or stops doing a quality work in securing the network, people in the Blockchain community can remove their votes, essentially firing the lousy actor. Voting is always ongoing.

→ Delegates are elected as witness. A delegate becomes a co-signer on an individual account that has the privilege of proposing certain changes to the network parameters. This account is known as the Genesis account. These parameters include everything from transaction fees to block sizes, witness pay and block intervals.

1. Anyone who holds the Blockchain base currency can vote for a Validator.



2. The Validator with the most votes gets to become a delegate, validating transactions and collecting the records for doing so.

* Delegated Proof of Stack Example :-

• Example Lisk :-

→ Lisk is a decentralized network similar to Bitcoin, Ethereum, or Bitshares. Lisk uses a simplified implementation of the Delegated Proof of Stake consensus algorithm.

→ Lisk token holders can vote for mainchain delegates who secure the network. There is a maximum of 101 active main-chain delegates whosoever got the most votes on the whole network, and they can earn block generation rewards. Every other delegate is on standby waiting to be elected, or securing a Lisk sidechain.

* Proof of Authority :-

- The Proof-of-authority consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than staking tokens.

- The group of validators is usually supposed to remain relatively small to ensure efficiently and manageable security of the network.

- Individuals under PoA earns the right to become a validator, that's why there is no incentive to be in the position that they hold.

- Validators are required to formally verify identity either on the chain or some public domain.

- The eligibility to become a validator is difficult to obtain, and the individuals need to go through many steps to become a validator.

* Proof of Authority Example :-

• Example PoA Network :-

— Proof of Authority Network is a Blockchain Platform founded on the core Principle of implementing PoA consensus in their

* Proof of Weight :-

- Proof of weight is a broad consensus classification based on the algorand algorithm which in turn specifies a new Protocol known as Byzantine Agreement.

- BA* Protocol is highly Scalable and secure.

- PoW concensus model runs a commitee where participants keep on changing, and the commitee achieves the consensus for the network.
- Every user over the network has a weight attached to them which is determined by the money they hold in their account.
- Proof of weigh Example :-
- Example Filecoin :-

—→ Filecoin is using Proof-of-Spacetime as a weighted consensus on how much IPFS data you're storing. The weight is based on different parameters. If the overall weight fraction of honest users is higher than two-thirds of the total weight then the network will remain secure. This method also helps in protecting the network from double-spend attacks.

—→ It is based on Algorand. While some may see similarities between Algorand and Proof-

of-Stake, they are not the same. In a PoS environment, the number of tokens held at any given time determines the amount of additional rewards users earn. Proof-of-Weight uses an entirely different weighted value.

TYPES OF Blockchain :-

Public Blockchain :-

- A Public Blockchain as its name suggests is the Blockchain which is available to all. In other words it is a kind of Blockchain which is - 'for the People, by the People and of the People.
- No one is in charge of the network, and anyone can participate in reading/writing/auditing the Blockchain.
- More complex rules are present for safeguarding it from malicious actors.

- All the decisions are made using the complex consensus algorithm.
- computationally these Blockchain expensive to mine & commit a Block over the network.
- Example :- Bitcoin Blockchain, etc.
  Ethereum Blockchain.

✱ Private Blockchain :-

→ An individual or an organization privately operate private Blockchain as its name suggest.

→ Unlike Public Blockchain in Private Blockchains, there is an administrator/anchor who looks after essential things such as permissions and identities.

→ The consensus is achieved on the whims of the central in-charge who can provide mining rights to anyone or not give at all.

→ Compared to Public Blockchain it is much faster and cheaper Because one doesn't have to spend an enormous amount of energy, time and money to reach a consensus.

→ It is less secure compared to the Public Blockchain.

→ Example :- Blockchain, Medichain, etc.

✱ Consortium Blockchain :-

→ This types of Blockchain removes the individual autonomy which gets vested in just one entity by using Private Blockchains.

→ Here instead of one in charge, we have more than one in charge. A group of companies or representatives coming together can make decisions for the benefit of the whole network.

→ As a way of achieving things much faster and also have more than one single point of failures which Protects the whole ecosystem.

→ In simple words, it's the best of both Private and Public Blockchains.

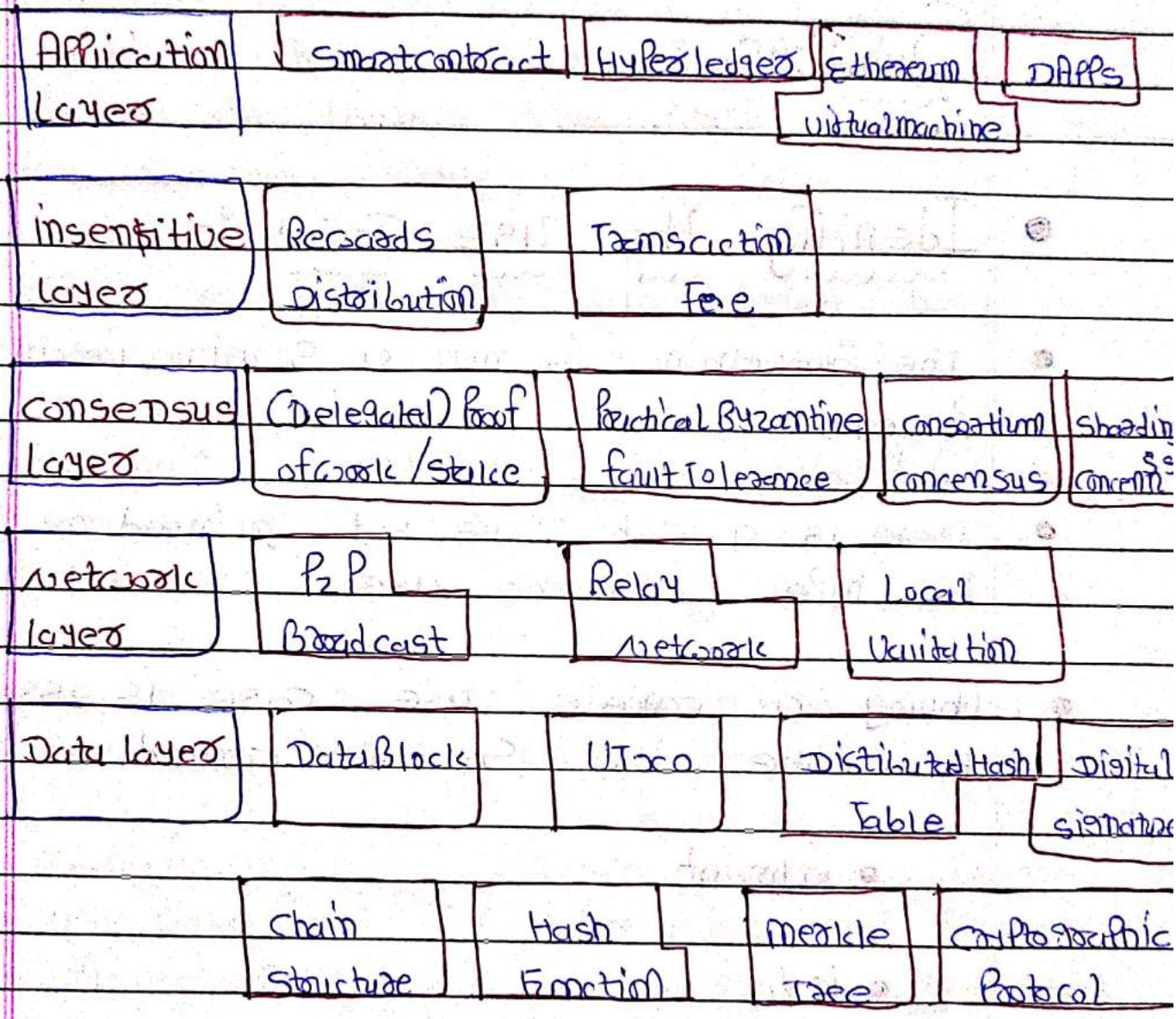
→ Gives options for rights and access management while leveraging the same Blockchain technology and reaping its benefits.

→ Example :- R3, Enzy, etc.

* Difference *

Property	Public	Consortium	Private
Consensus Determination	All miners	Selected few miners	Organization Participating.
Permissions	Read Permission to all	Could be restricted	Could be restricted
Immutability	Nearly impossible to tempered	Could be tempered	Could be tempered
Centralised	No	Partial	Yes
Efficiency	Low	High	High
Consensus Providers	Permissionless	Permissioned	Permissioned

Blockchain Architecture :-



Forming Your Own Blockchain Solutions :-

- **Identify the use case :-**
- The Blockchain is not a solution for all the problems.
- There is a lot of hype, but you need to map the hype with the use.
- Having a concrete use case is essential to weave the solution around.
  - Payment
  - KYC
  - Smart asset
  - Land Records

* Design a Workflow for Blockchain Integration :-

- Analyze whether you need a Blockchain as a solution or there are other ways to solve the existing Problem.
- Don't start churning up detailed technical specification without any validation.
- Blockchain should solve a Problem for existing centralized systems, e.g. expensiveness, transparency, and reliability.
- Have a feasible layout on integrating the technology into your development strategy.

Identification of use case for Blockchain → Design strategy for using Blockchain → Identify consensus Mechanism

* Identify the Consensus Mechanism :-

- Depending on your use case choose the consensus Mechanism

- Choose the mechanism which is apt for the use case.
- for example, A Private Blockchain solution may not require expensive PoW consensus.
- Some of the Popular consensus mechanisms are :-
  - Proof-of-Work
  - Proof-of-Stake
  - Delegated-Proof-of-Stake
  - Proof-of-Authority
  - Proof-of-Weight

- Identify the Platform :-
  - Depending on the consensus mechanism of your choice, choose the Platform which fits your needs and Plans.

- Blockchain started as open-source, and there are many platforms available free to use.
- Some of the major platforms are:-
- Bitcoin
- Ethereum
- multichain
- Hyperledger
- Corda
- Quorum
- BigchainDB
- Stellar

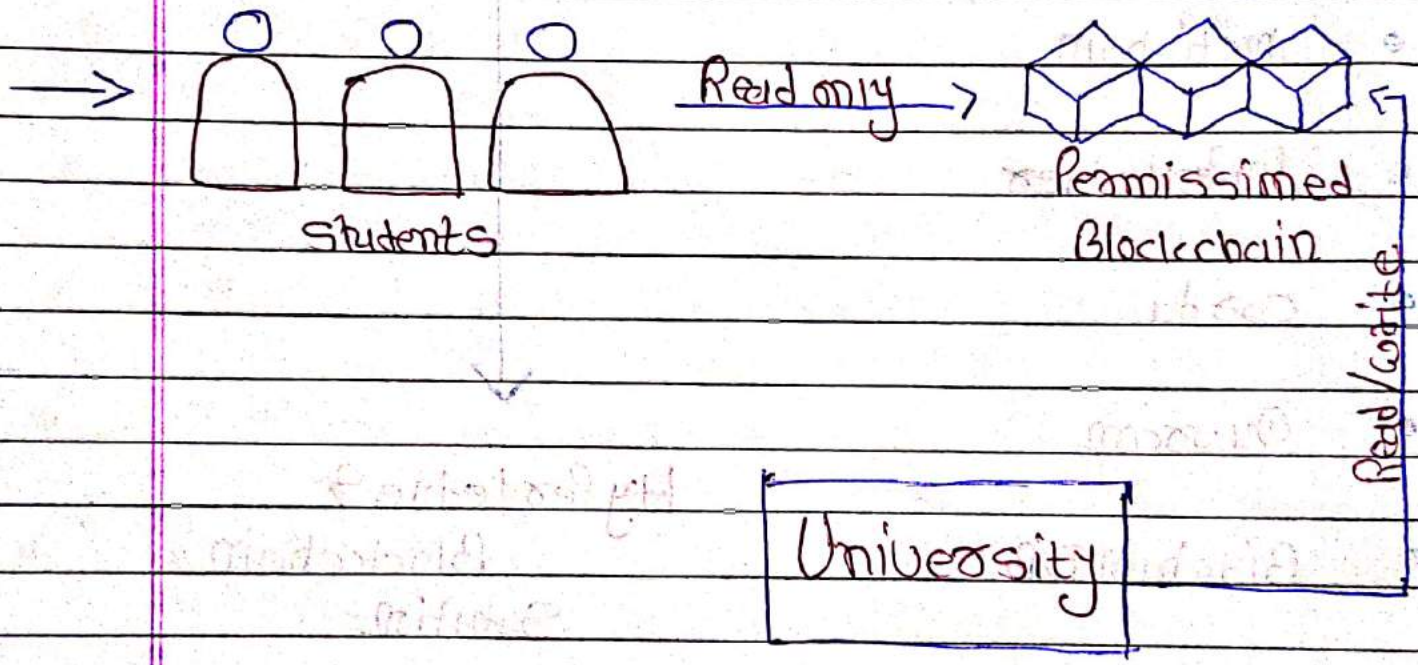
Dental | Orthopedic | Cardiology

Hyperledger Blockchain Solution.

* Design the Architecture :-

- The architecture includes elements such as the infrastructure, Software, and hardware configuration.

- The solution may be architectured on the cloud, on-Premises, or a hybrid model depending on the organization's need.
- Further architecture can be design according to Permission-less, Permissioned, Public, Private or hybrid.



Design the Blockchain Instance :-

- You need to Plan your instance carefully.
- In specific Platforms, it's difficult to

configure some parameters once set.

- Things needed under configuration can be as following :-
- Permissions
- Asset issuance / Reissuance
- Atomic Exchanges
- key Management
- Multi-signature
- Blocks Parameters
- Limits
- Network Protocols / Handshaking.
- key and Address Formats
- Native Assets

Build the APIs for your Blockchain.

- APIs are required by the developers and applications to interact with your Blockchain.
- Usually, Platforms come with APIs, and if you are Building from scratch, you need to look into design and schemas for your APIs carefully.
- As per your requirements you need to see which APIs to expose for your Blockchain.
- Some of the APIs that you might need :-
  - Generating key Pairs.
  - Asset issuance
  - Data Authentication
  - checking Blockchain Parameters.
  - Create and Read operations.
  - Smart Contracts.

