U-3

Blockchain Platforms & Consensus in Blockchain:

	Public	Private	Hybrid	Consortium
	• Permissionless	• Permissioned	• Permissioned & Permionless.	• Permisoned.
	• No control by central authority	• control by a central authority	• Control by a central authority	• Control by multiple authorities.
Adv	• Independence	• Performance	• Performance	• Performance
Adv	• Transparency.	• Scalability	• Low Cost	• Security.
Disadv	• Performance	• Security	• Transparency	• Transpareg
Disadv	• Scalability issues	• Trust	• Upgrading	
example →	• Bitcoin Litecoin	• Hyperledger Fabric	• XRP token	• Corda Quorum.

☆ Hyperledger

- open source project to support development of blockchain based distributed ledgers.
- collaborative effort to create needed frameworks → standard tools & libraries to build blockchain & related application.
- hosts no. of enterprise grade blockchain software projects.

Central components → 1) distributed ledger for all data recorded about transaction
2) Multiple peers (or nodes)
3) smart contracts that maintain trans^n logic

- Many enterprises have embraced hyperledger tech^n to build blockchain sol^n.

☆ Hyperledger Fabric –

- foundation for building blockchain appl^n, product or solutions.
- Fabric is private & permissioned system.
- smart contact in fabric is known as chaincode.
- chaincode holds business logic.
- Features of Fabric platforms –
  1) Channels. 3) Data Encryption 5) File Encryption.
  2) Visibility 4) Trespassing Protection

POS (stake)

- Block creators → validators
- Participant must own coins & tokens to become validators
- energy efficient
- security → community control
- validators → trans^n fees → rewards.

POW (work)

- Block creators → miners.
- may buy equipment & energy to become miner.
- not energy efficient
- security → expensive upfront investment
- Miners → Block rewards.

* IOTA (Internet of things angles).

- opensource, decentralized, highly scalable Distributed Ledger Technology (DLT), designed to support data transfer across network.
- We build IOT soln using IOTA framework.
- Is a blockless blockchain that provides blockchain for IOT products.
- It connects devices using DAG.
- Features → • Scalable • Quantum • flexible,
  • Fee less • Proof Security • No miners.

Merits → • Free trans^n
- Unlimited scaling.
- can process any data.
- achieve instant trans^n
- ~~Keeps~~ No IOTA mining
- Quantum resistance.

Demerits → • No finished product yet
- Unclear when project will be ready
- currently needing to use a centralized coord
- Has experienced lot of technical flaws & bu
- Many (including MIT) think it has bad security.

Bitcoin

- first appn of BT & first cryptocurrency
- 2009 → Satoshi Nakamoto
- digital wallet
- key → public & private key for users.
- Buy from Bitcoin Exchange
- bitcoin exchange → wallet address
- Miners verify transn → add to blockchain ledger.
- Miners → find has value → first → awarded with bitcoins → block reward.
- Block data + nonce = Hash value.
- value of Bitcoin –

$$\frac{S}{D} = \frac{T}{P}$$

S = supply of bitcoin
D → Duration BTC needed by trans
T → Total bitcoin transn / second
P → Price of bitcoin.

Ethereum –

- Open source blockchain platform → develop & deploy btc based applns.
- protocol → inter network communication → www
- DApp → acc address → contract accns.
- Users → transn → with Externally owned accts (EOA) as well as contract accs.

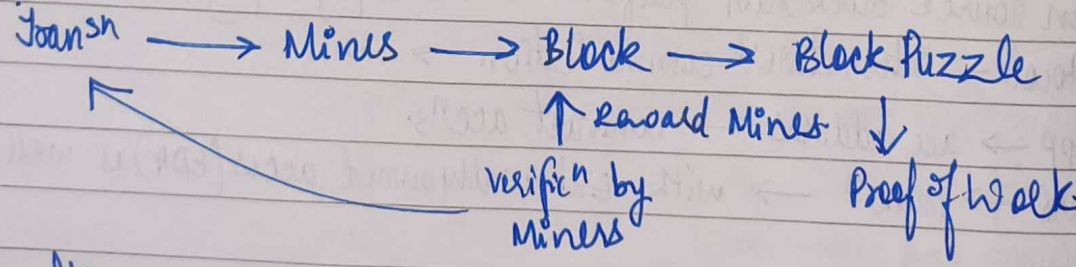
Consensus Algo -

- decision process for a group
- new block added → network → only version of truth.
- establish agreement on a single data → distributed process.
- ensures single, consistent & honest ledgers.
- work better in public while some is private.

Objectives →
- Fair & Equitable
- Avoid double spending
- unified agreement
- Fault tolerance
- economic incentive.

Proof of Work -

- First Conselnsus Algo → confirm trans^n & add new block to chain
- Uses SHA - 256 Algo.
- Protocol uses Merkel tree & P2P network.



