Blockchain Technology

U-I Mathematical Foundation For BCT.

→ Symmetric & Assymetric key Cryptography
→ Elective Curve Cryptography ECC
→ SHA256, Digital Signature, Merkel Tree.
→ Header of Block Size of Header Block, Actors of BCT.

→ Cryptography ⇒ Technique of Securing information and communication through use of codes, This is used to protect Information. It encodes the message using Algorithms which is hard to decode and only one person is intended to decode the message known as receiver.

→ Features —
- Confedentiality – Msg can only be accessed by person for whom it is intended
- Integrity – Info can't be modified in storage or during transition
- Non-repudiation – Creator/Sender can't deny his intention to send msg at later stage.
- Authentication – Identifies Sender and receiver

→ Types of Cryptography

Symmetric key – It's an encryption ~~technique~~ System where Sender & receiver of msg use single common key to encrypt and decrypt msg. This are faster & Simpler but Sometimes Sender & receiver has to exchange key Securely
ex – Data Encryption System & Advanced Encryption Sys.

Hash Functions – A hash value with Fixed length is calculated as per the plain text which makes it impossible For contents in plain text to recovered.

Asymmetric key – A pair of keys are used to encrypt & decrypt messages. Receiver's public key is used For encryption and receiver's Private key used For decryption. ex – RSA algorithm.

→ Steps & working of Asymmetric key –
1. Sender encrypts message using the receiver's public key
2. Encryption Converts plain text into Cipher text
3. The Cipher text is sent to receiver over the

~~Realtime examples & Case studies~~.
~~Why blockchain is important ?~~

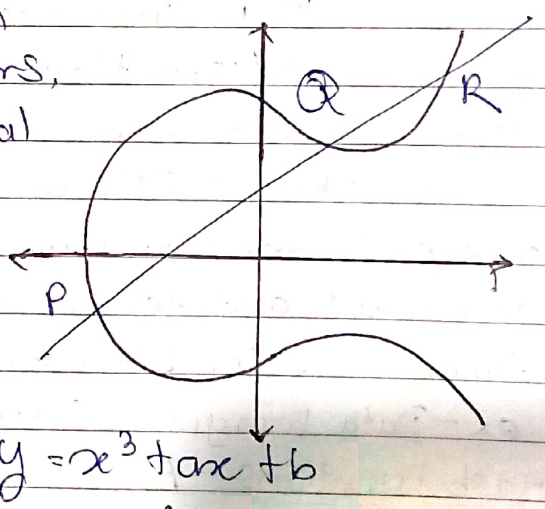
4. Receiver decrypts cipher text using his private key.
5. Private key is only known to Receiver.
6. After decryption, cipher text converts back into a readable plain text Format.

✗ Eliptic Curve Cryptography —

ECC is a key pair based technique for encryption data. ECC focuses on pairs of public and private keys for decryption & encryption of web traffic

ECC is an alternate technique to RSA, It generates security between key pairs of public key encryption by using the mathematics of eliptic curve

→ RSA's Security dependent on huge amount of prime numbers, ECC leverages the mathematical theory of eliptic curves to acheive same level of security



→ Components →
1) Keys → Public & Private.
2) Generator Point (GP).

→ Algorithms - Digital Signature Algos
→ Elliptic Curve Digital Signature Algo (ECDSA) - A highly complicated public key Cryptography encryption algorithm. ECC is a type of public key Cryptography uses the algaebric Structure of elliptic curves.
→ Edwards-Curve DSA
→ key Agreement Algorithms -
→ Elliptic-curve Diffie-Hellman (ECDH) - It's a key agreement protocol that enables two parties to estabhish a Shared Secret over an insecure channel.

→ Application of Eliptic c c —

→ Diffie Hellman – Diffie Hellman protocal ~~for~~ – Public key CryptoSystem Suggested for Secret key Sharing.

→ ECDSA – ECC is one of the most widely used DSA implementation approach in Cryptocurrencies. In order to Sign agreement.

→ Online Application – ECC is as encryption Standard that will utilized by most online apps in future due to its reduced key size & efficiency.

→ Blockchain Applica^{n} – Bitcoin employs ECC. Ethereum 2.0 makes heavy use of elliptic curve pairs with BLS Signatures.

→ ECC vs RSA

1) Works just on mathematical model of elliptic curve	Primarily based on the prime Factorization approach
2) Gives significant bandwidth savings over RSA	Provides much lesser bandwidth ~~Sharing~~ Saving than ECC
3) Encryption process takes less time	Takes more time.
4) Decryption takes more time	Decryption is Faster
5) much safer than RSA and is currently in process of adapting	heading towards end of its tenure.