- Address Specifications.

→ APIs ⟶ Creation of smart contract
Interacting with smart contracts

○ Designing the front End :-

→ You require a Front End for your users and administrators.

→ Most Platforms work on Json format which can be collaborated with major programming languages.

→ Some of the Platforms offer SDKs to integrate existing front-end applications with Blockchain.

→ You can use languages like HTML5, CSS, PHP, C#, Java, JavaScript, Python, Ruby, Golang, Solidity, AngularJS, NodeJS.

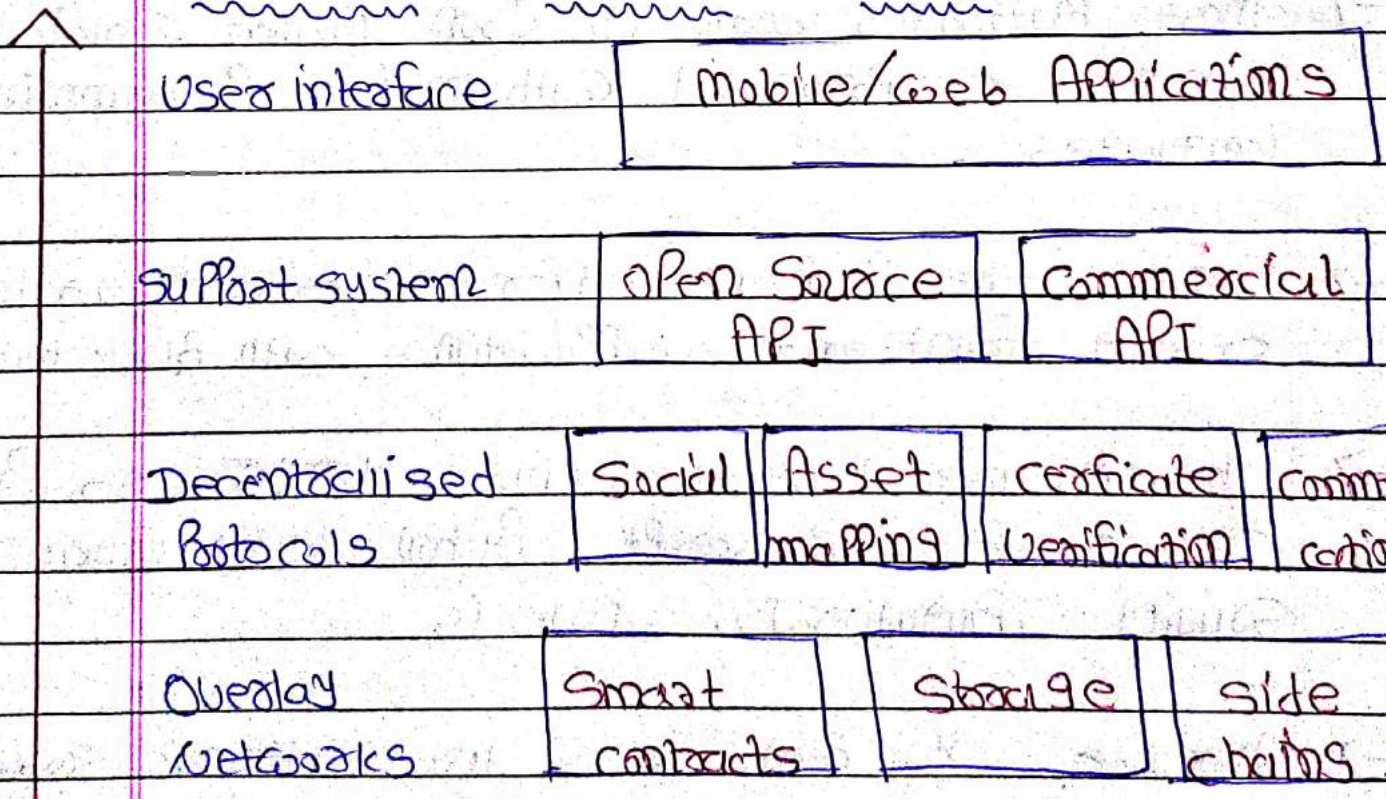
→ Moreover, you can also use external storages like cloud storage, NoSQL, RDBMS, etc.

Future Prospects :-

→ Once you have the stable application up and running, you can look into future integrations with other technologies.

→ You can enhance the power of your Blockchain solution by integrating Artificial intelligence Biomatics, internet of Things, Bots, Cloud, Cognative Services, Containers, Data Analytics, and Machine learning.

Blockchain Technology Stack :-



Blockchain :-

→ This is the base of all Blockchain Based applications.

→ It is a network of nodes spread across the world which run algorithms to verify and commit transaction over the Blockchain.

→ This is a decentralized network and mostly Based open source cryptography algorithm.

→ This can be created as Public, Private or consortium.

→ This can also include certificate Authorities and Membership services for Government and enterprises.

Overlay Networks :-

- This is a network that achieves additional functionality without bootstrapping the original protocols.
- They benefit from the network effects and build on top of that.
- Some of the additional functionalities you achieve are :-
  - Smart Contracts :- Crypto agreements between two parties
  - Storage :- Renting network
  - Sidechains :- Transfer tokens from one Blockchain to a different Blockchain.

Decentralised Protocols :-

→ This is the essential part of the Blockchain Technology Stack as it makes sure the Blockchain layer and overlay networks

do not depend on a single entity for validation and transactions.

→ It helps to create decentralized peer-to-peer datasets.

→ Decentralized Protocols can be based on asset mapping, social identities, verification algorithms or communications channels.

* Support System :-

- For building Blockchain applications, you require APIs to interact with the underneath technology.
- You can directly build a solution using the existing APIs, without depending and coupling on your ledger.
- Most APIs respond to JSON format, thus can be easily integrated with existing Front End Technologies.
- You can use the open source APIs like Bitcoin and Ethereum, as you can choose from commercial

APIs like Block io or Blockcypher for more boxed up functionalities.

* User interface :-

→ Finally, a user interfaces is required for your users to connect to your Blockchain.

→ User interface can Be Built with existing frontend mechanisms and can easily employ the Power of Blockchain by using APIs.

→ Some Platforms like Hyperledger also Provide Generators to Produce a box user interface for the applications built open them.

→ Most Blockchain Platform also Provides with connecting services to link Applications to Blockchain.

Blockchain Ecosystem :-

Blockchain Projects :-

→ The Blockchain ecosystem is currently running with some major Projects and more are under Pipeline. Some of the major Projects on Blockchain are :-

* **Bitcoin :-** This Project introducted the World to Blockchain.

* **Ethereum :-** This Project came with concept of smart Contracts where two Parties adhere to certain rules and create a trust. This opens the doors for more decentralized applications.

* **Neo :-** This Project Positioned itself as the "chinese Ethereum" but it Brought the Python as the main language for creation of Applications.

- Stellar :- This Project is trying to make cross border transactions simpler, stellar comes with extensive APIs which Helps the developers build applications fast, thus reducing the time to market for the applications.

- ## Blockchain Users :-

→ Blockchain users are normal People like you and me, who make use of the Blockchain or crypto currency to achieve some results. They can also be investors who buy crypto currencies to sell at a later date.

→ for creating a Blockchain user Base the technology or cosplo currency should have some utility related to the Problem being tackled.

- ## For Example :-

→ Bitcoin servers the major utility of Payment for goods and services. Currently there are over 50,000 merchants registered with Bitcoin including - Microsoft, PayPal and subway.

—7 Bitcoin was the first mover in Blockchain and it's high utility as Payment system made sure that a large part of its ecosystem is based upon users.

* Blockchain Exchange :-

- Every blockchain Project has a robust ecosystem growing under it and it always include a Decentralized exchange. These are developed by the Blockchain team or the community of other developers.

- A typical exchange is designed to find the cheapest rates of exchange between any two cryptocurrencies, making it more affordable to trade tokens/ cryptocurrencies.

- Exchanges used for trading can also might integrate with hardware wallets, or users can create their own wallet on the exchange website.

Blockchain Miners:-

→ To function a blockchain and maintain its integrity, it needs a large network of independent nodes around the world to maintain it continuously. In Private Blockchains, a central organisation has the authority over every node on the network. In the case of Public Blockchains, on the other hand, anyone can set up their computer to act as a node. The owners of these computers are called miners.

→ Since the integrity of the Blockchain is directly related to the number of independent nodes on the network, there also needs to be some incentive to mining. Different Blockchains utilize different mining systems however most of them contain some form of.

- An incentive system
- A consensus algorithm.

Blockchain Developers:-

→ Blockchain Technology is built by the Potential of Developers working Behind it. A strong team of developers can lead to a successful Blockchain Project. Currently there are too types of developers in the Blockchain ecosystem.

a. Blockchain developers.
b. dApp developers.

→ Blockchain developers build new blockchains with different levels of functionalities and Consensus Algorithms.

→ dApp developers work with decentralized applications that can run Blockchains thus Providing a similar functionality like Google Play Store over the Blockchain Technology.

→ The development of smart Contracts over the Blockchain has open Possibility for the developers to create extensive applications and use cases for the industries.

Blockchain Applications :-

→ Apart from exchange, Platform and users, another important aspect of the Blockchain ecosystem is the applications that industries, developers and communities build to serve a specific purpose.

→ There are various examples of Applications being build upon Blockchain, some of the major working applications are :-

- **Cryptokid :-** A decentralized document creation application.
- **Humanity :-** A fintech startup which connects unbanked people with global economy.
- **Augur :-** A Peer to Peer oracle and Prediction market Place.
- **Filament :-** Building the IoT applications over the Blockchain

o Bitcoin :-

→ It is a globally known crypto currency and digital Payment system.

→ First Decentralized Digital currency whose ledger is maintained by Blockchain openly and gave us the taste of the Blockchain.

→ It was founded by an unknown Person or group of People and released as open-source software in 2009.

→ Peer-to-Peer.

→ Transactions take Place between users directly. Without an intermediary.

→ Network nodes verify these transactions and record them in a Public distributed ledger called Blockchain.

* Features that differente Bitcoin from fiat currencies :-

• Decentralized System : The control of Bitcoin is not centralized. The nodes/ computers work

Together to mine the currency and process transactions which from the network, without any need of a central authority.

→ Simple Setup Process :- Regular banks make you go through a lot of processes to open an account. However, the configuration process of cryptocurrency is straightforward and free.

→ Anonymous and Transparent Usage : Users can have many Bitcoin addresses without a link to any personal identifying information. However, it records every transaction in a giant ledger called Blockchain.

→ Meager Transaction Fee : Bitcoin charges a minimal fee for international transfers.

→ Fast Network Process : The payment process is quick on the Bitcoin network.

→ Non-Refundable : once sent, Bitcoins cannot be refunded.

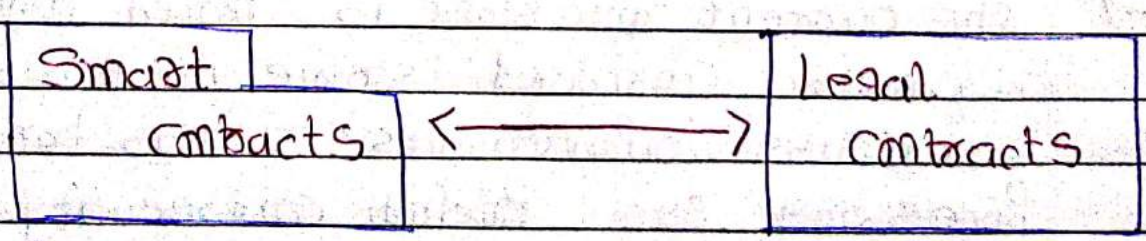
Ethereum :-

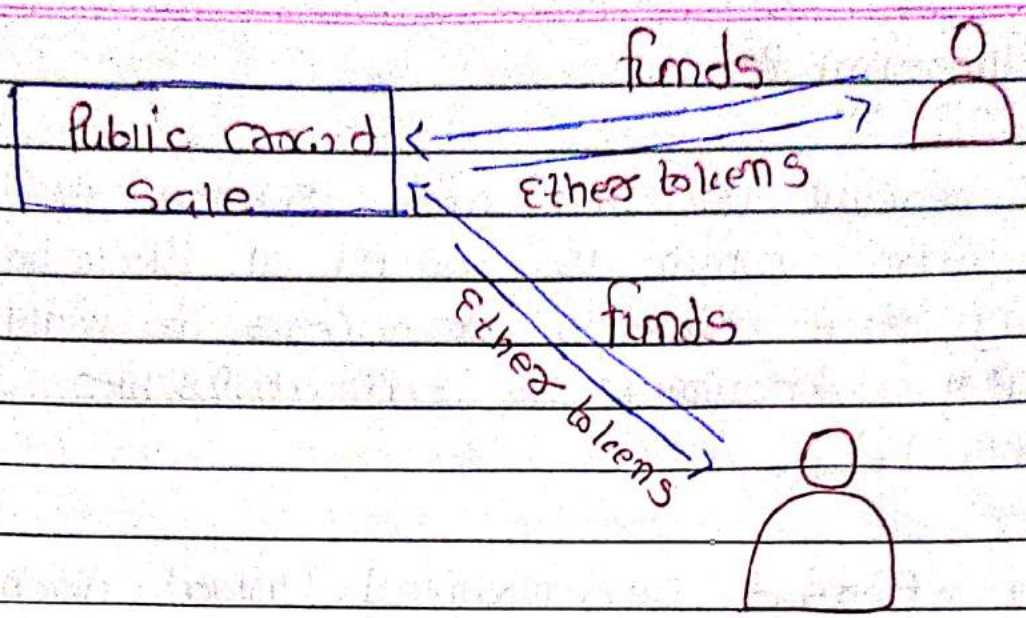
→ Ethereum is an open source software Platform which is based on Blockchain technology that enables developers to build and deploy decentralized applications like smart Contracts.

