#WEB-3

Topic : .....

PAGE NO. Avati
DATE / /

Blockchain → Decentralized
↳ First to digital coin - 1988, But had send copy problem i.e copy remains digitally & stored even if u send other. i.e Bay zantine General problem.
↓
Bitcoin solved it → Ethereum extended it
↳ Digital currency → But also smart contracts.
to aggreements than only money i.e smart contracts.

Diff types of blockchains exists.

Types of Blockchains:
↳ L1 → independent like Solana.
↳ L2 → Built on top of L1, ~~like~~ commonly Ethereum. L2s like Arbitrum, zkSync are built on top of Ethereum.

Mainnet → Real Money IRL funds.
Testnet → Practice Money.
Faucet → To get Testnet we go to faucet (typically site which is free).
ChainIDs → ~~Hetps~~ Unique no that tells which blockchain we are using.
Oracle Problem
↳ Blockchains runs on isolated system so hard to enforce IRL

Oracle → Service that bridges to RL.
Decentralized Oracles Networks (DONs)
↳ Oracle needs decentralized network to be trust worthy which is DONs gives.

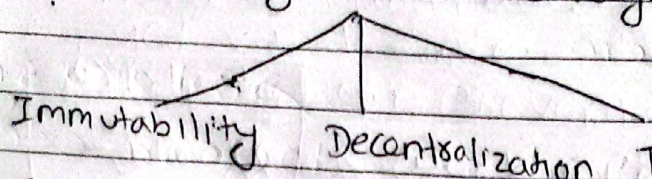
Never Stop Learning...

Topic : .....

PAGE NO. Aarati
DATE / /

⇒ DON is network of multiple, independent oracle nodes.

3 Pillars of Trustless Agreements



EVM (Ethereum VM)
- ↳ Engine for Ethereum smart contract.
  - ↳ used for running same code in all nodes.
- ↳ EVM Equivalence:
  - ↳ Its chain designed to behave identically to Ethereum mainnet in every way.
- ↳ EVM compatibility:
  - ↳ Its chain that can execute smart contracts in EVM, native langs like solidity.

Wallet
- ↳ secure digital application allows you to manage ur digital assets & interact with blockchain networks.
  - ↳ Eg: Metamask

Gas → Fuel for ethereum network.
- ↳ Gas is unit used to measure the computational effort used in transaction i.e gas price.

Transaction Fee = Gas used x Gas Price

Topic : .....

PAGE NO. Aarati
DATE / /

Smart contract needs more Gas.

If you offer more than avg gas price, it will be sent fast. same with ~~tow~~ less than avg gas price. These gas price are get by miners.

Smart contracts.

- Written in Solidity or Vypes.

```
contract SimpleTk {
    function mintToken() public {
        //code that creates tokens for
        whoever calls this function
    }
}
```

1) write smart contract code
2) Compile
3) Deploy.
   - Transparence code to all

Topic : .....

Blockchain Architecture.

① Sybil Attack
→ If some creates 9ts own 1000's of nodes it will have more weight & get valid state.

② ↳ Blockchain Prevents it by
- : Proff of work (PoW) } &
- Proff of State (PoS) } → sybil Resistance

② Finality
↳ when is transaction considered Final?

③ Consensus Problem
↳ How do we get all nodes to work together.

Bitcoin → PoW B.C
Ethereum → PoS B.C

Bitcoin → PoW
↳

Hash → length doesn't change
↓
Block — [Nonce, Data, Hash]
↓
Mine ← Miners had to find nonce (eg 7502) that when hashed with Block no 1 with data gave i would

Never Stop Learning...