Centralized vs Decentralized System + limitations
Digital Signature Algorithm
Lim.

SHA-256 -

SHA 256 is a part of SHA 2 family of algorithms Stands For Secure hash ~~Function~~ Algorithm. The Significance of 256 in the name stands for the Final digest value, i.e. irrespective of the size of plaintext the hash value will always be 256 bits.

> Features →

→ msg length - length of clear text should be less than 264 bits. The size needs to be in the comparison area to keep the digest as random as possible.

→ Digest length - Length of the hash digest should be 256 bits in SHA 256 algo. 512 bits in SHA 512

→ Irreversible - By design, all hash Functions such as SHA 256 are irreversible.

> Steps →

→ Padding bits - Original msg + Padding Bits. It adds extra bits to the message, such that the length is exactly 64 bits short of a multiple of 512. Total length to be 64 bits less than multiple of 512.

→ Padding length - add 64 bits of data to make the final plaintext a multiple of 512.

→ Compression Function.

→ output - The cycle keeps repeating until we reach last 512 bit block and you consider its output the

> Application → Final digest of length 256 bits.

1) DSA 2) Password Hashing 3) SSL Handshake 4) Integrity Checks.

In Compression Func^n entire msg broken down into multiple blocks of 512 bits. It puts each block through 64 rounds of operation, with the output of each block serving as input for following block.

Centralized	Decentralized
1) Single Firm manages and owns a centralized program cyber-attacks Raible, which Runs on a Single Server or cluster of Serves.	On a Blockchain network a decentralized application dApp runs.
2) User Interacts with traditional program	User Interacts with a Smart Contract-based blockchain.
3) User gets the app from app store and utilizes it by Sending request to Centralized Servers.	Users pay to the developer via CryptoCurrency to use these apps. User has facility to download the application's Source code via "Smart Contract
4) Backend code operates on centralized Server	Backend Code operates on a peer to peer network
5) Requires lower Computing power	High Computing Power
6) Less Secure	Highly Secure
7) Not trustworthy lack of transparency	Trustworthy highly transparent
8) If any Server goes down System collapse.	If any node goes down system will run normally.
9) Easy to use	diffical to use for end user.
10) ex- Google, Apple, Facebook	ex - UniSwap, Cryptokitties, Raribie, IDEX, MetaMask.

BCT U-II

Feature Engineering

What is Blockchain?

Blockchain is defined as a ledger of decentralized data that is securely shared. With blockchain cloud services transactional data from multiple sources can be easily collected, integrated & shared. Data is broken up into shared blocks that are ~~changed~~ chained together with unique identifiers in the form of cryptographic hashes.

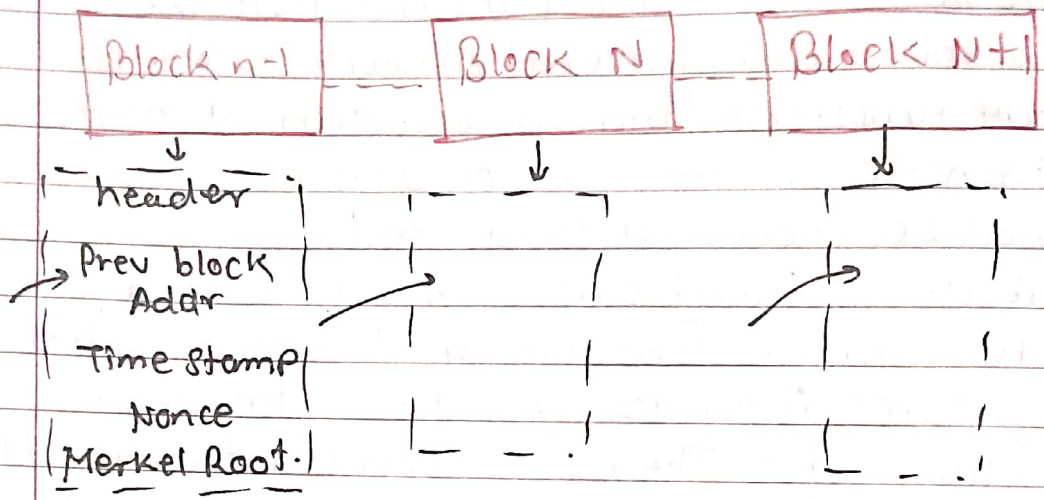
How does it works?