→ It offers a Decentralized Virtual Machine aka Ethereum Virtual Machine which can execute Scripts using a globally distributed network of Public nodes.

→ launched by Vitalik Buterin in late 2013.

→ The development for ethereum was funded by an online Public crowdsale during July-August 2014, by buying the Ethereum Token (Ether).





→ The first Public beta Pre-releases network known as "olympic." The olympic network Provides users with a bug bounty of 25,000 Ethers for stress testing the Ethereum Blockchain.

→ Ethereum's live Blockchain named "Frontier" was launched on 30 July 2015.

→ The current milestone is named "Homestead" and is considered stable. As it has led to various improvements such as transaction Processing, gas Pricing, and security.

→ There are at least two other Protocol upgrades planned for the future, i.e, Metropolis and serenity (Proof-of-stake).

Neo :-

→ NEO is a smart economy for the distributed network.

→ NEO was chosen as the name because "NEO" is Greek means "newness, novelty, and youth."

→ NEO was initially called Ant shares (ANS) which was launched in 2014, founded by Da Hongfei and Erik Zhang.

→ Antshares announced on June 22, 2017, that it planned to rebrand itself as NEO.

→ The first Ico on the NEO blockchain, Red Pulse Token (RPX) was announced soon after the rebranding finished.

→ Apart from the NEO cryptocurrency itself, the NEO Platform has another Crypto-token called "GAS" which was formerly called as "ANC-Antcoins."

* Hyperledger :-

→ Hyperledger is an open source created to advance cross-industry Blockchain technologies.

→ It is a global collaboration, hosted by the Linux Foundation, including leaders in finance, banking, internet of things, supply chains, manufacturing and technology.

→ Hyperledger acts as an operating system for marketplaces, data-sharing networks, micro-currencies and decentralized digital communities. It has the potential to vastly lessen the expense and complications in getting things done in the real world.

Private Blockchain solution with smart contract	Management of identities

* EOS :-

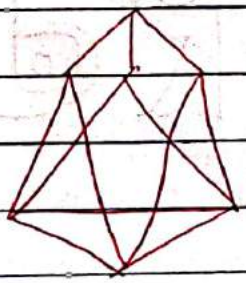
→ Eos is an operating system for market places, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly lessen the expense and

complications in getting things done in the real world.

→ Eos Blockchain aims to become a decentralized operating system which can support industrial-scale decentralized applications.

→ Eos is planning to delete transaction fees. Eos claims to have the ability to conduct millions of transactions per second.

→ Eos runs on DPoS consensus algorithm.



Eos

Corda :-

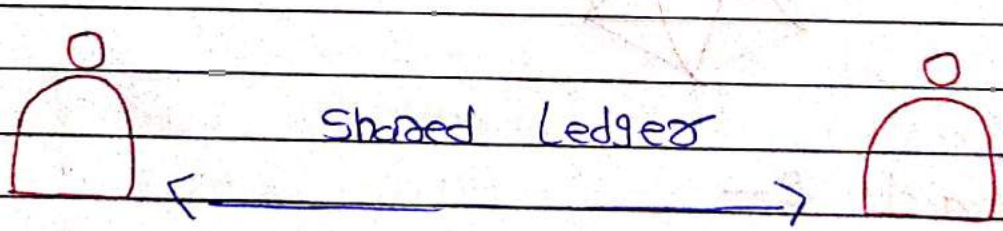
→ Corda is an open source blockchain aiming to meet requirements for use of blockchain in business.

→ Corda offers a solution where a shared ledger can be initiated between parties under the contract.

→ Corda's communications are Point-to-Point, meaning only participants of a transaction can see it.

→ With Corda's Point-to-Point architecture participants only have copies of the transactions they are participants to or observe as of. This means that every node in a corda network is likely to have a unique ledger. This is called as multilateral ledger.

CORDA



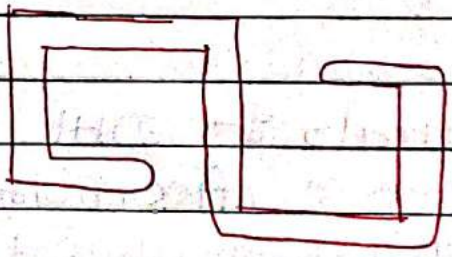
• Quorum :-

→ Quorum is the Baby child of J.P Morgan bringing in enterprise focused version of Ethereum.

→ Quorum Provides Private smart contract execution and enterprise grade performance.

→ Quorum uses zk-Snarks cryptography which allows verification of the computation correctness without even learning what was executed.

→ Quorum uses a hybrid Privacy design.



• Quorum •

* Multichain :-

→ Multichain was created by Gideon to make available a blockchain solution for organizations to build and develop fast.

→ Multichain is built upon Bitcoin Blockchain but offers the functionality of Permissions, Streams, and Assets.

→ Multichain also Provides other tools like explorers to interact with underline Block chain Seamlessly.

→ Bankchain is using Mutichain as it's base.

* Why do Industries need to adopt Blockchain ?

→

- Pharmaceuticals :- DHL worked with Accenture to establish a Blockchain-based track-and-trace system in six cities worldwide. Currently, the system has 7 billion unique Pharmaceutical serial numbers and handling more than 1,500 transactions per second.
- Fashion :- CAS has developed a system for tracking garments and compliances on raw materials for many apparels and fashion clients.

- Cross-Border Payments :-

→ IBM has developed a new Blockchain banking Solution that allows financial institutions to move quickly and cost-effe ctively Process Payments globally.

- Food-Safety :- IBM has developed a new Blockchain banking Solution that allows financial institutions to move quickly and cost- effectively Process Payments globally.

- United Nations :- United Nations is curre- ntly Blockchain for 16 agenci- es including Human Trafficking and World food Program.

- Jewelry :- Brilliant Earth has Partnered up with Everledger to use Blockchai- n in tracking and tracing the Provenance of diamonds of and other gem stones. This will also ensure that they are conflict- free.

* Blockchain Revolution :-

DAPPs & DAOs
- Autonomous decentralized applications
- Decentralized autonomous organizations
.... (?)

Tokens
- Smart Property
- Icos
- Smart Contracts

Coins
- Cryptocurrencies
- Payment services
- Trading of reserves
Beyond Payments

o Exciting Disruptions Coming Soon :-

- Entertainment Industry :- Mobie Braid was the first movie to be produced by doing an Icos.

- Property Rental :- Rentberry aims to address the common pitfalls and headaches of the traditional rental model.

- Politics :- Sierra leone carried out their elections on Blockchain.

- Education :- Socrates Coin is making big moves to change the traditional approach to a "3D internet".

- Digital Advertising :- Basic Attension Token is taking a crack to solve the problems with Digital Advertisements.

- Internet of Things :- Waltochain, an award winning chinese project that seeks to integrate IOT and blockchain technology on an unprecedented scale.

Industy challenges with Blockchain:-

* Energy Consumptions :-

→ Some major Public Blockchain use Proof-of-Work algorithms.

→ PoW involves the use of the computational Power of a machine to solve a complex mathemetical Puzzle to verify a transaction and add it to a block.

→ Currently Bitcoin energy consumption is almost equal to the consumption by Ireland.

→ By 2020 it's estimated that Bitcoin will utilize more energy consumption than the entire World currently uses.

→ A Probable solution for this has emerged in the form of different Concensus mechanisms like Proof-of-Stake, Delegated-Proof-of-Stake, etc.

Bitcoin Energy consumtion (annually):- 47.29 TWh	In January 2019, the 100% of minning reve mie was spent on Electricity. Making Bitcoin unProfitable to mine

* Scalability :-

→ Scalability has appered as a significant issue for the Blockchain networks like Bitcoin and Ethereum.

→ Blockchains are having trouble effectively supporting a large numbers of users on the network.

→ Moreover, the size of Public blockchain skeels on increasing, currently, Bitcoin ledger size is above 100 GB.

→ One Possible Solution which has emerged is storing a hash of data over the network.

* Public Perception :-

→ Presently, blockchain technology is almost is an synonymous with Bitcoin.

→ The majority of the public is still oblivious to the existence and potential uses of Blockchain technology.

→ As Bitcoin is anonymous and is used for shadowy dealings of money laundering, black market trade, and other illegal activities. The blockchain is also getting a bad reputation due to the same.

→ Mainstream adoption is needed to remove the sometimes- negative undertones of Bitcoin.

* Blockchain Standards and Regulations :

→ Blockchains are continuously evolving, but still, countries are skeptic about it as there is no proper definition for standards and regulations.

→ enterprises and Governments require regulations to protect their customers.

→ To tackle this problem, certain countries are trying to launch their regulations over the technology.

→ Mass adoption might also standardize the Blockchain.

Attacks over Blockchain :-

51% Attack :-

→ It states that group of miners controlling more than 50% of the network's mining hashrate, or computing power can take over the network.

→ It is a speculative attack described over Bitcoin blockchain.

→ Bitcoin Gold, at the time one of the top 30 crypto cu-

agencies suffered a 51% attack and lost $18 million.

→ Potential damage could be,

- The attackers would be able to prevent new transactions gaining confirmations, allowing them to halt payments between users.
- Attackers would also be able to reverse the transactions that were confirmed while they were in control of the blockchain network, meaning they could double-spend coins.
- The mining pool ghash.io was briefly exceeding 50% of the bitcoin network computing power in July 2014, leading the pool to commit to reducing its share of the network voluntarily.

Eclipse Attack :-

- This attack is based on Distributed application architecture that allocations tasks or workloads among peers without the need for a central coordinating server or stable hosts.

- Cripple a node in such a way that it can not talk to other nodes in the network.

- This attack is possible due to design strategy flaws in the Blockchain such peer's identity and peer selection strategy.

- Currently, Bitcoin has eight outgoing connections, and Ethereum has 13 which implies one node in Bitcoin only has access for eight nodes connected to it.

- So one node in Bitcoin has to depend on the other 8 for the complete view of the network which can be taken advantage by the hackers.

- Potential damage could be :-
  - Double Spending :
  - Attacks against second layer Protocols, e.g an attacker can obtain the Products / services without paying by tricking his victims into thinking that the Payment channel is still open while the non-edited part of the network sees that Payment channel is closed.
  - Smart contracts also may be attackable if users see inconsistent views of the Blockchain.

Sybil Attack :-

- In a sybil attack, the attacker attempts to fill the network with clients nodes that they control; if this happens then you could be most likely to connect with attacker nodes.

- Bitcoin never keeps a count of nodes for anything, If the attacker completely isolates a node from the honest network then it can help the attacker in the execution of other attacks.

- Potential damage could be :-
  - Attacker defuse the delay blocks
  - Attacker only delay blocks which he creates.

Timejacking Attack :-

- Timejacking attack is an extension of the Sybil attack.

- Each nodes internally maintains a network time counter.

- The counter is based on the median time of a node's Peers which is sent in the Version Message when Peers Connect.

- The network time counter reverts to the system time if the median time differs by more than 70 minutes from the system time.

- Potential Damage could be :-

  - An attacker could potentially slow down or speed up a node's network time counter by connecting multiple peers and reporting inaccurate timestamps.

  - Since the time value can be distorted by at most 70 minutes, the different between the nodes could be 140 minutes.

How Blockchain is taking over the World ?

- **World Domination :-**

→ The blockchain is already deployed in cold and continuously growing.

→ The 'World Economic Forum' anticipates that 10% of Global GDP will be Stored on the Blockchain by 2025.

→ The real Power of Blockchain is Yet to be unleashed.

Healthcare	Insurance	Banking
Payments	Entertainment	

* Real World Example :-

- Real Estate :- Blockchain is now being being used to complete real estate deals, the first of which was conducted in Kiev by Propy.

- Identification :- Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by Uport.

- **Railways :-** Russian rail operator RZD is storing inventory data on a Blockchain pertaining to repair requests and rolling stock.

- **Supply chains :-** IBM & Walmart have partnered in china to create a Blockchain Project that will monitor food safety.

- **Diamonds :-** The De Beers Group is using blockchain to track the importation and sale of diamonds.

- **Advertising :-** New York interactive Advertising Exchange has been experimenting with blockchain as a means of providing an ads marketplace for Publishers.

→ In a bid to boost its tourism economy, Hawaii is examining ways in which Blockchain-based crypto currencies can be adopted throughout the US state.

→ Arbit is blockchain based Project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

→ In china, a tax based initiative is using Blockchain to store tax records and electronic invoices led by Micanal Network.

- **Hyperledger Fabric :-**

— **What is Hyperledger ?**

→ HyperLedger is an open source collaborative effort created to advance cross-industry blockchain technologies. HyperLedger is an open source, collaborative software development approach which is pushing the Blockchain technology towards the mainstream adoption by Providing transparency, longevity, interoperability and support.

- **Hyperledger History :-**

→ HyperLedger launched in 2016 with 30 founding corporate members.

→ Hyperledger is built by Linux Foundations where developer and companies meet and collaborate to create a Blockchain framework.

→ Currently, Hyperledger is supported by more than 200 members including IBM, Intel, Cisco, SAP, Baidu etc.

→ Linux Foundations has also launched 7 to 8 open source organizations based on Hyperledger.

- **Hyperledger Framework :-**
- **Hyperledger Burrow :-**

→ Hyperledger Burrow provides a modular Blockchain client with a permissioned smart contract interpreter similar to Ethereum Virtual Machine. Initially contributed by Monax and co-sponsored by Intel.

- **Hyperledger fabric :-**

→ Hyperledger Fabric is lead by IBM. Hyperledger fabric is a plug and play implementation of blockchain technology with a flexible degree

of Permissions.

- **Hyperledger Grid :-**

→ Hyperledger Grid is an ecosystem of technologies, frameworks, and libraries that create together, letting application developers make the choice as to which components are most appropriate for their industry or market model. Cargill is investing it's resources for the development of Project.

