After Mid # 01

SUBJECT _____ Day_____ Month_____ Year (20)

⇒ Blockchain & Cryptocurrency

Lecture # 16

⇒ Public key VS Bitcoin Address

⇒ Public and Private key

Signature is of that authentic person or not?

↳ we use public key

⇒ Verification function → Signature, public key, message hash

↳ Check ans, Yes / NO?

⇒ Public key is used to do transaction, Transn krnay way waqt kam ati hai.

⇒ Bitcoin Address is used when we want to receive a bitcoin from someone else. Transn lainay way waqt kam ati hai

⇒ Bitcoin Address is derived from public key tou jab b kisi say Bitcoin laina ho tum usay apna B. addrs daitay hain.

⇒ Public key is used when we want to send or perform a transaction.

⇒ Bitcoin address is derived from SHA-256 algo.

⇒ we think about worst case scenario that if one day someone is successful in deriving Private key from public key.

then our whole sys will be compromised, so we add a type of security layer in the form of B.addrs, so if someone tries to # reverse engineer it, it will first derive the PK.

(HD) Wallets.

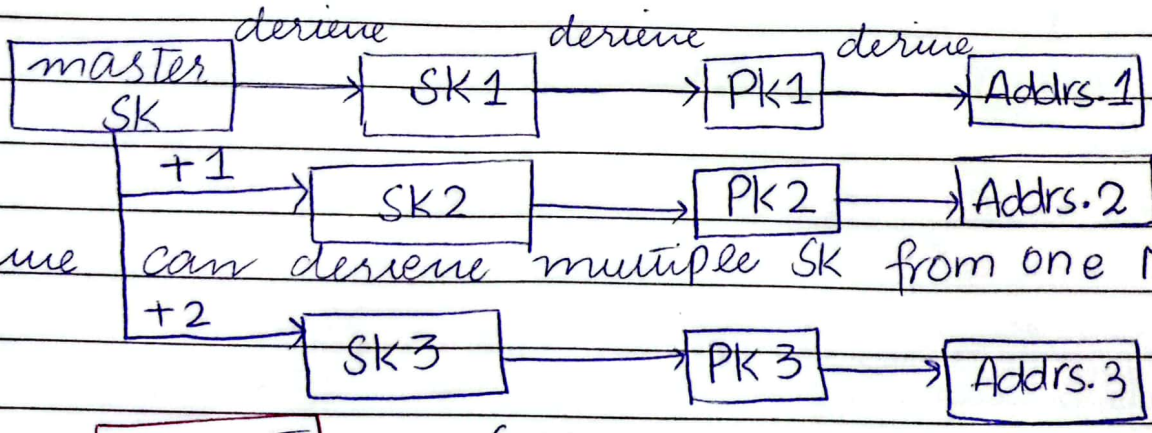
⇒ Hierarchicaley Deterministic Wallet :-

⇒ Privacy issue ⇒ pattern

⇒ an address is noted that this address is receiving or sending multiple Bitcoin to a same address. We might infer that this address belongs to someone rich.

⇒ So hackers can track our pattern this will increase the security risk.

↳ Solution → (HD) Wallets :-



Our wallets are smart enough to handle this so we can pay & receive payments from different addresses. This is a secure method.

Bitcoin 2008 → Satoshi Nakamoto.

SUBJECT _____ Day_____ Month_____ Year (20)

⇒ SK has no control to track what was done by MK, but MK can track anything. ✓

hierarchy is maintained:- CEO → emp1, emp2, emp3.

⇒ we cannot do payment from master keys (public) ← X

but can see the actions of public keys.

master public key → generate public keys.

lecture # 17

Ethereum :- 2013 → Vitalik Buterin

↳ provides us Ether.

⇒ How to run Smartcontracts app on Blockchain.

⇒ Create your own d-apps.

⇒ Ethereum has tokens → TRX, SNT, REP, AE

⇒ Ethereum is an open source blockchain-based platform.

↳ immutable, ledger

Ethereum Nodes (P2P based Network)

⇒ Scripting language used by Ethereum is Solidity

↳ a way to create programs using bitcoin

↳ It is a high level statically typed programming language used by Ethereum, specifically to write smart contracts on a blockchain

Purpose: Ethereum:- To create a platform to let others to create/build programs on top of it.