1) Transacⁿ - Represents different types of data such as financial transactions or digital assets. Each Transacⁿ is initiated by a participant in blockchain network.
2) Verificaⁿ & Consensus - Initiated Transacⁿ broadcasted into the network. Nodes in network verify the transaction's validity based on predefined rules and consensus mechanism.
3) Creaⁿ of Block - Valid transactions are grouped together into a block. Each block typically contains a fixed no. of dat transacⁿ.
4) Linking Block - Each block contains a reference (cryptographic hash) to the previous block in the chain. This linking blocks forms a chain of blocks.
5) Be Decentralized - Blockchain operates on a network of decentralized nodes. These nodes maintains copies of ledger, ensuring redundancy and fault tolerance.
6) Immutability - Once block is added to blockchain it becomes extremely difficult to alter or delete any transacⁿ within it.
7) Cryptography - Used to secure transacⁿ and blocks. Each ~~block~~ transacⁿ is cryptographically signed by the sender.

Features of Blockchain -

1) Immutable - Immutability means that the blockchain is a permanent and unaltered network. Blockchain technology functions through collection of nodes. Once transaction is recorded on the blockchain, it cannot be modified or deleted.
2) Distributed - Every participant have a copy of the ledger for complete transperency. This distributed ledger ensures redundancy and fault tolerance.
3) Decentralized - There's no central authority controlling the network. Instead the network is made up of large number of nodes that work together to very & validate transaction
4) Secure - All records in blockchain are individually encrypted. Using encryption adds another layer of security to entire process on blockchain network. All the blocks contain unique hash of their own and the hash of previous block. Blocks are cryptographically linked.
5) Consensus - Every Blockchain has Consensus to help the network to make quick & unbiased decisions. Consensus is decision making algorithm for the groups on network to reach on agreement quickly & faster and smoother functioning of system.
6) Smart Contracts - Blockchain platforms like Ethereum support Smart Contracts, which are self-executing contracts with predefined rules.
7) Timestamping -
8) Peer to Peer network -

Blockchain Architecture -



> Header - Used to identify the particular block in entire blockchain. It handles all blocks in blockchain. Block header contains essential info about the block and it is typically the part of block that miners work on when trying to solve Cryptographic puzzle.

> Prev Block Hash - This field in block header contains the Cryptographic hash of the previous block in blockchain. It links the current block to previous one.

> Timestamp - Timestamp in block header is a record when the block was created or added to blockchain. Verifies order of transaction and maintaining chronology.

> Nonce - These are randomly generated numbers that miners adjust while trying to solve Proof of work puzzle. Miners repeatedly change the nonce in an attempt to find valid hash value.

> Merkel Root - Merkel root is derived from data structure called merkel tree. It's a Cryptographic hash that represents all the transactions within a block. Transaction are organised into a binary tree structure. Merkle root is calculated based on hash value of transaction.

Layers of Blockchain – Blockchain consists of several layers. These layers work together to create a secure & decentralized system.

> Network Layer/propogan layer –

1) The peer to peer comminican that enables nodes in a network to find one another and synchronise with another node are handled by propagan layer.
2) Every node in network receives a broadcast when a ~~block~~ transacn is completed. Additionaly, when a node proposes a block, it is immediately broadcast throughout the whole network so that other nodes can use it.
3) This layer defines how a block or transaction distributes throughout the network and maintains the overall ~~Stability of~~ Stability of system.

> Applican Layer –

1) Multiple Applications can be built on a blockchain technology. Applican layer contains the applications that are used by end users to interact with blockchain network.
2) The applican layer includes user Interface such as wallets and blockchain explorers. These interfaces allows users to interact with the blockchain.
3) DApps are software applications built on top of blockchain tech. They often interacts with smart contracts and the blockchain through APIs.

> Execan Layer –

1) All instruccn performed at applican layer are handled by this layer for all nodes connected to blockchain network.
2) This layer has the actual code and rules that are executed. Execan layer consists of underlying rules, Smart contracts & chain code.

3) Execution layer also validates transactions to ensure that they comply with the rules and conditions set by Smart Contracts.
4) After execn This layer records results of Smart Contract execn including any change to blockchain state.

> Semantic layer -
1) This layer is also known as the logical layer in the Blockchain layer. This layer is concerned with validating both the blocks & transaction in a network
2) When transacn comes from a node, the set of instructions are executed on execn layer and are validated on the Semantic layer.
3) This layer defines a logical data model that includes entities, attributes, relationships. This layer can restrict access to sensetive data and apply role based access controls.
4) Semantic layer can encapsulate business ~~roteraly~~ calculations and th logic.