- **Hyperledger Indy :-**

→ Hyperledger Indy is a distributed ledger, purpose-built for Decentralized identity. The Indy code base, originally developed by Evernym, was donated to the Sovrin foundation.

- **Hyperledger Iroha :-**

→ Hyperledger Iroha is emphasing on mobile application development and a new, chain-based Byzantine Fault Tolerant consensus algorithm, called Sumeragi. This Project is developed by Soramitsu, Hitachi, NTT Data and Colu.

- **Hyperledger Sacatooth :-**

→ Hyperledger Sacatooth is a modular Platform for building, deploying, and running distributed ledgers. Which includes a novel concensus algorithm called Proof of Elapsed Time. This consensus is effective for large distributed Validator Populations with minimal resource consumption. This Project is developed by Intel.

- **Hyperledger Tools :-**

1. **Hyperledger Composer :-**

→ Hyperledger Composer is a collaboration tool for building blockchain business networks, accelerating the development of smart contracts and their deployment across a distributed ledger.

2. **Hyperledger Explorer :-**

→ Hyperledger explorer creates user-friendly Web application where you can view, invoke

deploy or query blocks as well as any other relevant data stored on the ledger. This Project was originally contributed by IBM, Intel and DTCC.

3. Hyperledger Cello :-

→ Hyperledger cello aims to bring the on-demand "as-a-service" deployment model to the blockchain ecosystem to reduce the effort required for creating managing and terminating blockchains This Project was initially contributed by IBM, Soramitsu, Huawei and intel.

4 Hyperledger caliper :-

→ Hyperledger caliper is the Performance benchmark tool for the Hyperledger Projects, contributed by Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM and the Budapest University of Technology and Economics.

5. Hyperledger Quilt :-

→ Hyperledger Quilt offers interoperability between ledger system by implementing inter ledger Protocol, which is Primary of Payments

Protocol NIT Data and Ripple contributed to this Project.

6. Hyperledger Ursa :-

→ Hyperledger Ursa is a shared cryptographic library that could enable people and projects to avoid duplicating other cryptographic work. This project is jointly being worked on by Fabric, Indy and Sawtooth developers.

Introduction to Hyperledger Fabric :-

Hyperledger Fabric :-

→ Hyperledger Fabric is a platform for distributed ledger solutions built upon modular architecture providing high degrees of confidentiality, resiliency, flexibility, and scalability. It supports pluggable implementations of different components and accommodate complex economic ecosystems.

Key Benefits :-

→ Plug-a-Play ability to integrate components such as consensus algorithm and membership services.

→ smart contracts called 'chain codes', which are hosted using the container technology.

→ channel technology for confidential transactions. Allowing a group of participants to create a separate ledger of transactions.

→ Identity management through a trusted membership service Providers.

→ Permissioned and modular.

→ Database Services like Level DB and Couch DB.

• Hyperledger Fabric Functionalities :-

→ Hyperledger Fabric is an implementation of distributed ledger technology that delivers enterprise-ready network security, scalability, confidentiality and performance. Inc

modular blockchain architecture. Hyperledger Fabric delivers the following blockchain network functionalities :

→ Identity management
→ Privacy and confidentiality.
→ Efficient Processing
→ Chaincode functionality.
→ Modular Design.

○ Identity Management :-

→ Hyperledger Fabric Provides a membership identity service that manages user IDs and authenticates all participants on the network.

→ Moreover, Access control lists can also be used to Provides additional layers of Permission through the authorization of specific network operations. for example;

→ In case of Academic exams over the Hyperledger, only the Universities / Educational institutions have the Permissions to create new smart contracts as exams over the network. on the other hand, the students

have the read or invocation Permissions over the network where they can take the exam or see the results.

- **Privacy and Confidentiality :-**

→ HyperLedger Fabric enables competing business interests, and any groups that require Private, Confidential transactions, to coexist on the same Permissioned network.

→ HyperLedger allows the creation of Private channels that Provides transaction Privacy and confidentiality for specific Subsets of network members.

→ All the data over the HyperLedger network can be made inaccessible unless the Proper Permissions are Provides to the network Participant.

- **efficient Processing :-**

→ HyperLedger Fabric Provides concurrency and Parallelism to the network by separating transaction execution from transaction ordering and transaction commitment.

→ This concurrent execution increases processing efficiency on each peer and accelerates delivery of transactions to the ordering service.

→ Besides enabling parallel processing, the separations of transactions to the ordering service, execution and ledger maintenance, while peer nodes are freed from consensus, workloads.

Chaincode functionality :-

- Chaincode applications encode logic that is invoked by specific types of transactions on the channel.
- Chaincode used for a change of asset ownership ensures that all transactions that transfer ownership are under the same rules and requirements.
- Hyperledger also has the system chaincode that defines operating parameters for the entire channel.

- Modular Design :-

→ Hyperledger implements a modular architecture in the form of pluggable components.

→ You can plugin specific algorithms for identity, ordering (consensus) and encryption into any Hyperledger Fabric network.

→ The resultant network is a universal blockchain architecture that can be adopted across different markets, regulatory and geographic boundaries.

- Pros and Cons of Hyperledger Fabric :-

- Pros :-

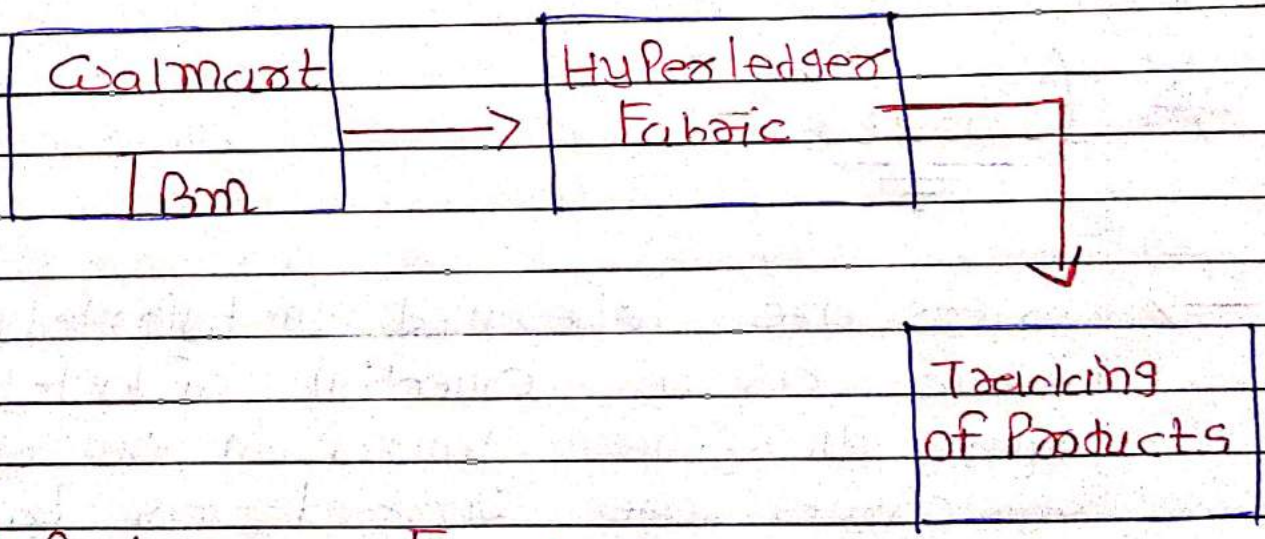
- Permissioned membership feature available where you can maintain the identities of participants.

- Performance, Scalability and high level of trust.
- Rich queries feature available over the ledger. This helps you to query the ledger in the most layman terms possible.
- Module architecture, with Plug-in components available.
- Protection of Digital keys given to the users and sensitive data, Moreover, certificates provides one additional layer of security.
- Hyperledger organizational structure elevates and incentivizes infrastructure work.
- Rich and open opportunities for more development and support.
- A strong team and community back it.

- **Cons :-**

- It is relatively new, thus not yet adopted throughout the blockchain ecosystem.

- There is no coin or cryptocurrency involved over Hyperledger. Although it's possible to develop native digital tokens, native currencies like Bitcoin or Ether are not supported.
- Hyperledger is focused exclusively on enterprise transaction-based applications.
- Still under adoption, although PoCs are available but complete deployment is still lacking.



- Hyperledger Fabric key Features

- Key Features :-
- Hyperledger Fabric outlines the key design features as following.

- Assets
- chaincode
- Ledger features
- Privacy (channels)
- Security and membership services.
- Consensus.

✱ Assets :-

→ Assets are represented in Hyperledger Fabric as a collection of key-value pairs. All the changes in the state of assets are recorded as transactions on a channel ledger where assets are defined.

→ Assets can be tangible entities like hard drives, USBs, etc. to intangible objects like contracts etc. Hyperledger Fabric provides the creation of assets using chaincode

and Hyperledger composer tool.

→ Assets in Hyperledger can be represented in either binary or json format.

✡ Chaincode :-

→ chaincode is the other name for the smart contracts in Hyperledger.

→ chaincode defines the business logic between multiple parties over the Hyperledger Blockchain network.

→ only chaincode can add or update data over the Hyperledger network.

→ chaincode must be installed on every single Peer of a channel or an organization.

→ There can be multiple chaincodes with different policies.

- chaincodes are two types :-

- Developed chaincode :- This is written in Go, Node.js and Java Programming language and deployed by users over the network to Perform business logic or specific functionalities.

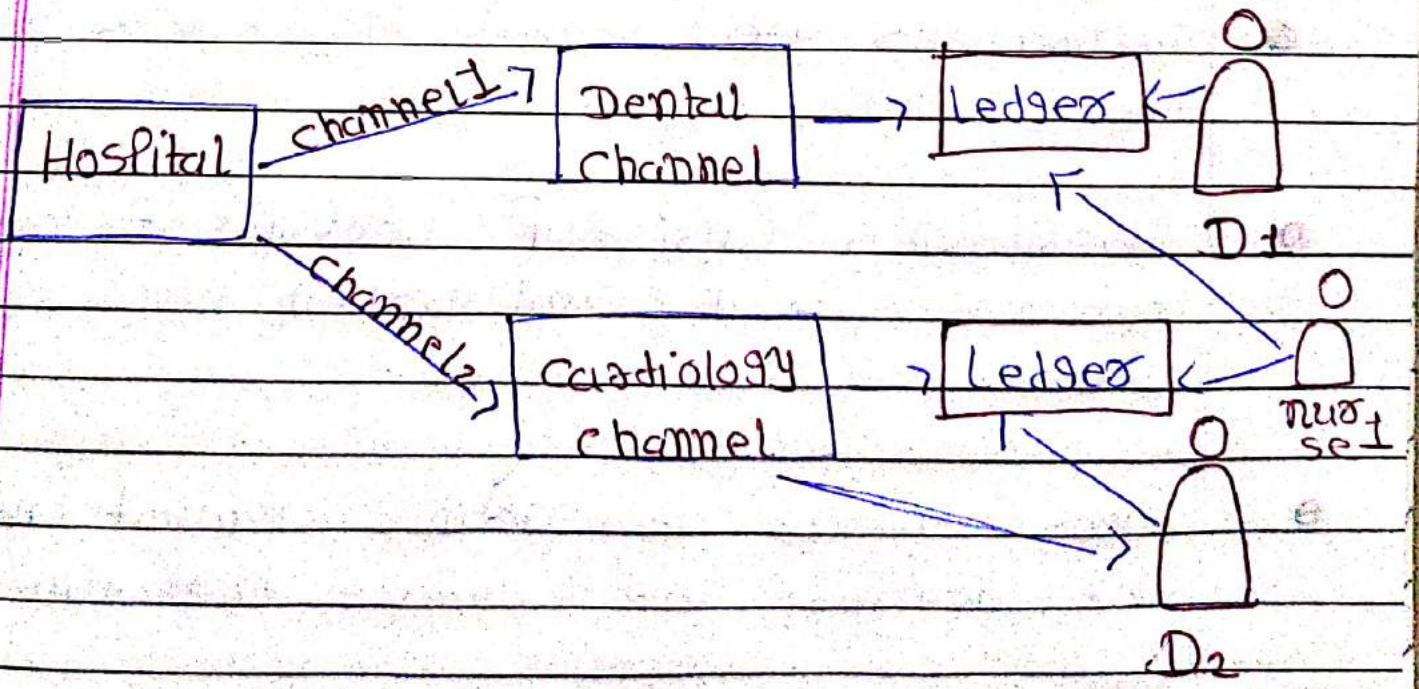
- System Chaincode :- This is used by the core of Hyperledger in managing the blockchain network to Intall, initiate and Update the network entities.

Ledger Features :-

→ The ledger is the Sequenced, tamper-resistant record of all state transitions in the fabric, State transitions are the resultant of chaincode Invocations Submitted by Participants.

→ A seperate ledger is maintained Per channel, and it Stores the Permenent, Sequenced record in blocks, as well as a State database to maintain current fabric state. Each Peer keeps a copy of the ledger for each channel of which they are a member.

- Transactions are ordered into blocks over the ledger.
- Transactions consist of versions of key/value that are read and written into chaincodes.
- Peers validate transactions against endorsement policies, and enforce the rules.
- A channel's ledger contains a configurations block defining policies, access control lists, and other pertinent information.
- Query and update of the ledger is done by using key-based lookups, range queries and composite vital queries.



Ledger Features :-

→ The ledger is the sequenced, tamper-resistant record of all state transitions in the fabric. state transitions are the result of the chaincode invocations submitted by participants.

→ A seperate ledger is maintained per channel, and it stores the permenent, sequenced record in blocks, as well as a state database to maintain current fabric state. Each peer keeps a copy of the ledger for each channel of which they are a member.

- Transactions are ordered into blocks over the ledger.
- Transaction s consist of versions of key/value that are read and written into chain codes.
- Peers validate transactions against endorsement Policies and enforce the rules.

- A channel's ledger contains a configuration block defining Policies, access control lists, and other pertinent information.
- Query and update of the ledger is done by using - key-based lookups, range queries, and composite key queries.