↳ It is a turing complete language

SUBJECT _____ Day_____ Month_____ Year (20)

Bitcoin:- Purpose was to create a cryptocurrency to eliminate banks (third-party) and allow us to trade permissionless or borderless.

⇒ **Understand Ethereum:-** We build a BC that not only allow us to store transaction data but actually allows us to store programs to facilitate the execution of a program & make any application decentralized.

Decentralized?

Decentralized Infrastructure:- Instead of relying on a central server or authority to operate, D-apps leverage a decentralized network of nodes (computers) running on Ethereum BC.

Smart Contracts: D-Apps powered by Smart Contracts, which are self executing code deployed on EBC. They define rules and logic of D-app and automatically executes when certain conditions are met.

Consensus Mechanism (POS) Proof of Stake. This allow participants (validators or miners) to agree on the state of blockchain without the consensus of ~~[illegible]~~ central authority.

What is Smart Contract?

→ Program / code that runs on BC.

⇒ A **Contract** is a set of rules/clauses that parties agree on, that governs the relationship between them.

Bitcoin → Coding language → Bitcoin Script
(Not turing complete)

Each node has :-
i) History of all smartcontracts and all T's
ii) Current state of all smart contracts

#18: Dapp → Backend ⇒ Decentralized applications
→ Frontend (DAPP)

⇒ Security Issue
: Viruses and auess to peivate file.
: Infinite loop / Heavy computations
→ Sol:-

Ethereum Virtual Machines (EVM) :-
⇒ People become part of EBC (participants) through EVM and then a local copy of BC is created on VM and not on our local ~~copy~~ machine, so in case of any attacks, only VM data will be affected.

Infinite loop sol :-
⇒ Developer of smart contract will be **penalized** for writing that code ⇒ Gas

SUBJECT _____ Day_____Month_____Year (20)

Gas :- Any computations that runs on BC, developer of the smart contract needs to pay.
- Any transaction that modifies the BC costs gas
⇒ Gas cost depends on the complexity of code.
⇒ It does not matter that Ether is high or low.
⇒ In the backend we pay with Ether.
⇒ If transaction is failed (not valid) Gas Price is not returned.
⇒ If T's is cancelled while staying in pending state, Gas fees is returned.

(DAO) Decentralized Autonomous Orgs :-
generic → rules way avoiding authorization or actions horay hain
→ har rule way against ain smart contract bana dataay hain. Services offered are handled automatically. All the activities are transparent & fully public
Ex - Automatic car without a driver.
⇒ These Smart Contracts are then launched as transactions on decentralized networks and they become decentralized apps.
⇒ No human intervention.
⇒ User and miners way consent way bagair there will be no change in the code.

SUBJECT lecture # 19 Day Month Year (20)

⇒ **Segregated Witness** (SegWit).

⇒ related to **Bitcoin chain**

⇒ Bitcoin block size → **1Mb** **parts of block:**
miners have to fill it → nounce
→ reciever's address
⇒ signature value takes → signature value etc.
most of the **space** of block. Miners raised a concern that there is very less space for transactions as most of the space is filled up by block's attributes.

⇒ We will need signature only when we want to **validate** transaction, as every transaction has a signature included to it, the size of transaction is becoming large due to this and less no. of transaction can fill up the block.

⇒ So miners that participate in verification recieve very **less incentive**.

⇒ So they decided to do voting of miners on this update, so they decided to segregate the signature.

⇒ Signature is basically the **witness** of our Tran. So, they thought that for signature they will use an **extra** memory that will contain signature and transaction detail and the **pointer** to this memory will be stored on the block.

SUBJECT _____ Day _____ Month _____ Year (20)

⇒ Memory can be centralized, extra details of transm make up to 60.% of that tranm so using transm id we can track down the extra memory. So this update was segregated witness.

⇒ Date of update :- 20 July [redacted] 2017 476768

⇒ Block no on which update was done :- [redacted]
↳ Soft fork

⇒ Compulsory update due to majority consent.

⇒ Stock Decentralized autonomous Org was created by vitalik. People put in their investments and everything else (oprs) were poured in to stock market.