- Its a power consuming protocol.
- Also has negative impact on environment..

Proof of Stake (POS) -

- Rather than Miners → there are validators / forgers.
- Miner choose → money to be transacted → network called stake
- Miner validate transaction.
- amt. of stake to be deposited > amt. of reward received after valid^{n}.
- eco friendly → no special hardware requirement.
-

Proof of Elapsed Time (POET) -

- lottery system followed for choosing miners
- used in permissioned blockchain
- certain random witing time → miner can start mining again.
- Blocks → validated → completed waiting time.
- protocol → FCFS & Intel based hardware
- sleep state → each node → awaits further instructi's

Proof of Activity (POA) -

- combo of POW & POS.
- For mining POA uses POW & to validate it uses POS.

Proof of Burns (POB) -

- used to avoid double spending attacks
- like POW without waste of energy.
- Miners get chace of mining by burning coins -
- Burned coins → can't be reclaimed.

U-4
Cryptocurrency
Bitcoin & Token.

* Bitcoin -

- peer to peer network
- can be purshased on several exchanges
- used as reward → miners in bitcoin mining.

* Features - • Distributed • Decentralized • Trasparent
  • peer to peer • public • permisionless.

* working - • user → bitcoin → bitcoin wallet
  • private & public key → create account.

* Buy bitcoin - • online exchange → exchange bit for normal currency

* Transactions - • Done using wallet
  • valid" → 10 mins.
  small trans" fee → speed up process.

* Mining → • Trans" → verified
  • requires → dedicated mining hardware.

* Cryptocurrency -

- digit assest → circulated without govt body & banks.
- virtual currency → cryptographic principles.

adv →
- network operates on a user to user basis
- quick & straightforward process.
- cryptocurrencies → transn → record → public list → blockchain
- cut out intermediatries → bank & online marketplaces
- widely used → large organization

disadv →
- lack of regularization
- fear about hacking & scams due to digitalization
- vulnerable for scams.
- security issues
- lot of ppl → less knowledge → huge loss
- fully digitalized → technically difficulty.

Types →
- Bitcoin (BTC)
- Ethereum (ETH)
- Zcash (ZEC)
- Ethereum classic (ETC)
- Bitcoin Cash (BCH)
- Ripple.

Type of Wallet →
- software wallet
  - ↳ Desktop wallet
  - ↳ Mobile wallet
  - ↳ Online wallet.
- Paper wallet.
- Hardware wallet
  - ↳ Trezor Model T & Ledger Nano X.

MetaMask

1) Web browser extension allows run ethereum D-Apps without running a full node.
2) Full node installation of → disk space & time
3) added from chrome web store
4) Interface to interact with block
5) Provides a valut acc-
6) provides credentials using group of 12 words using wallet-seeds.
7) Crypto wallet & gateway for blockchain apps for everyone.
8) Online / Free version

Binance

1) crypto exchange platform that can sustain 1,400,000 orders per second.
2) Users looking for binance wallet based extension to send & receive tokens
3) Online / Free version

Pros-
- → multiple cryptocurrency support
- → Very secure
- → SegWit & Bech32 address support
- → Built in exchange facility
- → trustworthy name in world

Cons-
- → Mediocre customer support
- → Not ideal for beginners

Coinbase

1) Allows users to buy-sell transfer & store digital currencies securely online.
2) provides balance sensor payment tools using one interface.
3) Traders in need of storing all kind of digital assets with crypto wallet.
4) Online / Free version

- Features
  - → ability to earn interest on coins
  - → Robust customer support of high quality
  - → Built-in-support for DApps digital marketplace

Pros-
- → easy to use for beginners
- → supports a large no. of crypto assets
- → access DApps across multiple blockchains
- → only charges network fees

Cons-
- → Has history of bad customer support
- → Not open source.

U-5

Blockchain Ethereum Platform using Solidity

Ethereum –

- decentralized blockchain platform
- peer-to peer network.
- opensource & distributed computer
- creation of smart contracts & decentralized appl^n → dapps.
- open source OS → deals with smart contract functionality.
- support second largest cryptocurrency → Ether.
- transaction based state machine.

Features –
- Ether → Ethereum's cryptocurrency
- smart contracts → Imp. & distribution of contracts
- EVM → fundamental technology → structural design & software
- DApps → decentralized appl^n.
- DAOs → Decentralized Autonomous Organisations (D

Appl^n –
- Voting systems
- Banking Systems
- shipping
- Agreements.

Types of Network –
- Mainnet
- Testnet.

Components →
1) Nodes
2) Ether
3) Gas
4) Ethereum accs → 1) externally owned acc 2) contract acc.
5) Nonce
6) storageRoot
7) Ethash

* Ethereum Virtual Machine (EVM).