Privacy (channels) :-

→ Hyperledger Fabric key benefit is the privacy which is provided through channels. channels are similar to private network hosting their ledger. these two or more members can conduct private and confidential transactions :-

- Hyperledger Fabric employee a ledger per channel.
- chaincode are present to modify the state of ledger over the channels.
- A ledger exists in the scope of a channel.
- Participants can connect to one or more channels in a Fabric network.

- Data can further be obfuscated by encrypting the data before putting up on a channel.

- channels provide fabrication of assets and participants over the Fabric network.

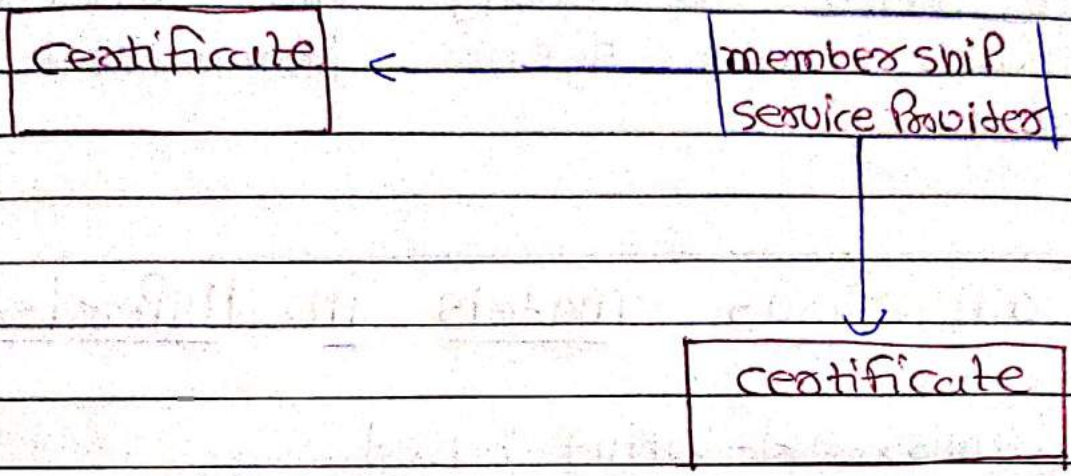
Security and Membership Services:

→ Hyperledger Fabric governs the participants with their identities. These identities are generated through a trusted membership service provider (MSP).

- Public key infrastructure is used to generate cryptographic certificates which are tied to organizations, network components and users or client applications.

- Data access control can be manipulated and governed on the whole network and channel levels, using the cryptographic certificates.

- Privacy and confidentiality can be maintained by combining channels and membership services.



- **consensus :-**

→ The consensus in Hyperledger Fabric network is a process where the nodes or computers in the network provides a guaranteed ordering of the transaction and validation of block that needs to be commited to the ledger. Consensus must ensure the following in the network.

- confirms the correctness of all transactions in a proposed block, according to endorsement and consensus policies.
- Agrees on order and correctness and the results of execution of the smart contract.

- Interfaces and depends on the smart-contract layer to verify the correctness of an ordered set of transactions in a block.

- **Consensus models in Hyperledger:-**
  - Permissioned - Voting - based
  - Lottery based

★ **Identity and Membership:-**

→ Hyperledger Fabric let's you create a distributed network consistings of many nodes which communicate with each other. The blockchain has the chaincode, ledger data and executes transactions over it. Apart from that we maintain the identities using membership service provide. Following are the components that makes up the complete Fabric architecture.

- Identity and membership:-
  - Ledger
  - Nodes
  - Private Data
  - Smart-contracts (chaincodes)

What is an Identity?

→ Identity is a unique digital fingerprint which is used to identify network participants. With HyperLedger, each of the network actors who consume blockchain services has a digital identity encapsulated in an x.509 digital certificate.

→ These identities determine the exact permissions over resources and access to information that actors have in a blockchain network. Identities also have a wide range of properties for an actor, such as the actor's organization, organizational unit, role or even the actor's specific identity. These properties are used to determine permissions.

→ The default MSP implementation in fabric uses x.509 certificates as identities.

Certificates → Public key + Private key

- Identity Example :-

→ User creates the profile using a mobile or desktop app.

User add the Government issued identity documents, which will be mapped in application as a unique digital identity.

User and organisations can connect to the application to retrieve the user details.

Data can be encrypted before storing at secure storage.

What are PKIs ?

→ A Public key Infrastructure (PKI) is a collection of internet technologies that provide secure communications in a network. PKI is the one that puts the S in HTTPS. If you're watching this video on a web browser, you're probably using a PKI to make sure it comes from a verified source.

Key Elements of PKIs :-

— These are four key elements to PKI:-

- Digital certificates.
- Public and Private keys.
- certificate Authorities.
- Certificate Revocation Lists.

PKIS - Digital Certificates

→ A digital certificate is a document which holds a set of attributes relating to holder of the certificates. The most common type of certificates is the x.509 standard which allows the encoding of an actor's identifying details in its structure.

→ Digital certificates is created using cryptography. Any tampering will invalidate the certificates. Crypto graphy allows the actors to present their certificates to others to prove her identity as long as the other party trusts the certificate issuer, known as a certificate Authority. Till the point CA keeps specific cryptographic information secretly, any one reading the certificates can be sure that the information about the actor has not tampered.

- Public and Private keys :-

→ The keys are used to provide integrity and authentication.

- Digital signature mechanisms required each party to hold two cryptographically connected keys: a public key that is made available to participants and acts as authentication anchor and a private key that is used to produce digital signatures on messages.

- Recipients of digital signed messages can verify the origin and integrity of a received message by checking the signature with the public key of the expected sender.

- Asymmetric cryptography is used here, which is a one-way process where you can generate the public key from the private key, but vice versa is not possible.

* Certificates Authorities :-

→ As we know that actors participate in the network using digital identities which are in the form of certificates, these certificates are generate

d by Certificate Authorities.

→ CAs are very common on the internet, for example, most websites use, GeoTrust, Digicert, GoDaddy, or comodo.

- Certificate Autorities - chain of trust.

Root RcA	intermediate IcA1	intermidiate IcA2	intermidiate IcA3

- Certificate Revocation Lists :-

→ A certificate Revocation List is a list of references to certificates that a CA knows to be revoked for one reason or another.

- When a third Party wants to verify another Party's identity, it first checks the issuing CA's CRL to make sure that the certificates has not been revoked.

- A verifier doesn't have to check the CRL, but if they don't, they run the risk of accepting a compromised identity.

- **Membership Service Provider :-**

→ Membership service Provider (MSP) identifies which Root CAs and intermediate CAs are trusted to define the members of a trust domain in the hyperledger network. For example an organization, either by listing the identities of their members or by identifying which CAs are authorized to issue valid identities for their members.

- **Key functions :-**

- List who is a network participant or member of a channel.

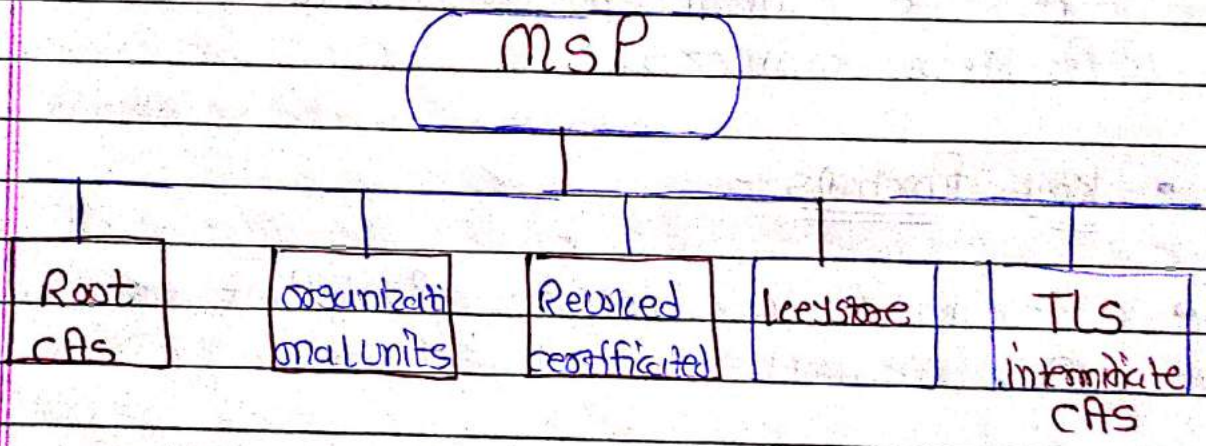
- Identify specific roles a participant might play in the network.

- Sets the basis for defining access privileges in the context of a network and channel.

- Identify the Participants whose certificates have been revoked.

→ MSP is available at different levels. for example: Channel MSP maintains the configuration of all Participants over a channel and a local MSP is specific to a individual.

- **MSP Structure :-**

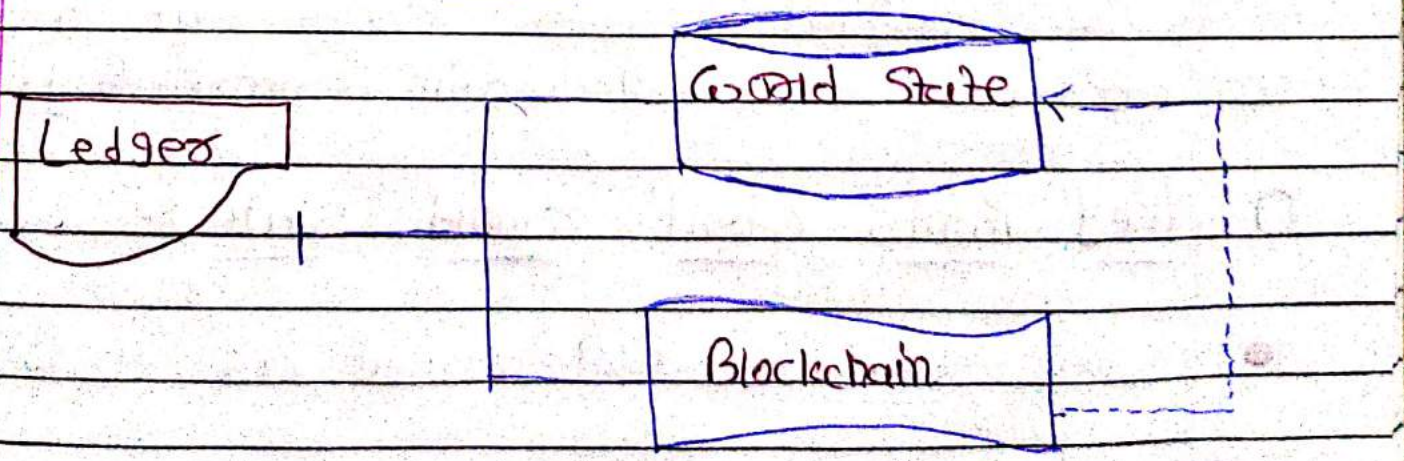


- **Ledger :-**

→ A ledger contains the current state or totaling of a business as a journal of transactions.

- **For example :-** A bank account statement. You can see your available balance. That's the amount you can spend at the current moment in time. If you want to see how your balance gets derived, then you can look through the transaction credits and debits that determined it. This is a real-life example of a ledger which has a set of ordered transactions that defines it.

- **Hyperledger Fabric Ledger :-**



Hyperledger Fabric Ledger :-

→ Hyperledger Fabric ledger consists of key value pairs which represent the data. There are two distinct parts to represent the ledger :-

- **World State :-** This is database that holds a cache of the current values of ledger states. The World State makes it easy for a program to directly access the current value of a state or data rather than having to traverse the entire database.
- **Blockchain :-** This is the transaction log that records all the changes that have resulted in the current World State. Transactions are collected inside blocks that are appended to the Blockchain immutably.

Key Points about World State :-

- World State is implemented as Database.

- World state is updated last transactions.
- When a new network is created, world state is empty.
- World state can be re-generated from the block chain at any time.

→ Key Points about Blockchain :-

- Blockchain is a historical records of the states which shows how we arrived at their current states.
- The Blockchain is structured as sequential log of interlinked Blocks, where each block contains a sequence of transactions.
- The blockchain is always implemented as a file in hyperledger, in contrast to the world state, which uses a database.

- **Blockchain Blocks :-**

→ A Block in Hyperledger consists of 3 main data sets.

- **Block Header :-** This mainly consists of current Block Hash, Previous Block hash and Block number.

- **Block Data :-** This section contains a list of transactions arranged in order.

- **Block Metadata :-** This section contains the time when the block was written, as well as the certificate, Public key, Signature of the Block Writter and Validation flags for each transaction.

- **Transactions :-**

  - **Header :-** This is metadata for transaction. For example : chaincode which is called and it's version.

  - **Signature :-** This is a cryptographic signature created by the client application.

2024

- **Proposal :-** This encodes the input parameters supplied by an application to the smart contract which creates the proposed ledger update.

- **Response :-** These are before and after values of world states.

- **Endorsements :-** This is a list of signed transaction responses from each required organization sufficient to satisfy the endorsement policy.

- **Channel :-**

→ A Hyperledger Fabric channel is a private "subnet" of communication between two or more specific network members, for the purpose of conducting private and confidential transactions.

- Every channel owns their separate ledger.

- Each transaction on the network is executed on a channel, where each party must be authenticated and authorized to transaction

2005

that channel.

- Peers can be Part of mutiPle channels, thus halding mutiPle ledgers caith them.