> Consensus layer -
1) This layer determines how nodes agree on validity of transacn and the order of transactions in blockchain Various consensus mechanism such as Proof of work and others, can be employd depending on blockchain design.
2) Layer also deals with the Security and Safety of blockchain.
3) There are variety of consensus algo that may be used to create cryptocurrencies like Bitcoin & Ethereum These algo employs POW mechanism to choose random node from network's nodes

4) Once new block is created, the block is propagated to all the other nodes to check if new block is valid or not with the transaction and based on the consensus from all other nodes the new block gets added on to the blockchain.

Limitations of Centralized System.

In Centralized Systems where controls and decision making authority are concentrated in a single or a few points of authority.

1) Single point failure - Centralized systems typically have a single point of failure, such as central server or authority. If this point fails then entire system will be vulnerable to attacks.

2) Scalability challenges - Scaling centralized sys. to handle growing number of users or transaction can be challenging.

3) ~~Tra~~ Data Privacy - This system often stores user data in a centralized database or server. This can be vulnerables to attack if ~~data~~ Server gets hacked.

4) Lack of Transperency - This sys. may lack transperency, as users often have limited visibility into the inner working of the system.

5) Bottlenecks can appear when traffic spikes - as the server can only have a finite number of open ports to which can listen to connection from client nodes. which reduces efficiency of server.

6) High costs - operating & maintainance of centralized sys., including hardware, software upgrade can be costly.

Why Blockchain is important -

Blockchain technology provides one of most secure and safe online transactions. So the field of Blockchain in IT sector is growing faster.

1) Decentralisaⁿ -
2) Immutability
3) Cybersecurity - Due to powerful encryptions and intermediate recording, the probability of attacks performed by malicious intruders falls to its lowest.
4) Cost reducⁿ - Blockchain removes the need for Intermediary in transacⁿ. Smart contracts are used which reduces the need of manual paperwork.
5) Tracebility - Ability to track and verify the origin journey, and history of a product asset, or data through a transparent and immutable ledger.
6) Transparency
7) Smart Contracts.

Limitations

1) Scalability Issues - As No. of transacⁿ increases it is difficult validate transacⁿ quickly. This can result in Slow process.
2) Transacⁿ Costs - Transacⁿ fees can be high on some networks. This can limit affordability of using BCT.
3) Privacy & Security challenges -
4) Irreversible Transacⁿ
5) Long confirmaⁿ time
6) Loss of private keys
7) Complexity - Developing & deploying blockchain Solⁿ can be complex.

UIII BT

Platforms & consensus in BCT

Types of Blockchain -

1) Public blockchain -> It is a permissionless distributed ledger on which anybody can b join and conduct transaction.
2) It's non-restrictive ~~from~~ Form of the ledger in which each peer has a copy. This also means that anyone with internet can access public blockchain.
3) This user has access to historical & contemporary records and the ability to perform mining operan.
4) These complex computan must be performed to verify transaction and add them to ledger.

On blockchain network, no valid record or transacn may be altered. Because source code is open, anybody can check the transacn, uncover problems, & suggest fixes.

> Advantages.

1) Trustable - Proof of work procedure.
2) Secure -
3) Open & Transparent.

> Disadvantage -

1) Lower transacn per second in public blockchain is extremely low.
2) Scalability issues -
3) High Energy Consumpn - PoW is expensive.

2) Private Blockchain -

1) A blockchain network operates in private context, such as a restricted network, or is controlled by a single ~~identity~~ entity.

2) It operates like a public blockchain network in the seer sense that it uses peer to peer connections and decentralizan. this blockchain are smaller in size.

3) Private blockchains typically are operated on a small network inside a company or organizan. They're known as permissioned blockchains.

> Advantages - 1) Speed.
2) Scalable.

> disadvantage -> lower security
2) Trust building 3) Centralization.

3) Hybrid Blockchain -

1) Organizan who expect ~~both~~ best of the both worlds use hybrid blockchain, which combines both private & public blockchain.

2) It enables enterprises to construct a private ordering side a public blockchain system, allowing them to choose who has access to certain Blockchain data & what data is made public

3) In hybrid bCT, transcan and records are typically not made public, but they can be validated if necessary by granting access via a smart contract.

> Adv - 1) Secure 2) cost-effective

> Disadv - 1) Lack of Transperancy

2) Less incentive - Upgrading can be difficult users ~~to~~ have no incentive to participate.