Nonce = Number used once

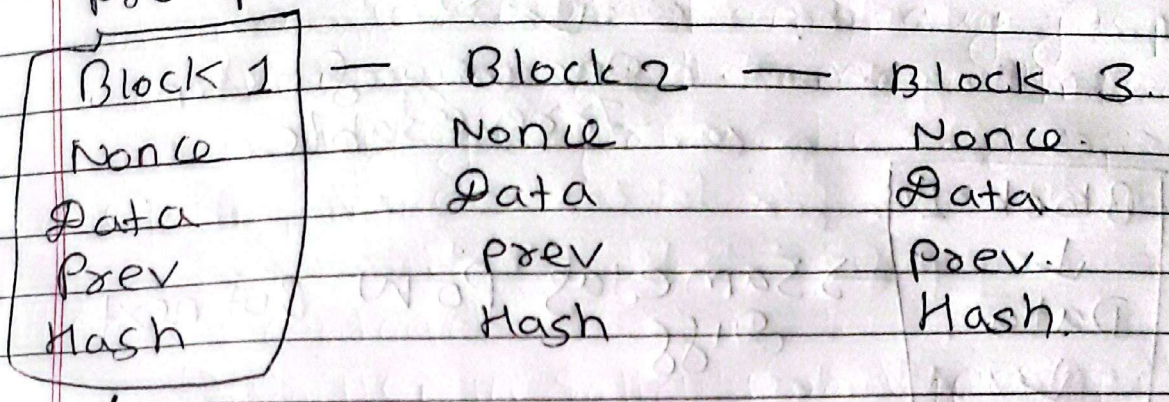
Topic : .....

PAGE NO. Aarati

DATE / /

start with 4 zeros. They have force.

prev points to prev hash



↳ Genesis Block: First block of blockchain.

~~But how~~

Who has more correct hash ⇒ Real block

PoW : Longest chain Rule

Occasionaly 2 miners might solve a block nearly same time called fork. Network resolves it by longest chain Rule. Whichever chain has next block added to it first becomes longest.

Signatures

↳ Private key

↳ Public key

ECDSA Signature :

↳ Generate Seed phrase

↳ Derive public & Private keys.

↳ Generate Addresses

↳ Sign Msg ⟶ custom or Ethereum using private key

↳ Verify Signature

Never Stop Learning.

Topic : .....

DATE / /

PoS Blockchain

↳ keccak256 hashing

↓

one way function

Irreversable

Block 1

↓

Data

↓

Hash

→ Same as PoW But next Diff

↓ Sign instead of Mining.

Block No: 2

Transactions: - - -

Current block hash

Signed Hash =

Prev hash

Instead of Miners we have validators. They dont compete. Instead they all vote on which is correct hash.

If validator do bad things their stake gets slashed (burnt).

2048 = Max stake

32 Eth = Min stake to participate as validator.

Never Stop Learning

Topic : .....

PAGE NO. Aarti
DATE / /

Each 12 sec validator proposes block this time is called slot. Every 32 slots = 1 Epoch = 6.4 min. Other validators will vote if 2/3rd is voted its valid block.

Blockchain Vulns

↳ Infeasable Rn (Never happened in BTC & Eth)

(1) 51% Attack

↳ If someone does attack & have more than half of vote: If they have in PoW 51% of vote they can rewrite history. In PoS if they ~~ca~~ have 51% vote they can exclude certain transactions, reorder for profit. But not reverse finality it need 2/3rd of vote.

↳ But pointless cuz they would just abandon that chain & create new one. This system is called social layer. called Blockchain Reorganization.

(2) MEV & Sandwitch Attack

↳ occurs even in Eth.

↳ Our Transaction queed in mempool.

↳ Maximum Extractable Value

↳ ~~Bot would take ur~~

Steps:

① Users submit a large buy for token, which enters mempool.

Never Stop Learning...

② A bot monitoring mempool detects this large market-moving transaction.

③ Bot sandwiches user's transaction by submitting it with higher gas fee which increases token's price. Bot immediately submits a sell order for tokens it just bought. Gaining profit. Its legal but unfair.

⑤ Replay Attacks

↳ occours when actor takes valid signed transaction from one B.C & rebroadcasts in other. Modern B.C have ChainID & Nonce to prevent it.

④ Bugs in Code.

Hard forks

↳ Hard fork is technical process used to implement protocol upgrade on Eth.

↳ votes occours & it's high = Protocol changes

↳ changes in Eth begin with formal techical document Ethereum Improvement Protocol (EIP). Anyone can propose it which goes long months or years review

↳ EIP stages:

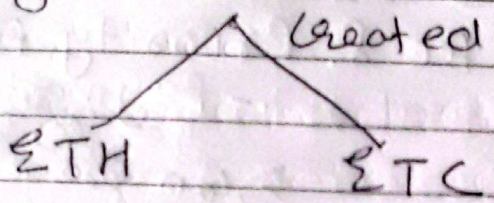
① Drafted
② In Review.
③ Last Call
④ final

Topic : .....