✡ Nodes and Peers :-

→ HyPerledger Fabric let's you create a distributed network consisting of many nodes cahich communicate caith eachother. The blockchain has the chain code, ledger data and executes transactions over it, a Part from that we maintain the identities using membership Service Provide. Following are the component that makes uP the compiete Fabric architecture:

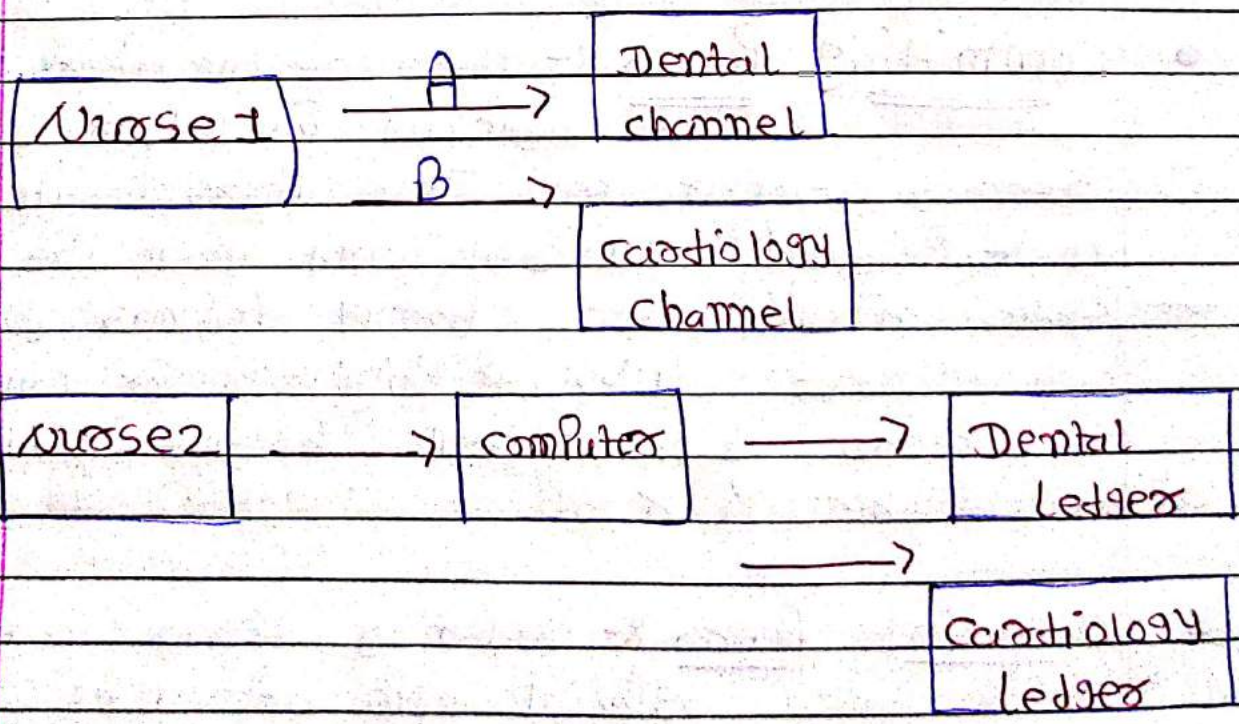
- PeersC Nodes)

- What are Peers ?

→ A blockchain network is comPrised of computers cahich are known as Peer nodes; each of these Peers can hold coPies of ledgers and Smart contracts.

→ Peers in Hyperledger can be created, started, stopped, reconfigured, and deleted. They expose a set of APIs that enable administrators and applications to interact with Hyperledger services like ledger and chaincode.

→ A peer can host more than one ledger and chaincode, which is helpful because it allocas for flexible system design and modularity.



- Types of Peers :-

- There are three types of Peers in hyperledger fabric :-

- Endorsing Peers :- Endorsing Peers are those Peers which simulates transactions and checks it's validity. After simulation they sign the transaction to verify that they have validated the transaction.

- Committing Peers :- These are the Peers which maintain full ledger of records at their end. These Peers create the distributed network and main the states of different channel ledgers. You can different types of Privileges for committing Peers to make them behave as admin or anchor Peer.

- Ordering Peers :- Ordering Peers are special type of nodes whose key roles are to receive endorsed transactions from SDKs, Package them into blocks as per the configuration file and send it to all other Peers so that they can validate

those transaction and update their ledgers.

o Private Data :-

- What is Private Data ?

→ Initially to have data private on HyperLedger form other participants, you need to create a channel, but this creates an overhead of maintaining channels from version 1.2, a new capability was introducted to manage private data known as private data collections.

→ Private data collection, allows a defined subset of organizations on a channel to endorse, commit, or query private data without having to create a separate channel.

o A collection is the combination of two elements :-

→ The actual private data which is sent peer-to-peer via gossip protocol to only the organization (s).

authorized to see it. This data is stored in a closed state database on the peers of authorized organizations, which can be accessed from chaincode on these authorized peers. The ordering service is not involved here and does not see private data.

→ A hash of that data, which is endorsed, ordered and written to the ledgers of every peer on the channel. The hash serves as evidence of the transaction and is used for state validation and can be used for audit purposes.

Private Data Example :-

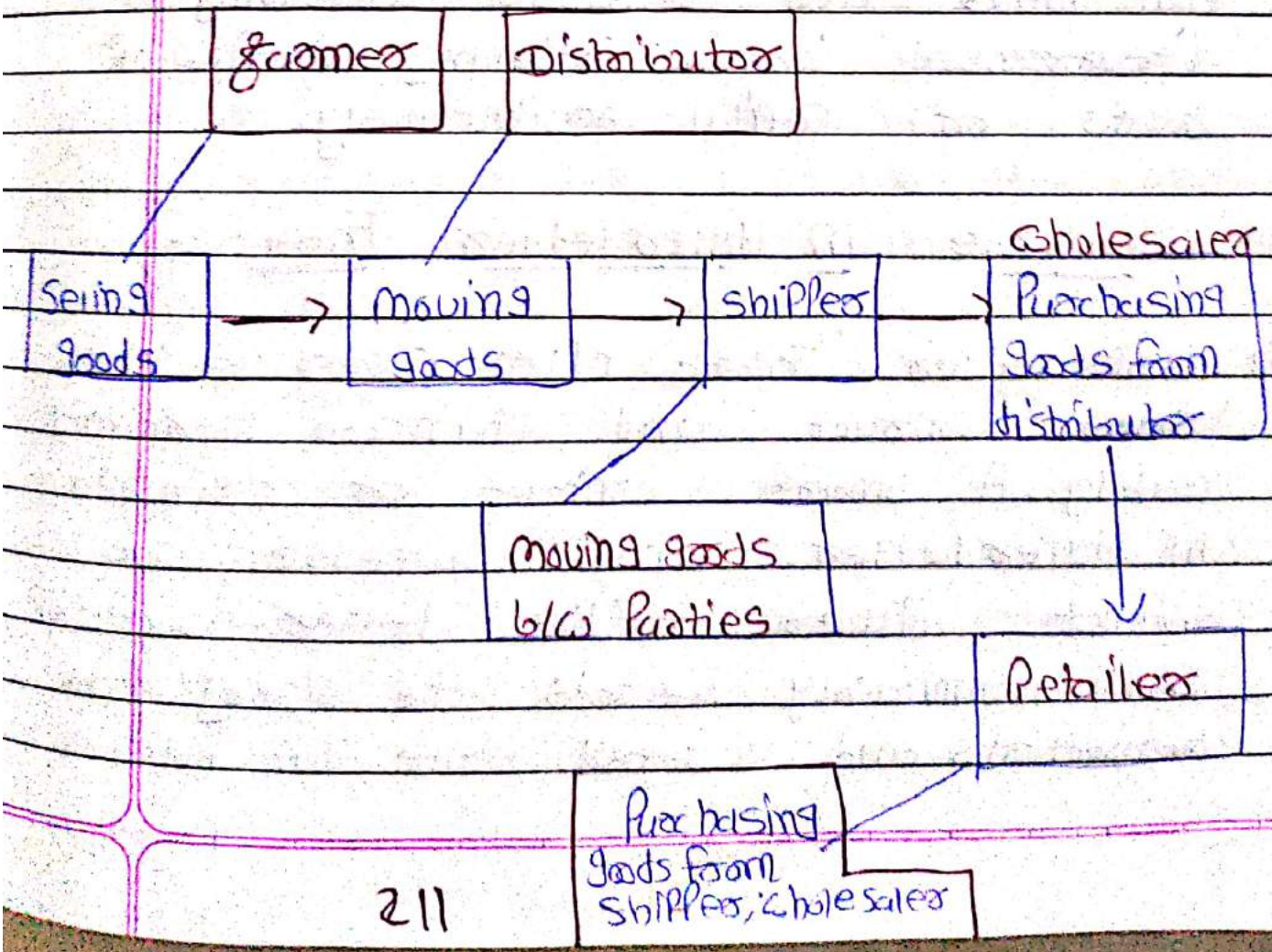
→ Consider a group of five organizations on a channel who trade produce.

- A farmer selling his goods abroad
- A Distributor moving goods abroad
- A shipper moving goods between parties
- A wholesaler purchasing goods from distributors.

- A retailer Purchasing goods from shippers and Wholesalers.

— The following Private data collections can be created between them.

- PDC1: Distributor, Farmer and Shipper
- PDC2: Distributor and wholesaler
- PDC3: Wholesaler, Retailer and shipper



* Chaincode (Smart Contract) :-

- What are Smart Contracts ?

→ Smart contracts define a standard set of rules covering common terms, data, rules, concept definations and processes laid out between multiple Parties in the form of execution code.

→ for example, a Smart contract might ensure that a new car delivery is made within a specified timeframe, or that funds are released according to Pre-programmed terms, improving the flow of goods or capital respectively.

o Chaincode in Hyperledger Fabric :-

→ Hyperledger Fabric often uses the terms smart contract and chaincode interchangeably. A smart contract or chaincode in Hyperledger may access two distinct pieces of the ledger - a blockchain, which immutably records the history of all transactions and a world state that holds a

cache of the current value of these states.

→ Smart contracts primarily put, get and delete state in the world state, and can also query the permanent blockchain record of transactions.

- A get typically represents a query to retrieve information about the current state of a business object.
- A put typically creates a new business objects or modifies an existing one in the ledger world state.
- A delete typically represents the removal of a business object from the current state of the ledger, but not its history.

- **Technical overview of chaincode :-**

- Chaincodes are developed in Go, Java and Node.JS programming language for now and Hyperledger is working to enter other languages too.

- chaincode runs in a secured Docker container isolated from other Peer processes.
- chaincode instantiate and update ledger states through transactions submitted by clients.
- chaincode must be installed and instantiated on all the agreed upon Peers of the network.
- A chaincode can be invoked to update or query the ledger state via transaction proposal.
- A chaincode may invoke another chaincode, either in the same channel or in different channels to access variable states.

→ Docker is a computer program that performs operating-system-level virtualization.

→ chaincode also defines the roles for the Peers.

Key Points about chaincodes :-

- Every chaincode has an endorsement policy that applies to all of the smart contracts which defines the organizations in a blockchain network that must sign a transaction generated by a given smart contract in order for that transaction to be declared valid.

- The contract takes a set of input parameters called the transaction proposal and uses them in combination with its program logic to read and write the ledger.

- A chaincode transaction that is distributed to all peer nodes in the network is validated in two phases.

  - The transaction is checked to ensure it has been signed by sufficient organizations according to the endorsement policy.

  - It is also checked to ensure that the current value of the world state matches the read set of the transaction when it was signed by the endorsing peer nodes. This is to make sure that there has been no intermediate update.

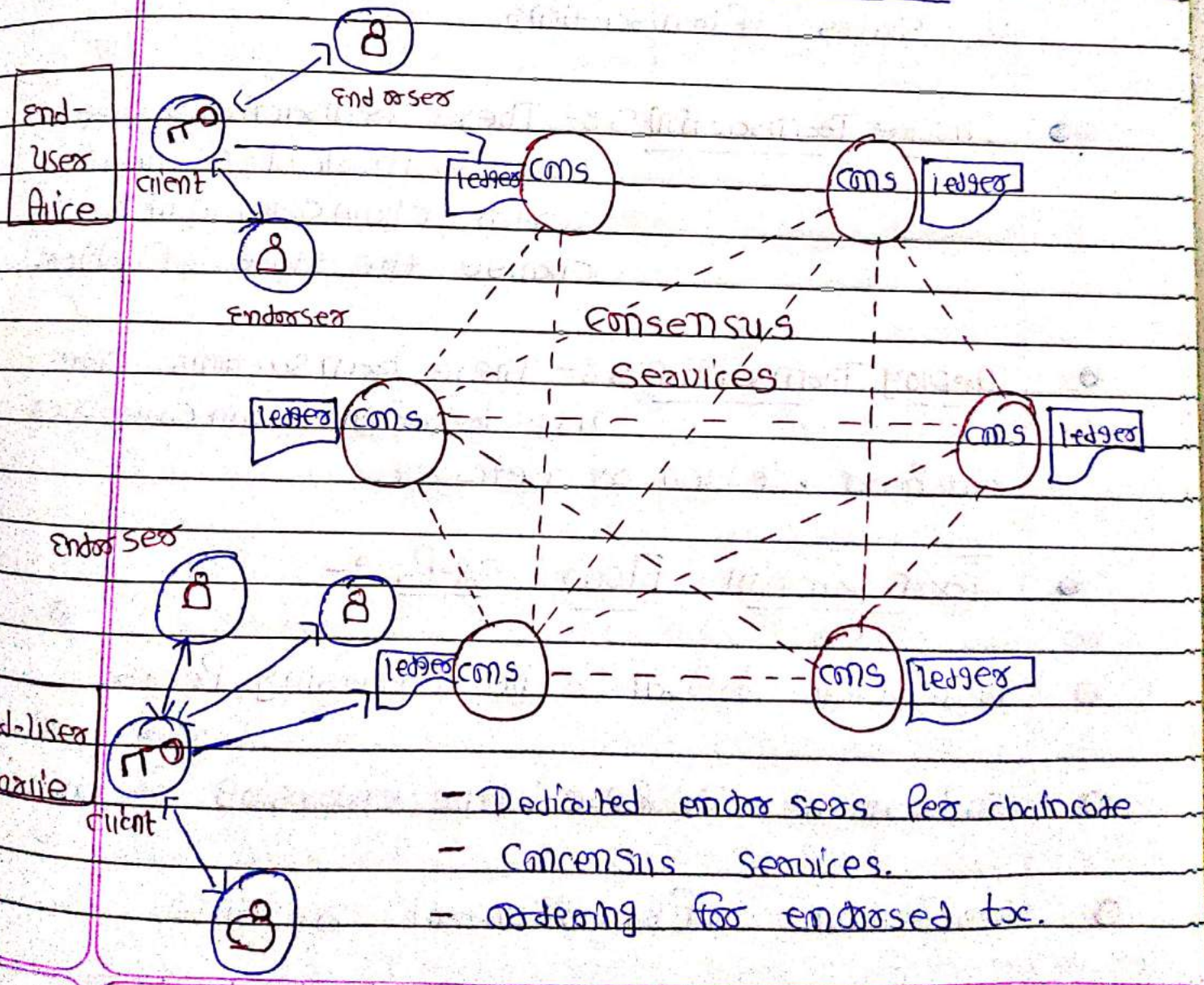
- Smart contracts are able to call to other smart contracts both within the same channel and across different channels.