3) Consortium Blockchain - Similar to hybrid blockchain, ~~is similar~~ in that it has private & public blockchain features. ~~But it's different in that multiple organizati~~

> Instead of being under control of a singular central authority, the member organiza^n. manage the nodes that verify transac^n.

> In sector where multiple organiza^n must work on a single platform while keeping control over their data & transactions. This blockchain is used.

> In general, consortium blockchains provide a balance betn decentraliza^n & control, making them appropriate for use cases where no. of well known & trustworthy parties must collaborate on a common ~~platfo~~ platform

Advantages -

1) Greater efficiency.
2) Enhanced security
3) Better Data privacy
4) Scalability

Disadv -

1) Limited Decentraliza^n
2) Limited Transperancy
3) Risk of network Fragmentation.

Bitcoin –

1) Bitcoin was introduced in a 2008 it is a Peer to peer electronic Cash System by unknown person 'Satoshi Nakamoto"

2) Bitcoin operates on decentralized peer to peer network & utilizes blockchain technology. Transac^ are recorded on a public ledger which is maintained by network of nodes.

3) Blocks of transac^ are added to blockchain through process known as mining. Bitcoin mining involves Solving Cryptographic puzzles to validate transac^. This process is based on proof-of-works mechanism.

4) Bitcoin's price has been characterized by high volatality, with significant price Fluctua^ over Short period.

5) Features.
1) Distributed
2) Decentralized.
3) Transparent.
4) Peer to peer
5) Public
6) Permissionless.

6) Bitcoin can be created using bitcoin Crypto wallet Each be bitcoin has. 2 things.
Public key, Private key

Ethereum – It's a decentralized, open-source blockchain platform that enables the creation & execu^ of Smart Contracts & decentralized applica^ (DApps)

1) Ethereum introduced the concept of Smart contracts, Self executing Contracts with the terms of agreement directly written into code. Ethereum's Scripting language, Solidity its a turing complete allowing for the crea^ of complex & programmable contracts.

> Ethereum enables development of decentralized Apps that run on blockchain.
> Ether is the native cryptocurrency of the ethereum & is used to compensate miners for securing the network & execute smart contracts.
> Ethereum has proof of stake mechanism, & known as Ethereum 2.0. It aims to improve scalability, energy efficiency & security.

Hyperledger – Hyperledger is an open source collaberative project hosted by linux founda" Hyperledger provides the platform for developing blockchain based software. Hyperledger has the advantage of creating a secured & personalized blockchain network
> Hyperledger was set up with the aim of accelerating industry wide collaboration for developing high performance & reliable blockchain & distributed ledger based technology framework.
> Projects from hyperledger include a range of permissioned blockchain system that are enterprice, where network users are familiar with one another and have inherent incentive in taking part in consensus making
> Hyperledger layers.
- Consensus layer
- Smart contract layer
- Communication Layer
- Identity management Layer
- API Layer.

Page No.
Date

IOTA – It's a decentralized and open-source distributed ledger tech designed to ~~enabd~~ enable secure & feeless transfac^n between devices in IoT ecosystem.

> IOTA's underlying data struct is Tangle. a directed acyclic Graph. In Tangle each transac^n confirms two previous transac^n

> IOTA is known for its feeless transac^n, Participants in the network contribute to the validation process by confirming other transac^n

> The Tangle's structure allocos for parallel processing of transac^n potentially improving scalability

-> The Tangle's DAG structure eliminats need of traditional blocks & chains & participants can directly approve transac^n, leading to a more efficient & streamlined valida^n process

Corda – It's an open source blockchain platform designed for building DApps specifically for businesses. Developed by R3, a consortium of financial institutions. Corda aims to provide a secure and efficient platform for managing & recording financial agreements.

> Operates on permissioned network, where participants are known entities with identity and access controls.

> Corda supports development & execu^n of smart contracts, referred as "CorDApps".

> Corda focuses on privacy & confidentiality. It ensures that only parties involved in transac^n can have access to relevant data. It does not use global broadcasting of transac^n. Transac^n are only shared with the involved parties

> Corda is interoperable with other systems & supports uses of common programming lang such as Java, Kotlin.

* R3 - It is a financial tech company that focuses on developing distributed ledger Tech soln for businesses and financial institutes
> It's initial goal was to explore and develop blockchain soln for financial services.
> R3 developed corda, corda is known for its focus on privacy, security & ability to handle complex financial agreements
(Further write about corda)
> Corda employs UTXO Similar to Bitcoin (Unspent Transacn output) to manage and track ownership of assets.