⇒ It became very popular among people.

⇒ 17 June 2016 attack was the biggest hiest in the world of Blockchain.

⇒ 50 million dollars were successfully stolen. 50,000,000 dollars.

ESCROW State :- Money Transm is approved and after sometime it will move to the receiver's account.
↳ child account (intermediate State).

⇒ DAO way apnay account say approve hoi hai tranm of 50 million, [redacted] to an account ABC.

SUBJECT _____ Day_____ Month_____ Year (20)

⇒ As it is a public address we cannot tell who's account is this. It is anonymous.
⇒ Organization was seeing this all but couldn't do anything at the moment bcz people would panic and DAO would fail and this DAO was created by Ethereum people, so Ethereum's chain reputation would be at stake, eventhough it was not the chain fault. There was some issue in the DAO's smart contract 'a loop hole'.
⇒ Audience were revealed about this later on. Money belonged to people, so to save Ethereum's stake. There came an update that was not compulsory and chain was broken into two parts. 'Basic Ethereum' (ETH) & 'Ethereum classic'. (ETC)
⇒ all chain in hierarchy may transaction. (ETC)
⇒ Dosari chain ko centralized nhi transaction is reverted back. (ETH)
⇒ hard fork → soften rules → updation is not compulsory
⇒ Spilted in ~~2016~~. 20 July 2016
⇒ after reversion process, DAO was updated

SUBJECT _____ Day_____ Month_____ Year (20)

⇒ In case of Soft fork, chains are **not** **Spitted** because it is compulsory as it comes after the consent of majority miners

Bitcoin updates

① 20 July 2017 (Soft Fork)
↳ Segregated witness on block **476768**

② 1 August 2017 (hard fork)
↳ Bitcoin block size up to 8MB **BitcoinCash**
current " 32MB
↳ Spitted in two chains
↳ Bitcoin Cash → Block no: **478558**
↳ Bitcoin

③ 24 October 2017 → ASIC resistant net
↳ hard fork (again chain is
↳ spitted → **Bitcoin Gold**
↳ Block no → **491407**

Lecture # 12, 13

Nounce → 32 bit number — 4 billion nounce, 4 billion different hashes.

Range → 0 to $2^{32}-1 \simeq 0$ to 4×10^9.

Total no of possible hashes $= 16 \times 16 \times \dots 16 = 16^{64} = 10^{77}$

" valid hashes (with 18 leading zeros) $= 16^{64-18} = 2\times10^{55}$

Prob that a randomly picked hash is valid $= \frac{2\times10^{55}}{10^{77}}$

$= 2\times10^{-22}$

probability that one of the hash is valid $= 4\times10^9 \times 2\times10^{-22}$

$= 8\times10^{-13} \cong 10^{-12}$

(Using only Nounce is not enough.

↳ see → Timestamp:

↳ 32-bit

when timestamp change, miners can start again from 0th Nounce.

current hashing rate is equal to 180 million trillion/sec.

4×10^9 nounce is checked in 4×10^{-9} seconds

$4\times10^{-9} \ll\ll\ll 1$ sec. (problem)

before a change occure in timestamp, all the nounces are already exhausted.

Mempool → area where all unconfirmed transactions are placed.

miners try to chose transaction that has more fees ~~when~~ when in less than 1 sec all nounces are checked, miner will replace its Tran with min fees with a Trans that has fees relatively just small to the previous transtion. (process → change Block configuration)

when timestamp finally changes, miner can again pickup the transaction with more fees. If ur fees is very very low it is possible that a miner never picks up your Tranx.

Mining Pool:- collect group of miners who combine their computational resources over a net. The primary purpose to join it is to increase the chances of successfully mining the block & receiving the associated block reward. The reward is distributed among the participating miners based on their contributed hashing power.

*an innovation that significantly alters the way that consumers, industries or businesses operate

SUBJECT Blockchain Day Month Year (20)

⇒ Blockchain and Cryptocurrency ⇐

Q: Why should we study Blockchain?

disruptive technology* and give us the idea of trust.

Q: What is Blockchain?

⇒ Any data written on block is immutable,

⇒ ledger book → block.