Chaincode Lifecycle :-

- Participants over the ledger must agree on a chaincode before it can be used.
- Participants also review the chaincode and sign it to prevent tampering.
- chaincode is passed around using the package format which includes the source code, the policies and the list of entities that have agreed and signed on the chaincode.
- only Peer endorsed chaincode can be installed and instantiated over the Peers in the Network.
- chaincode is installed over Peers using Docker containers.
- Peer instantiated with chaincode is responsible for managing the chaincode lifecycle.

→ There's also special kind of chaincode called System Chaincode which is part of the system process. it is used to implement low-level ledger features like the endorser system, query system, and validation system.

- **HyPerledger Fabric Architecture :-**



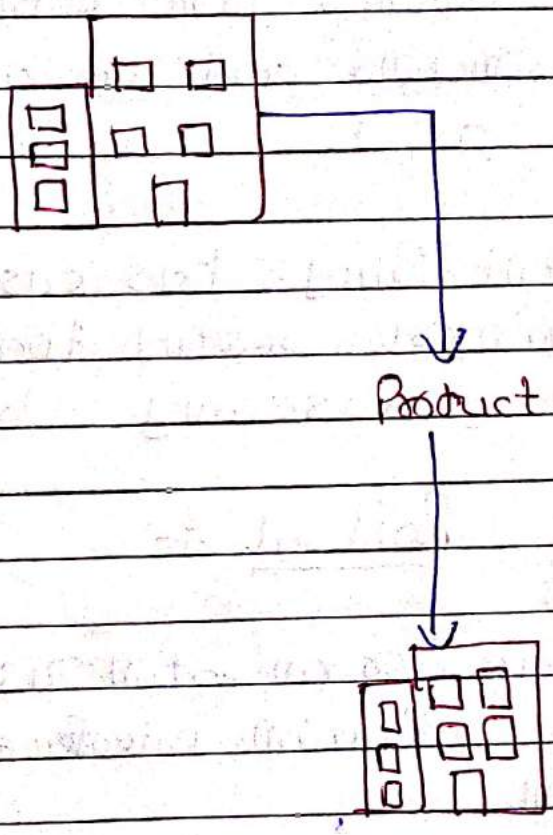
- Dedicated endorseers per chaincode
- Concensus services.
- Ordering for endorsed tx.

Hyperledger Fabric Transactions :-

→ All the updates over the ledger are performed through transactions. A transaction is invoked when we are calling a function under the chaincode. Transactions are the major entities that deliver the actual data for clients and applications. With Hyperledger Fabric, we have 2 types of transactions.

- **Invoke Transactions :-** These transactions are use to invoked a function under chaincode, which change the state of ledger.
- **Deploy Transactions :-** These transactions are use to deploy chaincode over the peer, ledger or network.
- **Transaction Flow Steps :-**
  - Transaction Proposal to the endorsing Peers.
  - Endorsment response by the endorsing Peers.
  - Verification of Endorsement response.

- Invocation request to the ordering services.
- invocation response to the Peers by validating and committing the transactions.
- ledger gets updated.



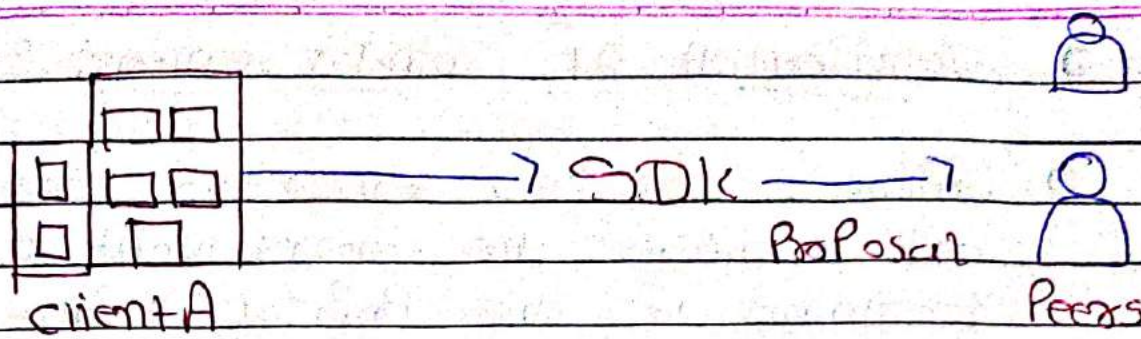
- Transaction Flow Assumptions.
- channel is properly setup and running.
- The application user has registered and enrolled with the organization's certificated authority (CA) and received back necessary cryptographic.

material, which is used to authenticate to the network.

- The chaincode is installed on the Peers and initiated on the channel.
- The chaincode contains logic defining a set of transaction instructions and the agreed upon price for an asset.
- An endorsement policy has also been set for this chaincode, stating that all the Peers must endorse any transaction.

- Transaction Proposal :-

- A client or an organization uses Hyperledger SDK or an application interface to initiate the transaction.
- Transaction Proposal is prepared and is sent to endorsing
- The Proposal is a request to invoke a chaincode function so that data can be read and/or written to the Peer ledger.



- **Endorsement Response :-**

- Endorsing Peers check for the validity of the format of the transaction Proposal, for the duplicity of the transaction Proposal, the signature and authorization of the requesting client is checked using membership service Provider.

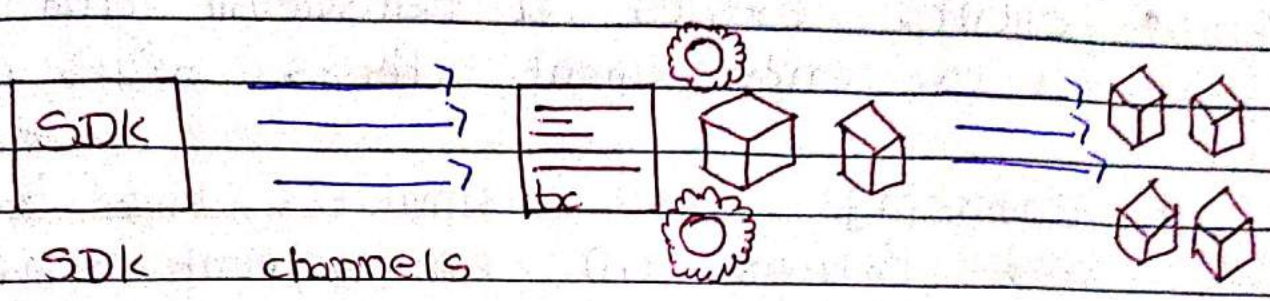
- endorsing Peers take transaction Proposal inputs as arguments and Pass to chaincode function for simulation.

- chaincode gets executed against the current state database to Produce response value, read set, and write set.

- These sets along with the endorsing Peer's signature is Passed back as a "Proposal response" to the SDK.

- **Verification of Endorsement :-**
  - Application verifies endorsing Peer signatures and compares the endorsement response to determine if the Proposal response are the same.
  - If application only queried the ledger, then the query response is inspected.
  - However, the application determines if the Specified endorsement Policy has been fulfilled before submitting the transaction to ordering services.
  - **Broadcasting to ordering Service :-**
    - The application "broadcasts" the transaction Proposal and response within a "transaction message" to the ordering service.
    - The transition contains the read/write sets, the endorsing Peers signatures and the Channel ID.
    - The ordering service simply receives transactions from all channel is the network, orders

them chronologically by channel, and creates blocks of transactions per channel.

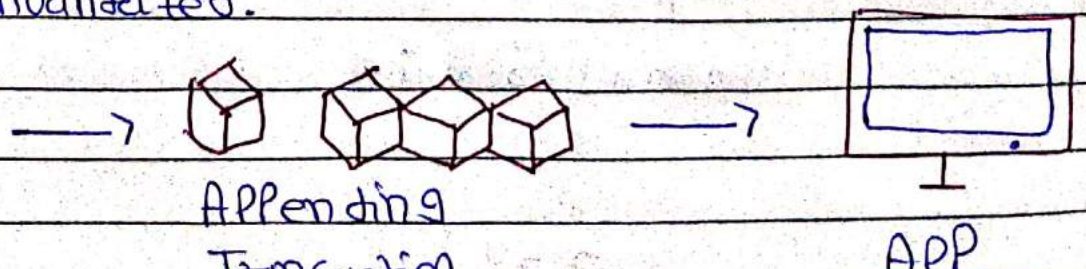


- **Ledger Updated :-**

- All the Peer appends the block to the channel's chain.

Writes Sets are committed to current state database for all valid transactions.

- An event is emitted to the application that invocation response has been immutably appended to the chain, as well as notification of whether the transaction was validated or invalidated.



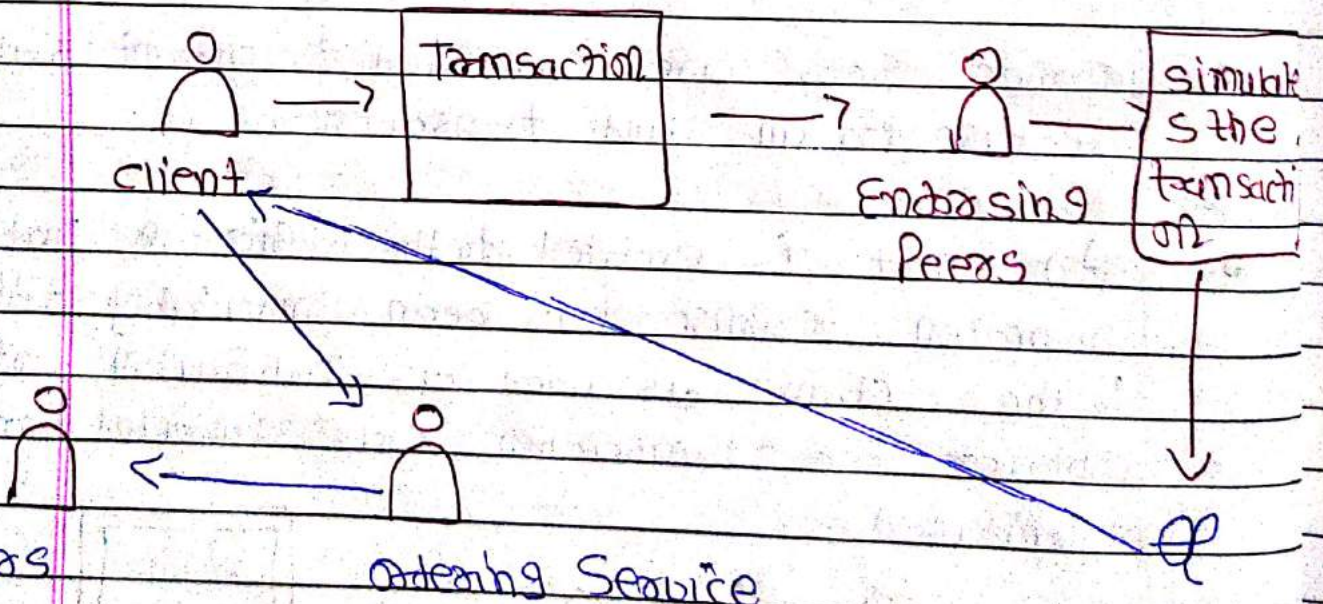
- Endorsement Flow :-

- clients creates a transaction and send it to endorsement Peers of its choice.

- Endorsing Peers simulates the transaction and Produces an endorsement signature.

- Client collects the endorsement signatures for a transaction and broadcasts it through an Ordering Service.

- Ordering Service delivers the transactions to Peers.



Client Creates a transaction Proposal :-

→ Client initiates the process by submitting a Purpose message to the endorsing Peers of it's choice.

→ The set of endorsing Peers are made available to the client which are available under endorsement Policy.

- The format of a PROPOSE message is < PROPOSE, tx, [anchor] >, where tx is a mandatory and defined as < client ID, chaincode ID, txPayload, timeStamp, clientSig > and anchor optional argument contains read version dependencies (which is used to bind the transaction to specific key value entry within the ledger.

- txPayload is also defined as < operation, metadata >, where operation is the specific function from the chaincode and metadata is additional information. for the invocation. For deploy transaction txPayload is < source, metadata, Policies >

→ Client decides the sequence of transactions with endorsers. For example they can send only the transaction without anchor to one endorser. Later endorser can compute the anchor and client can user that anchor to communicate with other endorsers.

⓪ Simulations of Transaction :-

→ Once the endorsing peers receive the <PROPOSE, tx, [anchor]>, it verifies the client, signature and simulates the transactions.

→ Simulating a transaction involves endorsing peer executing a transaction by invoking the chaincode over the copy of state that endorsing peer holds locally. This gives the peer the change of state in readset and writeset.

→ If a client specifics anchor in the PROPOSE message then client specified anchor must equal readset produced by endorsing peer when simulating the transaction.

- Important :- endorsing Peer do Not update its State, it only interprets the transaction records accessed by chaincode for reading and writing.

→ If a client specifices anchor in the PROPOSE message then client specified anchor must equal readset produced by endorsing Peer when simulating the transaction.

