BlockChain

1.What is Blockchain?

A **blockchain** is a chain of **blocks**, where each block contains **information or transactions**.
All these blocks are connected one after another, like links in a chain.

2. How it actually works

- When someone performs a transaction, it is stored inside a **block**.
- When the block is full, it is locked and connected to the **previous block** using a **hash** (a unique code that acts like a fingerprint).
- If someone tries to change old data, the hash will change — which breaks the whole chain.
  So, past data cannot be easily modified.

3. Not controlled by one person

Blockchain is **decentralized** — there is **no single owner**.
Instead, the same data is stored on **many computers (nodes)** across the world.
Everyone can see the records, so it's **transparent, secure, and difficult to hack**.

4. Where it is used

- **Cryptocurrencies** like Bitcoin & Ethereum
- **Smart contracts** which run automatically
- **Supply chain** to track goods
- **Voting systems**, **health records**, **NFTs**, etc.

Example

Suppose you send **1 Bitcoin** to a friend:

1. Your transaction goes to the Bitcoin network.
2. Many computers (miners) check and verify it.
3. If valid, it is added to a block.
4. The block is linked to the chain forever.

Nobody can erase or change it later.

5.Who are Miners?

Miners are people or computers that **keep the blockchain running and safe**.
They check every transaction and add it to the blockchain.
You can think of them as:

Digital accountants who confirm every transaction and make sure no one cheats.
In return, they get **cryptocurrency as a reward**.

What Miners Do (Example: Bitcoin)

1. Pick Up Unconfirmed Transactions

- Whenever someone sends Bitcoin, the transaction goes into a public pool.
- Miners gather these unconfirmed transactions.

2. Verify the Transaction

Miners check:

Does the sender have enough Bitcoin?
Is the signature genuine?
Is the same Bitcoin being spent twice?

If everything is correct → the transaction is marked valid.

3. Solve a Puzzle (Proof of Work)

- To add a block to the blockchain, miners must solve a **difficult math puzzle**.
- They must find a special number called **nonce**, which makes the hash correct.
- It needs heavy computing power, so it's like **a race between miners**.

4. Add the Block to the Chain

- The miner who solves the puzzle first announces the solution.
- Other computers check and confirm it.
- If valid, the block gets **fixed to the blockchain forever**.

5. Reward for Mining

The winning miner gets:

Block reward (newly created coins — like 3.125 BTC)
Transaction fees from all transactions inside that block

6.Why Mining Matters

Why it’s needed	Explanation
Security	Keeps hackers from changing data
Double spending prevention	No one can use the same coin twice
Decentralization	No central authority controls the network

7. What is a Nonce?

A **Nonce** means **"Number used only once."**
It is a number that miners keep changing again and again while trying to create a valid block.

Each time the miner changes the nonce, a **new hash** is generated.
If the hash matches the required rule of the blockchain (difficulty), the block gets accepted.

Why Nonce is Needed

In **Proof of Work (PoW)** systems like Bitcoin, miners must find a hash with a certain number of **leading zeros**.

Example of a valid hash:

00000000000000000004e9f3ab2c9d3fcd8a2d4b...

To get such a hash, the miner must:

1. Take all block data
2. Add a nonce
3. Pass it through a hashing function (like **SHA-256**)
4. Check the result

If the hash **doesn’t** have enough zeros → try a new nonce.
This happens **millions or billions of times per second**.

Only when a nonce gives the correct hash →
⇒ Block is accepted
⇒ Miner gets reward

Table

Term	Explanation
Nonce	A number used once during mining
Who uses it	Miners
Why change it?	To generate a valid hash
Role	Helps in block creation & network security
Result	Fair mining + one true winner

Example

Imagine a lock that opens only with **one correct 4-digit PIN**.

You try:

0001 → wrong
0002 → wrong
0003 → wrong
2851 → (correct!)

This correct PIN = **Nonce**
The moment you find it → lock opens → block is mined.

8. What is a Prefix

A **prefix** simply means **something added at the beginning** of another word or value.

Example:
In **unhappy**, the prefix is **"un-"** because it appears *before* the word **happy**.

So, a **prefix = starting part** of something.

Prefix in Blockchain / Hashing

In **blockchain mining**, *prefix* means the **required pattern at the beginning of a hash value**.

In Bitcoin, this pattern is usually a series of **leading zeros**.

Example

If the target prefix is:

0000

Then a valid block hash must start like:

0000f7b8a12d93e4c8...

If the hash:

- starts with 0000 → Block is accepted
- doesn't match → Miner changes **nonce** and tries again

Why Prefix Matters

- It sets the **difficulty level** of mining
- More zeros in prefix → **harder** to find a valid hash
- Higher difficulty → Requires **more computing power**
- Fewer zeros → Mining becomes **easier and faster**

Relation

Prefix + Correct Nonce → Valid Hash → New Block Added

If nonce doesn't create a hash with required prefix → retry.

Table

Term	Meaning
Prefix	Required starting pattern of a hash
In Blockchain	Usually zeros at the beginning
Purpose	Controls mining difficulty
More Zeros =	Harder mining
Found by	Trying different nonces