⇒ transactions are encrypted

⇒ Blockchain is a distributed immutable ledger which is completely transparent. It is a growing list of records, called blocks, which are linked and secured using cryptography.

Applications of Blockchain.

i) Smart Contract

ii) Voting Systems

iii) Product Tracking

iv) International Wire Transfer { Sender Bank → Correspondent Bank → Reciever Bank }

v) HealthCare System.

Hashing Algorithm.

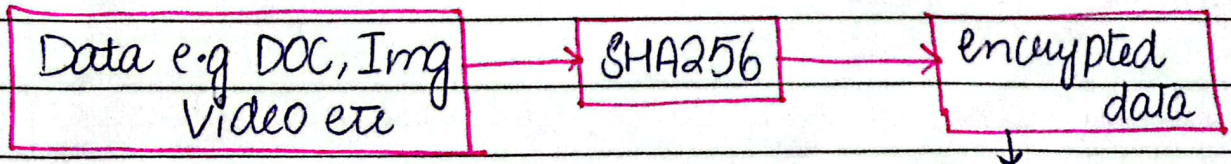
Block Contains:-

Data eg "Hello World"

Prev Hash

Hash (fingerprint of block)

↳ generated by "SHA 256" Algorithm.



64 hexadecimal chars each of 4 bit.

total 64*4 = 256 bits

SHA – Secure Hash Algorithm

SUBJECT _____ Day _____ Month _____ Year (20)

⇒ first block is called "genesis block" (don't require previous hash)

Requirements of Algo

* One Way — Data → Encrypted ✓ ; Encrypted ✗ ← Data
* Deterministic (same hash for same data every time)
* Fast Computation
* Withstand Collision. (no hacker can easily hack it) (Creating / altering doc to have the same hash should not be possible)
* Avalanche Effect. (Even a single bit of data would result in an absolutely different hash).

Immutable Ledger :- Blockchain prevents alteration of data.

→ if hacker wants to hack a block, he will have to forge the blockchain

→ SHA is developed by National Security Agency (NSA)

→ World Bank → 70% of population doesn't have entitlement to their properties.

What is Distributed P2P Network?

Centralized Network : a single server responds to all clients requests.

→ easily hackable (all data is at one location)

Distributed P2P :- no single server, every comp is connected directly or indirectly with every other comp on the network (difficult to hack).

→ used for recovery of data, if hacker is successful in forging a blockchain.

SUBJECT _____ Day_____Month_____Year (20)

Blockchain Mining

Blockchain mining creates a trustworthy and secure environment because there is no single authority, first the transaction is checked by the miner to make sure if it is valid or not, then the block created by the miner is verified or validated by other miners before adding it to the chain.

Transaction → mempool → miner creates a block → solve mathematical problem

Lecture :- → tell others to mine the block → verify block → reward to miners

Comparison with Traditional Database

T.DB :- * Centralized: data is stored typically on a single server or a cluster of servers controlled by a single entity

* Control: a central authority has all control over the whole DB. they can modify, delete, insert or manipulate data as needed

* Trust: Trust is established through central authority ~~which can be compromised or untrustworthy~~

* Security: Security relies on access controls, firewalls encryption, which are vulnerable to attacks

Blockchain :- * Decentralized: data is stored on a network of nodes which work together to maintain DB.

* Control: no single authority. Transaction & data changes are governed by consensus mechanism typically Peloof of work (POW)

* Trust: derived through transparency and cryptographic algorithms. Data is immutable and can be verified by anyone.

SUBJECT _____ Day_____ Month_____ Year (20)

* Security: it is inherent due to immutability of data & consensus mechanism. Once a block is added, it is nearly impossible to alter previous blocks.

Why we need new Technology :-

Several concerns:- 1) Trust and Transparency :-

2) Security 3) Immutable Records (Once data is added it cannot be altered)

4) Global accessibility: B.C operates on global scale, accessible to anyone with an Internet Connection.

5) Reducing Intermediaries : (peer to peer direct connection) reducing the need for brokers, banks, hence reducing cost & speeding up the process.

⇒ Distributed / Decentralized Ledger Technology :-

It distributes data across multiple nodes or location within the network. Data is synchronized & shared across a network of nodes by often using consensus to validate & record transaction.