PAGE NO. Avanti
DATE / /

Types of Hard forks.

1. Non-contentious Hard forks (Planned upgrades).
   - Common scenario. All agrees.
2. contentious Hard forks (Chain splits)
   - Here significant portion of community disagree with proposed change.
   - Can create split in B.C
   - Eg: DAO forks



EIP Types.

- Core:

ERC (Ethereum Request for Comment).

- Standard for Blockchain. like RFC in web
- All ERCs are EIPs but not all EIPs are ERCs.
- Common Framework for B.C.
- Eg: ERC20, ERC721...

Gas

- More Transaction = More Gas Price

Never Stop Learning...

DATE

Topic :

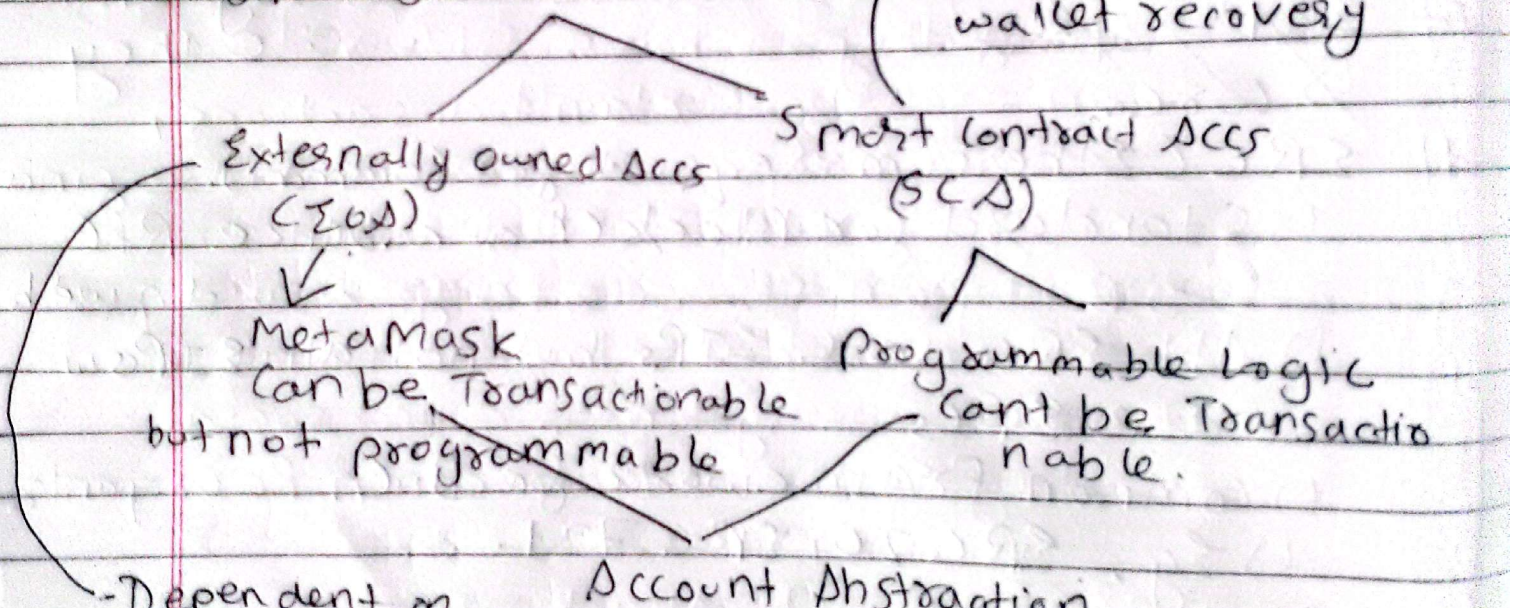
Types of Transactions

(1) Type 0: Legacy
- First Price Auction Model.
- They said gas Price & gas limit one with high price woould get fast.
- legacy & stuck in pending state.

(2) Type 2: EIP-1559
- Split into Base fee & Priority fee (Tip)

(3) Type

Types of Accs



- Dependent on Private key
- Requires funds to pay gass fee.

Account Abstraction
↓
Abstracting Those problems
↓
Smart Wallets.
↓
EIP 4337.