- main of Ethereum protocol & its fuctionality
- Provide runtime that can execute code written in smart contracts.
- It is similar to JVM [Java Virtual Machine]
- executes smart contracts & compute state of Ethereum network.

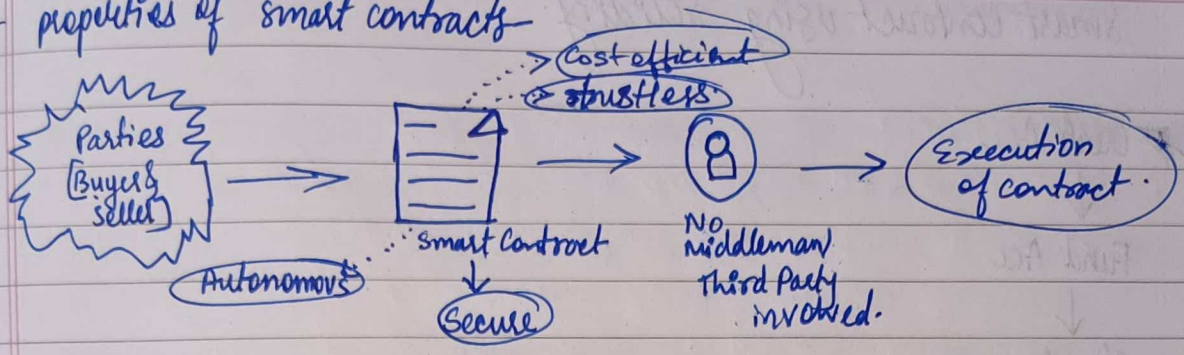
EVM Architecture (diagram in text)

adv → • permits anyone to create their own DApp.
- infinite potential use cases for this type of software.
- isn't profited to limited group of ppl.
- adv of smart contracts.
- latest example → Non fungible tokens (NFTs)
- easy access to art market in virtual way.
- everyone may create digital art & sell it.

* Smart Contract.

- program that runs on Ethereum blockchain
- computer immutable programs that run deterministically

* properties of smart contracts



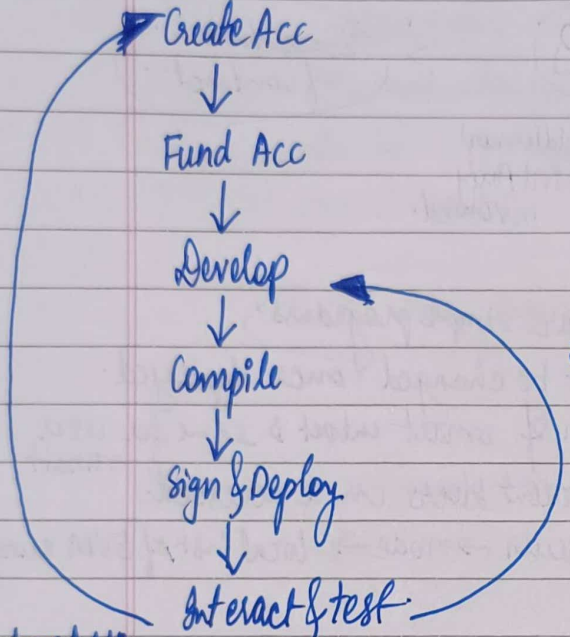
- compute program → smart contracts are simple programs.
- Immutable → smart contract code can't be changed once deployed.
- deterministic → outcome of execution of smart cotract is same for user running it.
- EVM context → very limited context, recent blocks can be accessed.
- decentralize world computer → each ethereum → node → local inst of EVM running.

Adv → • speed & savings • security & trust • Autonomy
• speed • accuracy • Unreliable input.

high level language (smart contracts → • LLL • Serpent • Solidity
• Vyper • Bamboo

Types → • Smart Leagal contracts (Legal action take)
• Decentralized Autonous Organization (DAO) (self enforcing code)
• Appln Logic Contracts (ALC). (sync with other contracts)

* Smart contract using Solidity.



- onboard/add users
- create new accs
- develop new appln.

* Solidity -

1) Pragma → define solidity version. (code was in).
   eg → pragma solidity ^0.4.0 ;

2) Variables → State
   - value permanently stored in contract storage.
   - eg → uint storedData; // state variable
   - Local → • value present until fun^n executes.
     eg → variable inside fun^c
   - Global → special variable → get info about blockchain
     eg → block.difficulty (uint)

3) Access modifiers - Public, Private, Internal & external.

4) Enums - way to create user defined types. Assign names to constants.
ex → enum Week { Mon, Tues, Wed }.
// Access using Week.Mon.