* Consensus Algorithm -
> Consensus Algo are methods for collective decision-making in which members of group create & support decision that will benefit group as whole
> A consensus Algo is a proceduore through which all the peers of blockch. network reach a common agreement about present state of distributed ledger.
> In this way, Consensus algo acheive reliability in blockchain network & establish trust betn peers.
> Consensus make sure that every new block that is added to the block chain is one & only one version of the truth that is agreed upon by all the nodes.
> consensus protocol consist of objectives such as coming to an agreement, collaboran, co-operan equal rights to each node.

> Proof of Work -

> This consensus algo is used to select miner for the next block generation. Central idea is to solve complex math puzzle & easily give out soln

> Purpose is to bring all the nodes in agreement, that is, trust one another.

- All transactions in the new block are then validated and the new block is then added to blockchain
- Block will get added to the chain which has longest block height.
- Miners perform computational work in solving complex math problem to add block to the network

> Proof of Stake - This is most common alternative to PoW In this ~~type~~ type of consensus algo, instead of investing ~~on~~ expensive hardware to solve a complex puzzle. Validators invest in the coins of the system by locking up some of their coins as stakes.

> After that, all the validators will start validating block Validators will validate block through a ~~de~~deterministic process that often considers factors like amount of cryptocurrency staked.

> PoS is more efficient than PoW since it doesn't require the massive computation power used to solve puzzles.

> PoS is secure as it would be economically irrational for validators to act maliciously & risk staked assets.

> Variats.

Delegated PoS

Liquid PoS

> Proof of Burn - With PoB instead of investing in expensive hardware equipments, validators burn coins by sending them to an address from where they are irretrievable.
> Participants who have burned cryptcurrency gain the right to validate transac^n and create new blocks
> Primary goal is of burn is to reduce the available supply of a cryptocurrency. By reducing supply the value of remaining coins may increase.
> PoB aims to maintain network security & decentraliza^n. Participants are motivated to act honestly to preserve value.

> Proof of Elapsed Time - It's one of the fairest Consensus algo which chooses the ~~network~~ next block using fair means.
> widely used in permissioned Blockchain network. In this algo every validator gets fair chance to create their own block.
> Nodes in POET are required to wait for randomly assigned time before attempting to create new block. wait time is determined by secure enclave. It ensures wait time is truly random
> The created blocks are broadcasted to network ~~The created blocks are bro~~. The winner is the validator which has the least timer value in proof. block from winning validator node gets appended to the Blockchain.

Page No.
Date

* Byzantine General Problem - In the byzantine general problem is a classical problem where a group of generals, each commanding a portion of byzantine army maind city. The generals need to agree on a common plan of action - either attack or retreat
However critical challenge is some of generals may be traitors who will deliberately send contradictory msg.
> Objective is to acheive consensus among loyal generals. General need to determine strategy to ensure that they can reach a consensus
> Solution - Various algo have been proposed to solve the byzantine general's problem such as the practical Byzantine Tolerance (PBFT) algo and HoneyBadgeBFT protocol. These Sol^n involve cryptographic tech, redundancy & voting mechanism to ensure loyal generals.

UNIT Bitcoin & Token

Page No.
Date

Types of Cryptocurrency

→ Bitcoin

→ Altcoin - Alternatives to Bitcoin

- → Ethereum
- → Litecoin - based on Bitcoin technology, but It uses different hash Func^n It's open source peer to peer cryptocurrency. Litecoin aims to provide faster transac^n confirma^n time than bitcoin
- → Ripple - It operates on unique consensus algo & doesn't really rely on traditional PoW or PoS mechanism. designed to enable cost effective Cross border payments. Primary goal is to facilitate efficient low cost international money transfer.

→ Tokens - Digital assets created on blockchain, a token ~~refers to~~ represents various assets or rights and are often used within decentralized applica^n.

2 types -

1) Utility Token - Designed to provide access to a specific func^n or service within DApp

2) Security Token - Represents ownership of an underlying asset, and they are subject to Securities. This asset includ traditional Financial instrument like Stocks or bonds.

Page No.
Date

* Cryptowallets - Thes are Software applicat on computer or mobile devices. They use an internet connection to access the blockchain network.
> Cryptocurrencies are not stored anywhere - they are bits of data stored in database. Sending & receiving cryptocurrency is very easy using these applicat.
> Typically Sender enters recipient's wallet address and then enter amount to send cryptos from their wallet.
> There are two sub categories hot & cold, hot has internet connect & cold doesn't have any connect.