Topic : .....

PAGE NO. Aarati
DATE / /

EIP 4337 (Smart Contract Process):
- ① User operation
- ② Alt Mempool
- ③ ~~Bot~~ Bundlers
- ④ Entry Point Contract.

Temporary Smart Wallets (EIP-7702).
- ~~EOA~~ allows EOA to acts as SCA for 1 transaction. Delegate to Smart ~~to~~ wallets. for 1 transaction. Delegate to Batch Transaction Smart contract.
- These are Type-4 Transaction.
- Metamask has it built in.

B.C & S.C Use cases.
- Decentralized Finance (Defi).
- Decentralized Exchanges (Dexs):
  - Platform like Uniswap & Curve allows to trade digital assets directly without center intermediary. without KYC acc creation.
- Lending & Borrowing.
- Yield Farming = Reward users with additional token for participating.

Tokens = Digital Representation of value or utility that exists on blockchain.

Never Stop Learning...

PAGE NO.
DATE / /

Topic : .....

Types of Blockchain Token

- Native Tokens: Eg: ETH, BTC, SOL.
- Fungible Tokens = Non-unique
  - Stable Tokens
  - Utility Tokens
  - Reward Tokens
  - DAOs.
- Non-fungible Tokens = One of kind
  - In Metadata
  - Usecases: Digital Art, ENS Domains / Ingame Assets
- Semi-fungible Tokens = ERC1155
  - Usecase: Even Tickets, Certs, Token Gating.

RWA = Real World Assets.

Stablecoins = Providing reliable medium of exchange & store of value without volatility associated with other crypto.

- Types of stable coins
  1. Fiat-Backed
     - Backed by country like USDT
     - Centralized.
  2. Crypto-Backed.
  3. Algorithmic.

More Tokens = More weight in vote

Topic : .....

PAGE NO. Aarati

DATE / /

2 ways to Acquire & Trade Tokens

CEXs

CoinBase, Binance

fast.

On Ramps: Currency to Crypto

Off Ramps: Reverse

There are Sellers in CEXs.

DEXs

~~P2P using ZK Ps~~

Your wallet, or private key

Uniswap

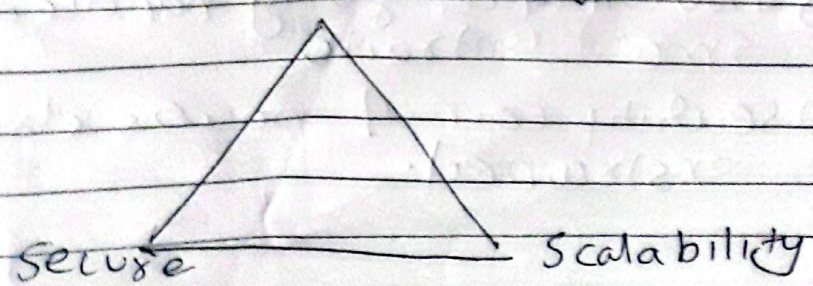
There is Liquidity pool where u put your tokens & you just swap them instead of trading

Uses . AMM (Automated Market Makers)

L1 = Main chain

L2 = Testnet built on L1

~~Rollups~~ : #Blockchain Trillema



only 2 can happen in B-C

Never Stop Learning...

ZkSync = L2 scaling soln for Eth

PAGE NO. Aarti
DATE / /

Topic : .....

Eth has just Decentralized & Secure lacks Scalable. only 15 transaction/sec xn.
No of transac req = Gas Price

Rollups fixes it by executing transaction on L2 chain & bundling or rolling up hundreds of them into single batch & then transfered to L1.

Types of Rollups:

- Optimistic Rollups
  - All transaction in batch are valid by default. If there is fraud proof the fraudlent batch is reverted
- ZK Rollups.

#Rollup stages = Measure decentralization maturity, not direct security

0

1. Stage 0 – Full Training wheels
   - Heavy reliance on operators.
2. Stage 1 – Partial Decentralization
   - security council limited to emergency fixes
3. Stage 2 – No Training wheels
   - Governance fully handled by smart contracts
   - Security council powers strictly constrained.

Sepolia = Public testnet for Eth

Topic : .....

PAGE NO. 1

DATE / /