5) Arrays - type arrayName [size];

6) structs - struct struct_name {
type1 name1;
type2 name2;
}

7) Mapping - dictionary in Solidity.

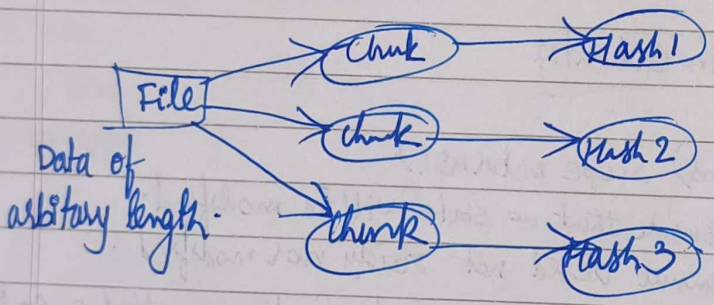
8) Fuction - fe name (parms) scope returns()
→ 1) view - ensure that no state will be modified.
2) Pure - ensure desed not ready nor modified.
3) Fallback - when non-exsistant fuction is called on contract

9) Events - Declared event keyword. inherital makes of contact.

Solidity → Adv → • allows complex data types & member variable.
• provide Appln Binary Interface → type safety.
• refers to Natural Language Specifications → user specification into language that machine can understand

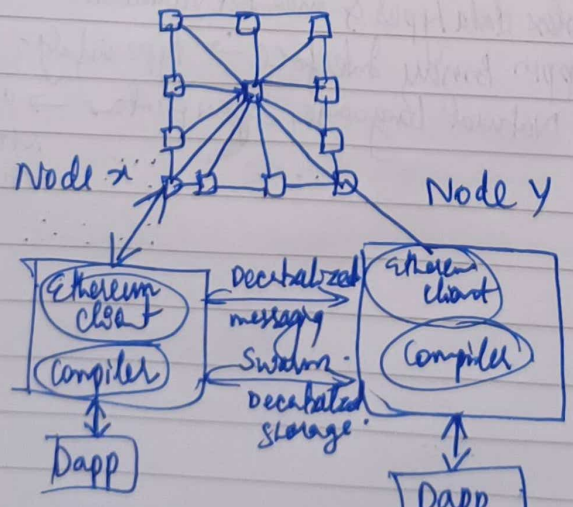
Swarm –

- decentralized storage & comun^n platform.
- deliver permissonless, censorship resistant infrastructure.
- provide a range of Web 3.0 services including messaging, music & vide streaming & hosting database.
- base layer infras^n for fully decentralized internet.
- Basically a giant distributed Hashtable (DHT).
- decenteralized protocols → IPFS, BitTorrent use DHT storage.
- Distributed storage chunks (DISC) underlying storage model for Swarm.
  Immutable
- Swarm cuts data in chunks → each chunk → max of 4 KB



Whisper –

- Decentralized, peer to peer, censor resistant, messaging communication protocol that DApp uses to communicate with each other.



Decentralized Messaging Platform → 1) StatusIM 2) Matrix 3) Wickr 4) Signal.

U-6

Blockchain Case Studies -

Blockchain Appln

- Agriculture
  - RFID based Agri food system
- Healthcare
  - Medical Record
  - Medical sharing
- Supply chain Logistics
  - Food traceability system
- Business
  - Finance
  - Banking
  - Insurance
- Energy
  - Carbide energy system

Blockchain in Retail –

1) Supply chain / inventory oversight
2) Taxation [Due to trasparency & less fraud]
3) Preventing Fraud & counterfiets goods.
4) Digital identity management for customers

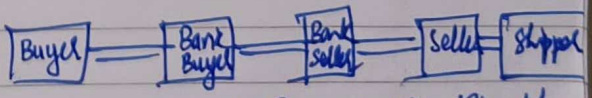
Benefits →
- Reducing streamline Tax
- Reducing Cyber Crime
- Proper Inventory Management
- Use of crypto as payment method.

Banking & Finance –

- Trade Finance –

1) Letter of Credit [Bank does that on rule buyer will pay seller once items have been received.
2) Bill of lading [shipment receipt].

Adv →
1) Trust Mechanism
2) Fraud & Authenticity
3) Reduced times.
4) Traceability
5) Information Transmission.



Trade Finance using Blockchain (HSBC case study)

Govt Sectors & Public Sectors.

- Smart Cities
- Tracking Vaccinations
- Tracking loans & Student Grants
- Payroll tax collection.
- Central Banking
- Validation of Education & Professional Qualifications.
- Voting

Healthcare –

- Supply chain transparency.
- Patient centric electronic health records.
- smart contracts for insurance & supply chain settlement
- medical staff credential verification
- IOT security for remote monitoring.

IOT use cases –

- Distribution
- Immutibility
- Decentralization.