> Metamask - It's a famous Cryptowallet and browser extension that allows user to interact with Dapps.
> Metamask serves as a secure digital wallet where user can store & manage their Ethereum-based cryptocurrency
> Metamask provides user with a 12 word seed phrase for backup and recovery purpose.
> Metamask is available as a browser extension. It integrates seamlessly with browser, making it easy for user to interact with DApps. It supports Web3 Javascript API.
> Metamask Support diff. Ethereum networks Such as mainnet, testnets

> Coinbase - Popular Cryptocurrency exchange platform that provides various services related to buying, selling & managing digital currency.
> Coinbase operates as a cryptocurrency exchange, allowing user to sell & trade a variety of cryptocurrencies.
> It has user-friendly interface It provides users with an online wallet to store their digital assets securely

> Coinbase has mobile app, allowing users to manage their Cryptocurrency portfolios.
> Users can fund their Coinbase account using various payment methods including bank transfer.
> Coinbase implements 2 Factor authentication to enhance protection. Majority of user funds are stored in cold storage, which is not connected to internet.

> Binance -
> Binance offers wide range of trading pairs, allowing users to exchange various cryptocurrencies against each other
> Binance has it's native cryptocurrency called Binance Coin (BNB), can be used to pay trading fees.
> Binance Smart chain is a blockchain developed by Binance. it operates parallel with Binance chain and support Smart contracts. It also is compatible with Etherium virtual Machine.
> Binance supports two Factor authentication for Security and cold wallet Storage

MetaMask	Coinbase	Binance.
It's a wallet & Browser extension	Cryptocurrency exchange & wallet	Cryptocurrency exchange.
Browser extension	NO	NO
Supports Ethereum & compatible Network	Multiple network.	Multiple network

MetaMask	Coinbase	Binance
Uses private keys stored locally.	2 Factor authentica° biometric	—/— API.
Protec° of seed phrase for backup	authentica° insurance Fund	key security cold wallet Storage
Support DApps	Limited DApps	—/—
No Native Crypto - currency	No	Yes BNB coin
Transac° fees for Ethereum transac°	varies (buy/sell, Fees)	varies —/—
No staking & staving	staking & earning interest on savr.	—/—

Unit V BT

BCT Ethereum platform using Solidity

Ethereum -

> Ethereum networks -

> Mainnet (main network) - Ethereum is the live and and produc^{n} ~~based~~ ready blockchain. It is where real transac^{n} takes place, and users can transfer Ether (ETH) & other tokens. Smart contracts deployed on mainnet are fully operational, and any changes are permanent.

> Testnets - It is specifically designed for testing and development purposes. They allow developers to experiment with Smart contracts and DApps without using real ether. The three main testnets -

1) Ropsten - A PoW closely mirrors Ethereum mainnet
2) Rinkeby - A PoA testnet with faster block times
3) Kovan - Another Proof of authority testnet with a unique consensus mechanism.

> Private or consortium networks -

Ethereum virtual Machine (EVM) -

> EVM is computa^{n} engine that manages the state of blockchain and enables Smart Contract Functionality. It provides a sandboxed environment where Smart contracts written in high level prog. language.

> Smart Contracts are written in high level lang but are compiled into bytecode which is machine readable EVM is responsible for executing this bytecode.

> EVM enables decentralized computation by ensuring that Smart contracts are executed uniformly and deterministically across all nodes

> The EVM operates Ethereum network, which uses a consensus mechanism called PoS as Ethereum 2.0 upgrade
> EVM uses concept called 'gas', Gas is a unit that measures the computation work required to execute operation in Smart contract.
> EVM designed to be platform independent allowing it to run on any device

* Intro to Smart Contract – Smart contract is a self executing contract with terms of the aggreement directly written into code. Smart contracts automatically enforce and execute the terms of contract when predefined conditions are met.
> Self-executing – Smart contracts are autonomous and self-executing. They run automatically when the speed specified conditions, encoded in the contract are met.
> Smart contracts operate on decentralized blockchain networks. They're distributed across multiple nodes, ensuring transperancy, security & immutability.
> Smart contracts operate of in trustless environment. meaning that participants don't need to trust each other
> Once deployed on blockchain the code & terms are immutable. They can't be altered or tampered
> Smart contracts use cryptographic techniques for security such as digital sign & hash func^n to ensure integrity of contract.

* Purpose –
> Smart contracts play central role in DeFi applic^n, providing decentralized & lending, borrowing, trading without need for traditional financial intermediaries.

> Smart contracts ~~play~~ used to automate and Streamline Supply chain processes. They can track and verify the authenticity of products, automate payments and trigger actions based on predefined conditions.

> Smart contracts can be employed for creating Secure & transparent voting system, reducing risk of fraud.