- Endorsement Generation :-

→ After simulating the transaction the endorsement Peer forwards the transaction PROPOSAL internally to the endorsing logic.

→ endorsing logic accepts the transaction PROPOSAL and signs, following messages are sent back through endorsing logic.

- if the transaction is accepted :-
- if the transaction is rejected :-

Where :-

- tran-Proposal := (ePID, tid, chain code ID, tx content Blod readset, writeset), ePID is the endorsing

Peer ID, tid is the transaction ID, chain codeID, is the chaincode called, trcontent Blob is transaction specific information.

- epsig is the endorsing Peer signature on the tran-Proposal.

Collection and Broadcasting :-

→ The submitting client waits until it receives 'enough' messages and signatures on (TRANSACTION-ENDORSED, tid, *, *) statements to conclude that the transaction Proposal is endorsed. It depends upon the chain code endorsement Policy.

→ If the client do not receive enough transaction Proposals then the client abandons the transaction with the option of retry.

→ if the endorsement Policy is satisfied then the client invokes the ordering Service by Pussing the endorsement blob to the ordering Service

- Following event occurs:-

broadcast (blob), where blob = endorsement.

- Transaction Delivered to Peers

→ Once the ordering Services receives the Endorsement blob and validates against its state, it initiates a deliver event for Peers which is defined as: deliver (seqno, prevhash, blob).

→ All the Peers in the network receives the deliver even and does the following.

- It checks that the blob, endorsement is valid according to the Policy of the chaincode.
- It also verifies that the dependencies (blob, endorsement, tx-sProposal, readset) have not been violated, meanwhile.

→ Peers validates the transactions and change the state if required / validated. Peer applies blob. endorsement. tx-sProposal. content to blockchain state. Invalid transactions do not change state but are maintained in ledger too. All the Peers will have the same state after the deliver event has been executed.

- **Endorsement Policy :-**

~~> Endorsement Policies are used to instruct a Peer on how to decide whether a transaction is properly endorsed. Endorsement Policies are the conditions which are to be met to endorse a transaction. Endorsement Policies are referred by deploy transactions which install specific chaincode over the Blockchain.

~~> endorsement Policies should not be large in numbers, instead it should be a set of Proven Policies that guarantees security and Performance.

- **Transaction Evaluation :-**

→ A transaction is declared valid only if it satisfied the endorsement Policies and only after that it could be committed over the ledger.

- **Endorsement Policy may refer to :-**

- keys or identities relating to the chaincode for example, a set of endorsers.

- Metadata of the Chaincode.
- Elements of the endorsement and endorsement transaction Proposal.
- These could be more data as per the business requirement.

- **Endorsement Policy Example :-**

— Chaincode can be used to specify the endorsers set: E = C Alice, Bob, Mary, Dave, Eve)

- Some Examples for Policies :-

- A valid Signature from on the same tran-Proposal from all member of Endorsers Set.
- A valid signature from any single member of Endorsers set.
- Valid Signatures on the same tran-Proposal from endorsing Peers according to the condition.
- Valid Signatures on the same tran-Proposal by any 3 out of the 5 endorsers.

- Policies could also be relate to stake weigh tags to each member.

Gossip Protocol :-

- What is Gossip Protocol ?

~~> A gossip Protocol is a Procedure or Process of computer Peer-to-Peer communication that is based on the way that epidemics spread. The concept of gossip communication can be illustrated by the analogy of office workers spreading rumors. There are two types of gossip Protocols.

- Data Dissemination :- These use gossip to spread information ; they basically work by flooding agents in the network.

- Data Aggregation :- These compute a network wide aggregate by sampling information at the nodes in the network and combining the values to arrive at a system-wide value.

Gossip Protocol with HyPerledger Fabric:-

→ HyPerledger Fabric implements a gossip data dissemination Protocol. The gossip-based data dissemination Protocol Performs three Primary function on a Fabric network.

- manages Peer discovery and channel member ship, by continually identifying available member Peers, and eventually detecting Peers that have gone offline.

- Disseminates ledger data across all Peers on a channel. Any Peer with data that is out of sync with the rest of the channel identifies the missing blocks and sync itself by coping the correct data.

- Bring newly connected Peers up to speed by allowing Peer-to-Peer State transfer update of ledger data.

→ For dissemination of new blocks, the leader Peer on the channel Pulls the data from the ordering service and initiates gossip dissemination to Peers in its own organization.

Gossip Protocol Leader Election :-

→ The leader election mechanism is used to elect one Peer per organization which will maintain connection with the ordering service and initiate distribution of newly received blocks across the peers of its own organization. There are two possible modes of operation for a leader election module.

- **Static** :- A system administrator manually configures a peer in an organization to be the leader.
- **Dynamic** :- Peers in the organization execute a leader election procedure to select one peer in an organization to become leader.

- **Anchor Peers** :-

→ Anchor peers are used by gossip to make sure peers in different organizations know about each other.

→ When a configuration blocks that contains an update to the anchor peers is committed, peers reach out to the anchor peers and learn from them about all of the peers known to the anchor peer(s). Once at least one peer from each organization has contacted an anchor peer, the anchor peer learns about every peer in the channel.

→ As communication across organizations depends on gossip in order to work, there must be at least one anchor peer defined in the channel configuration.

- Gossip Messaging :-

→ Online peers indicate their availability to other by continually broadcasting 'alive' messages, each containing the public key infrastructure ID and the signature of the sender over that message. Peers maintain channel membership by collecting these alive messages.

→ If no peer receives an alive message from a specific peer, this "dead" peer is eventually purged from channel membership. Because "alive" messages are cryptographically signed, malicious peers can never

other Peers, as they lack the signing key authorized by Root certificates authority.

→ In addition to the automatic forwarding of received messages, a State Reconciliation Process synchronizes world state across Peers on each channel. Each Peer continually pulls blocks from other Peers in the channel, in order to repair its own state if discrepancies are identified.

Introduction to Hyperledger

Composer

- Hyperledger Composer is an application development framework which simplifies and expedites the creation of Hyperledger fabric blockchain applications.
- Composer allows you to model your business network and integrate existing systems and data with your blockchain applications.

- Composer supports existing Hyperledger Fabric infrastructure and runtime like Pluggable Blockchain consensus Protocols to ensure that transactions are validated according to network Policy.

- ## Key Concepts of Hyperledger Composer :-

→ Hyperledger offers two types of storage locations.

- the ledger.
- the state database.

→ The ledger is the actual "Blockchain". It is a file-based ledger which stores serialized blocks. Each block has one or more transactions. Each transaction contains a read-set which modifies one or more key/value pairs. The ledger is the definitive source of data and is immutable.

→ The state database holds the last known committed value for any given key. It's populated when each Peer validates and commits a transaction. The state database can always be rebuilt from re-Processing the ledger. There are currently two options for the state database: an embedded

LevelDB with Hyperledger Fabric or an external couch DB.

- **Connection Profiles :-**

→ A connection Profile is a JSON document which is a part of a business network card. These Profiles are usually provided by the creator of the system they refer to and should be used to create business network cards in order to be able to connect to that system.

→ A simple analogy for connection Profile and business network cards could be.

- A business network card is like your id card for the office.
- A connection Profile is like the permissions the id card hold inside the office.

- **Assets :-**

→ Assets could be tangible or intangible goods, services or property. Assets are stored under registries with Blockchain State Storage. Example

for an asset could be: a Property for sale, a food item listed, certificates, insurance terms, Patient data etc.

→ Assets must be have a unique identifier under Hyperledger Composer. Apart from that assets may be related to other assets or Participants. For example :- a land certificate could be related to a Property for Sale.

→ Assets can be created on Hyperledger Blockchain using chaincode and Hyperledger Composer. Native currency is not supported on Hyperledger Fabric Blockchain.

- Participants :-

→ Participants are member of a business network. A Participant is like an actor in a business network. A Participant can create assets and also exchange assets with other Participants. Participants are the actors who submit transactions over the Business network.

→ Participant types are modeled like assets, with identifier and other properties as required in order for a new participant to join a business network, a new instance of the participant must be created in the business network. Participants are also stored in registries.

- Identities :-

→ An identity is a digital certificate and private key. Identities are used to authorize transactions on a business network and must be mapped to a participant in the business network.

→ A single identity is stored in a business network card and if the identity has been mapped to participants, it allows the user of that business network card to perform transactions on a business network as that participant.

→ Identities are maintained as a set of mappings to participants in the Identity Registry.

→ When that participant uses their identity to submit transactions to the deployed business network, the composer runtime looks for a valid mapping for that identity in the identity registry.

Business Network Cards :-

~~> A Business Network card Provides all of the information needed to connect to a blockchain business network. A Participant can only access a Blockchain Business Network through a valid Business Network card. It is similar to the Identity cards in corporated offices without which a Person is not allowed entry into the office Premises.

~~> Business network cards are a combination of an identity, a connection Profile, and metadata. Business network cards simplify the Process of connecting to a business network. A Business Network card can be exported and shared with others, allowing them to connects to the business network.

~~> Contains the identity, certificate and the connection Profile for a Participant.

- **Transaction :-**

~> Transactions are the mechanism by which Participants interact with assets. Some of the examples of a transaction could be.

- A Participant Placing a bid on an asset during an auction.
- An auctioneer marking an auction closed
- Automatic transfer of ownership for the asset to the highest bidder.

~> The base class of transaction include transaction id and timestap which are inherited by all the transactions.

- **Queries :-**

~> Queries are used in HyperLedger Composer to return data about the blockchain world-state.

~> Queries are defined within a business network and can include variable Parameters like "WHERE, LIKE" etc. for simple customization.

~> Queries are sent by using the Hyperledger composer API.

~> Queries in Hyperledger composer are written in a bespoke query language which offers rich query format.

* Event :-

~> Events are defined in the business network defination in the same way as assets or participants.

~> Once events are defined, they can be emitted by transaction processor functions to indicate that some important update has taken place over the ledger.

~> Applications can subscribe to emitted events through the composer-client API.

~> Events are defined under model file and emitted under transaction processor file.

* Access control :-

→ Business networks may also contain a set of rules to define access to data for participants.

→ Access control rules allow control over what participants can access, transaction and under what conditions.

→ The access control language allows conditions through which we can map the ownership of assets and define proper rules.

→ Externalizing access control from transaction processor function logic makes it easier to inspect, debug, develop and maintain.

→ Hyperledger composer also offers access control for network administrators to access certain network level operations.

• Historian Registries :-

→ The historian is a specialised registry which records successful transactions, including the participants and identities that submitting them.

—> The historian stores transactions as Historian Record assets, which are defined in the Hyperledger composer system namespace.

—> When a transaction is submitted, the Historian Record is updated and, maintains a history of transactions within a business network.

—> Historian Record assets can be queried using composer queries to extract specific records or data.

• How does Hyperledger works ?

—> Components of composer :-

• Execution Runtimes :-

—> Hyperledger composer has been designed to support different pluggable runtimes, and currently offers 3 runtime environments.

- Hyperledger Fabric V1.1
- Web based runtime environment which is used by Playground.

- Embedded, which executes within a Node.js process. This is primarily for unit testing of business logic.

- Connection Profiles:- These are used to specify how to connect to an execution runtime. They are part of Business Network cards. There are different configuration options for each type of execution runtime.

- For example, the connection profile for a Hyperledger Fabric v1.1 runtime will contain the TCP/IP addresses and ports for the Fabric peers as well as cryptographic certificates etc.

- IDE Extensions (VS code and Atom Editor):-

→ Hyperledger Composer has editor extensions for VS code and Atom.

- The VScode extension validates Composer model and Acl files, providing syntax highlighting, error detection and snippets support.

- The Atom Plugin is much more simple and only has basic syntax highting.

- Javascript SDK :- The hyperledger composer Javascript SDK consists of node.js APIs that enables developers to create, manage and interact with deployed business networks. There are two types of APIs available

- composer-client :- This is used to perform create, Read, Update, Delete operations on assets and participants.

- composer-admin :- This is used to manage business networks (install, start, upgrads).

- REST Server :- composer's REST Server automatically generates an Open API REST API for a business network. The REST server is based on LoopBack technology and is used to convert the composer model into an Open API definition. it implements Create, Read, Update and Delete API support for assets and participants and also allows transactions to be submitted for processing or retrieved.

- LoopBack connector :- It is used by the composer REST server. It can also be used standalone by integration tools that support LoopBack natively. it may be used with the LoopBack tools to create more sophisticated customizations of the REST APIs.

- Command Line interface :- The CLI tools enables developers and administrator to deploy and manage business network definitions.

- Playground Web user interface :- Playground is a web UI is used to define and test business networks. it allows quick important of samples and prototyping of business logic that executes on the web or Hyperledger Fabric runtime.

- Yeoman Code Generators :- Hyperledger composer uses the open source Yeoman code generator framework to create skeleton Projects.
  - Angular Web Application
  - Node.js application

Oskeleton business network

* Architecture of Hyperledger Composer

→ Hyperledger composer is a Programming model containing a modeling language, and a set of APIs to quickly define and deploy business networks and applications that allow participants to send transactions that exchange assets.

- Modeling language called CTO.
- UI called Hyperledger composer playground for rapid configuration, deployment and testing
- command-line interface (CLI) tools for integrating business networks modeled using Hyperledger composer.
- Different environments to create Blockchain Applications &-

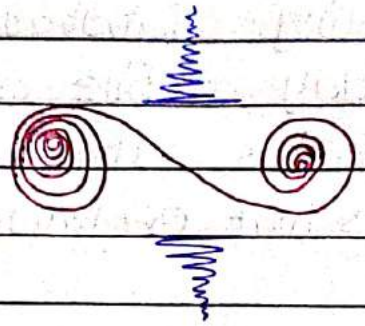
→ Windows 10 Pro - Linux Subsystem for Windows.

→ Windows 10 Home - Dual Boot with Windows.

→ Ubuntu - Stand alone

→ Ubuntu - compute machine with cloud

→ Mac - Stand alone



250