Hence, no single point of control.

SUBJECT Blockchain

obj + shortquestions (co
(mcq's)
partial code (Syntax
_____.

Tokens → digital assests or representation of assests built on top of existing blockchain platform using smart contracts.

how public keys and signatures can be used for authentication. Dictates on how to agree on updates to the protocol itself. How nodes come to consensus over things.

Satoshi Nakamoto

Proof of Work (POW)

Q: What is Bitcoin? lecture # 11

Bitcoin:- Blockchain based network or decentralized technology or protocol. How miners will communicate, when they will be rewarded etc.

⇒ 3 important layers in Crypto World:-

Technology	Protocol/coin	Token/NFT
(Blockchain)	(Waves, Bitcoin, Neo Ethereum, Ripple)	(Bitcoin and Ripple has ~~no tokens~~.)

Protocol:- rules that guides how miners have to communicate with each other, and other users what power miner has etc.

↓

→ how participants of network communicate with each other (rules, IP, HTTP protocols.)

The Bitcoin Ecosystem:-

① Nodes, ② Miners, ③ Large Mines (→ government agencies), ④ Mining Pools (multiple individual miners collaborate)

no central authority, nodes can communicate directly

Nodes → sys that perform transactions

Bitcoin Monetary Policy:- (maintaining supply of money)

① Block frequency (kitnay time baad new block lagta hai)

[" Reward

② The Halving

SUBJECT _____ Day _____ Month _____ Year (20)

Bitcoin → BTC (Reward)

⇒ The Halving:-

⇒ after every 4 years, reward is halved.

ultimately goes to zero → then miners will leave blockchain? but miners will earn from transaction fees. Why people will give transaction fees? (after mid 1)

⇒ Bitcoin Protocol have some spaces that don't even allow majority miners to change something one of them is to change BTS (reward)

→ There is no code for it.

Block freq	Avg block time
ethereum	15sec
bitcoin	10min
ripple	3.5sec
litecoin	2.5 min

SUBJECT _____ Day _____ Month _____ Year (20)

Byzantine fault Tolerence:-

If our system has 1/3 or less traitors then our system will be still in safe state. Tolerence factor is 33% traitors. Tolerence factor is usually client specific

Merkle-Damgard Transform:-

We require that our hash functions works on inputs of arbitary length. As long as we can build a hash function that works on fixed len inputs, there's a generic method to convert it into a hash function that works on arbitary length.

SHA-256 is based on Merkle-Damgard.

SHA-Merkle Damgard Transform:-

⇒ it takes 256 previous output & bits

⇒ fix size input. Hashing is done in layers. First layer uses dummy 256 bits output.

⇒ We apply padding to the message if it is less than fixed input size.

SUBJECT _____ Day____ Month____ Year (20)

⇒ If the compression function C is collision free then SHA-256 is collision feree.

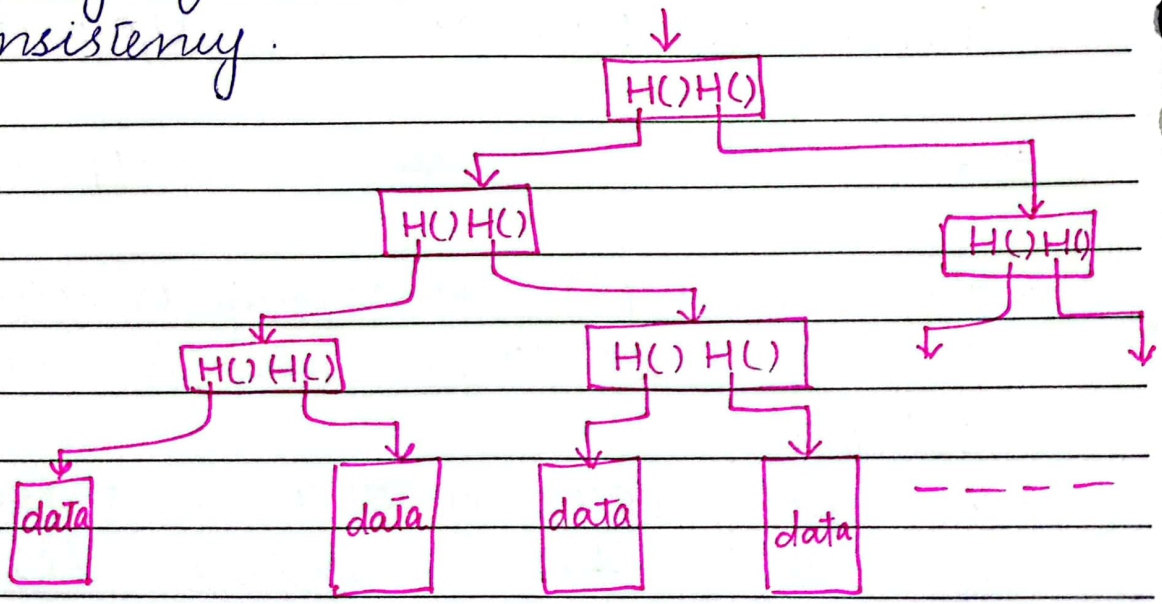
⇒ Merkle Damgard is used to design cryptographic hash functions like SHA-256. It involves the usage of fixed length of C functions that iteratively processes a block of data to produce a hash value.