> Insurance policies & claims can be automated.

Types of Smart contracts –

1) Smart legal contract – Designed to encode and automate the terms and condition of a legal agreement. It combines traditional legal agreements with programmable & self-executing code or blockchain or distributed ledger

> It provides transperancy & immutability. (write about smart contract again).

2) Decentralized Autonomous organization –

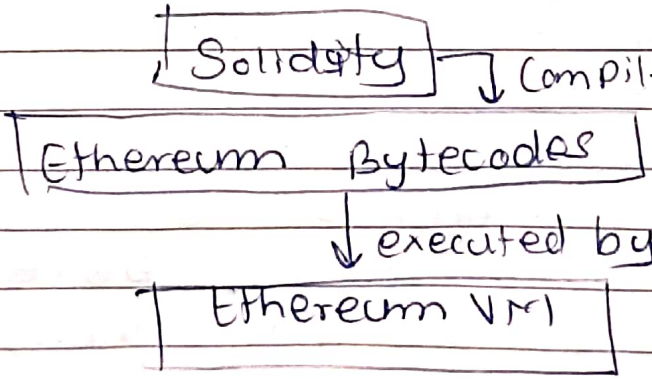
> A set of established guidelines that are defined using Smart Contract can serve to define these communities.

> Every person is bound by community's rules. DAOs are decentralized entities, meaning that control and decision-making authority are distributed among their members.

> DAO members have ability to vote on proposals & decision making. DAOs can manage funds & allocate resource based on predefined rules & member consensus.

3) Applicaⁿ logic contracts - It consist of applicaⁿ-based code that typically remains synced with various other blockchain contracts. It enables interactions betⁿ various devices, like the IOT or blockchain integⁿ These are not signed between humans or organizaⁿ but betⁿ machines & othe contracts.

Solidity Programming - Solidity is OOP language created specifically by Ethereum network team for constructing and designing smart contracts on blockchain.
> It's used to create smart contract that implement business logic and generate a chain of transacⁿ record in blockchain system.
> It acts as a tool creating machine level code & compiling it on EVM. Solidity has variables, functions classes, string manipulation.
> It supports common data types like Boolean, Int, String, Modifier, Array
> Pragmas are directive to compiler about how to handle code. Every line of Solidity source code should begin with Version Pragma.
> The Contract keyword declares a contract that encapsulates the code. different Functions can be executed on I executed on IDE like Remix
>



> Advantages -

1) Apart from fundamental data types, Solidity allows complex data types & member variable.
2) Solidity has comprehensive documentation and resources available making it easier for developers to learn & understand language
3) It supports OOP principles.
4) Solidity is statically typed, variables are declared at compile time.

* Swarm - Swarm is decentralized storage platform that operates on the ethereum network. Its primary goal is to create a decentralized and resilient storage infrastructure, providing users with a peer to peer network storing & retreiving files.

> Swarm' system built on following component

1) Chunks - Data stored on swarm is split up into smaller blocks called chuncks no bigger than 4KB.
2) Reference - A unique file identifier that facilitates the retreival of data stored in chuncks for clients.
3) Manifest - A data structure that allows for URL based content retreival.

> To enhance fault tolerance & ensure data availability swarm redundantly stores data across multiple nodes in the network.

> When client request content on swarm, the manifest uses the unique reference to identify the relevant data chuncks so that they can be retreived from the nodes that are hosting them.

Page No.
Date

> Swarm allows dapps developers to store and distribute data & content to blockchain users securely and efficiently.
> Swarm provide node to node messaging functionality & base layer in architecture designed to provide media streaming services.
> ex. - Ethersa, zetaseek, Scaleout.

Whisper - (decentralized Storage)

> Ethereum whisper is a messaging protocol that enables nodes on Ethereum network to send & receive messages. The messages can be used for a variety of purposes, such as peer to peer communicaⁿ.
> It uses decentralized architecture to provide secure & ~~provio~~ private se Communicaⁿ betⁿ nodes, Messages distributed across the network in peer to peer fashion.
> It uses distributed Hash Table to Store&distribute messages across Ethereum ~~AE~~ network. When a node wants to send a messge, it first encrypts the msg using recipient's public key. Encrypted msg then hashed and added to DHT.
> Whisper messages are routed through a series of randomly selected nodes before reaching final destinaⁿ even if attacker is able to intercept the msg they will not able to it determine identity of sender or receiver.
> Whisper can be used for developing decentralized chat applicaⁿ as it is secure & decentralized betⁿ nodes on the network.