⇒ It is primarily use to create variable-len hash fun with a fixed-len output.

Merkle-tree :-

⇒ Binary hash tree, used for efficiently verifying the integrity of data in a larger dataset.

⇒ They are used in blockchain to verify the validity of transactions and ensure data consistency.



SUBJECT _____ Day_____Month_____Year (20)

Q: How Byzantine fault tolerence works in BC?

Consensus Protocols

→ others

Proof of Stake (PoS) (used in ethirium)

Proof of Work (PoW) (early used in ethirium now " in Bitcoin)

⇒ Helps us in preventing attacks and in competing chain problem

⇒ Miner tried to add a malicious block at the end of blockchain (as a new block) Miner has to solve a mathematical problem that is a costly process it's require high computational power, electricity usage. When they solved it, they tell other miners about the new block, other " will validate data and verify the block if it is valid it will be added to the chain and the miner will be rewarded but if majority of other miner say that it is not valid then it will not be added in the blockchain and miner will have to face a loss.

SUBJECT _____ Day_____ Month_____ Year (20)

Q: What will happen when two miners solve the problem at same time?

In real world, latency in network always exists. Two miners have solved the problem, their blocks are also valid, however their blocks hash will be different because they have selected different transaction.

Miners will send their respective blocks to other miners for validation. If one Miners let's say Miner A block reached to majority of miners for validation and they have validated it then consensus protocol will ask which block should be added in blockchain and then block of A will be repeied back by majority and it will be added in blockchain.

Q: What if Miner A & Miner B blocks receive 50%, 50% validation?

Competing chain problem:-

A network in which we have two or more valid chains then the majority voted chain will become the part of blockchain.

for ex:- 50% orange
50% purple
] on block 11

Now protocol will provide them with another problem to solve for block 12, then if orange ones found them before purple ones then entire chain will be accepted because whole chain will become longer than purple ones. (Longest chain Rule)

The block of purple ones will be dropped, it will be called orphan block and purple ones will not be rewarded. ↳ block that was valid but due to latency could not become a part of blockchain

---

What is Bitcoin?

Blockchain based network or a decentralized technology or protocol.

Nonce

Q: How mining works? | What is Nonce?

⇒ Nonce → Number only used once.

⇒ It is also included in computing hash along with Block Number, Data & Previous Hash.

⇒ The Nonce keep on changing which results in changing of Hash.

⇒ It is the number that blockchain miners are solving for.

⇒ It adds extra power and flexibility to the security of the network.

How mining works (The cryptographic puzzle)

⇒ Hashes have always finite range.

⇒ Network publically generates a hash value (target hash), Miners have to find the hash saying beneath or equal to target " value, The one who finds it, win.

⇒ If we opt Round Robbin, then whose turn is next will be predictable and a factor of authority will be added.

Golden Nounce:-

⇒ If you find a hash below the target, you will be allowed to create a block.

⇒ The value on which we were able to create a block is called 'golden nounce'.

The ~~algorithm used in blockchain~~ is decentralized ~~autonomous~~ organization.

———.