Proof of Work

1.Why Proof of Work is Needed

In a decentralised network, anyone could try to rewrite transaction history or create fake blocks. PoW prevents this because altering data would require re-doing the heavy computation for every block again, which is nearly impossible on a large network.

2.How PoW Works — Step by Step

1. **Transactions are collected**
   Miners gather pending transactions from the network.
2. **Puzzle solving begins**
   Miners compete to find a special value called a *nonce* that makes the block's hash meet the difficulty requirement (usually starting with several zeros).
3. **Whoever solves it first wins**
   The miner who finds the correct hash broadcasts the block to the network.
4. **Other nodes verify**
   Everyone checks whether the solution is valid and whether the transactions follow the rules.
5. **Block is added to the chain**
   The winner receives a block reward (newly generated coins + transaction fees).

Key Features of PoW

- **Secure** – Attacking the network requires massive computing power.
- **Fair** – Everyone has the same rules; success is based on real work.
- **Decentralised** – No central authority decides which block is correct.
- **Proven over time** – Bitcoin has run safely on PoW for over a decade.

Drawbacks

Despite its strength, PoW demands:

- High energy consumption
- Expensive mining hardware
- Slower block creation compared to some newer methods

Even so, many trust it because it mirrors age-old principles — effort earns reward, work builds value, and integrity is upheld through proof, not promises.

3.Why Bitcoin Takes 10 Minutes

Bitcoin is designed so that **one new block is added every 10 minutes**.
Not too fast, not too slow — just around 10 minutes.

1) Time to share the block with everyone

If blocks were created very fast, they would not reach all computers in time.
That would create confusion.
10 minutes gives the network **enough time to stay in sync**.

2) To release new Bitcoin slowly

If blocks came too quickly → new Bitcoins would be created too fast.
This could reduce value.
10 minutes keeps the **supply slow and controlled**.

3) Difficulty keeps adjusting

Every **2016 blocks (about 2 weeks)**, the system checks how fast blocks are being mined.
If miners become faster → the puzzle becomes harder.
If they become slower → it becomes easier.
This keeps the average **close to 10 minutes**.

In short:

Bitcoin takes 10 minutes per block so that the network stays stable and Bitcoins are released slowly and fairly.

4.Step-by-Step: What Happens When Vijay Sends 1 BTC to Priya

1) Transaction is Created

Vijay enters Priya's Bitcoin address, chooses 1 BTC, and sends it.
This creates a transaction that includes:

- Vijay's wallet address
- Priya's wallet address
- Amount: 1 BTC
- Vijay's digital signature (proof it's really him)

The wallet broadcasts this transaction to the Bitcoin network.

2) Transaction Goes to the Mempool

The transaction first enters the **mempool**, which is like a waiting area.
All unconfirmed transactions sit here until miners pick them.

Mempool = waiting list for pending transactions.

3) Miners Choose Transactions

Miners look into the mempool and pick transactions for the next block.
They usually select **high-fee transactions first**, as it increases their reward.

Higher fee = faster confirmation.

4) Proof of Work Begins

Miners now compete to solve a tough puzzle.
They try different **nonce** values to find a valid hash for the new block.
This takes electricity and computing power.

On average, someone solves it in about **10 minutes**.

5) Block is Added to the Blockchain

The miner who solves the puzzle first broadcasts the new block.
Other nodes check if everything is valid.
Once confirmed, the block is added permanently to the blockchain.

6) Confirmation of Vijay’s Transaction

The block containing Vijay → Priya transaction is now part of the chain.
That gives it **1 confirmation**.
As more blocks stack on top (2, 3, 6…), the transaction becomes harder to reverse.

Around **6 confirmations** = strongly final.

7) Priya Gets the Bitcoin

Priya’s wallet sees the confirmed transaction.
Her balance shows **+1 BTC**, and Vijay’s balance decreases.
After 6 confirmations, it is considered **fully safe and final**.

5.What Is Hashing in Blockchain?

Hashing means taking any kind of data — a message, a transaction, or an entire block — and turning it into a **fixed-length code** using a special mathematical formula called a **hash function**.

This result is known as a **hash**, and it acts like a digital fingerprint.

Bitcoin uses a hash function called **SHA-256**.
No matter how large or small the input is, the output is **always 256 bits (64 hex characters)**.

Example

Original text:
"Vijay sends 1 BTC to Priya"

SHA-256 hash (example):
f4c3d0d8c6f98e36a83e5c9e28b6c3e41cf5a6e3c5b4a1f8e92a9a3b3c3e7b9a

Now change just one small letter ("Vijay" → "vijay") —
the entire hash becomes completely different.

This sudden change is called the **avalanche effect**.

6.Why Hashing Matters in Blockchain

1. Security

- Hashes cannot be reversed to find original data.
- This keeps blockchain records safe.

2. Block Connection

- Each block stores the **hash of the previous block**.
- If someone changes old data, the hash breaks and the chain no longer matches.

3. Easy Verification

- Instead of checking full data, nodes can simply compare hashes.
- If the hash matches, data is unchanged.

4. Speed & Efficiency

- Hashes are short and fixed in size, making validation quick.

In Short:

Hashing turns data into a unique digital fingerprint that keeps blockchain secure, fast, and properly linked.

website for more understanding:https://andersbrownworth.com/blockchain/blockchain

7.Why the Longest Chain is the Truth in Blockchain

Step 1: Miners Compete

When a transaction enters the mempool, many miners try to put it inside the next block.
Each miner builds a block and tries to solve the **Proof of Work puzzle**.

Step 2: One Miner Solves First

If Miner A solves the puzzle first, he broadcasts his block to the whole network.
Other computers verify it and add it to their blockchain.

But sometimes, Miner B also solves a block at almost the same moment.
Now we have **two valid chains for a short time**.

Step 3: Temporary Fork

There are now two versions of the blockchain:

- One chain with Miner A's block
- One chain with Miner B's block

Some nodes follow A's chain, others follow B's chain.

This situation is called a **fork**.

Step 4: Mining Continues

Miners continue to mine the next block on whichever chain they received first.
After some time, **one chain grows longer** than the other.

Step 5: Longest Chain Wins

Bitcoin follows a simple rule:

The chain with the **most Proof of Work** (the longest chain) is the true chain.

When one chain becomes longer, the shorter one is dropped.
Blocks in the shorter chain become *orphan blocks*, and all miners switch to the longer chain.

Step 6: Why This Works

Because every block needs real computational work to be created,
a longer chain means **more work**, **more security**, and **more honesty** in it.

An attacker would need more computing power than the whole network combined to change history — which is almost impossible.

8.Bitcoin Supply Limit

Total Bitcoins That Will Ever Exist

Bitcoin has a **maximum supply of 21 million coins**.
This number is written permanently in the Bitcoin code by **Satoshi Nakamoto**.

No government or organization can increase this supply.

So even 100 years later, there will still be **only 21 million Bitcoins — never more.**

Why Was This Limit Created?

The goal was to make Bitcoin **scarce**, similar to precious metals like gold.
When something is limited, its value tends to remain strong.
This protects Bitcoin from **inflation**, unlike regular currency where more notes can be printed anytime.

Mining and the Halving Process

New Bitcoins enter circulation through **mining**.
Miners solve Proof of Work puzzles and receive BTC as a reward.

When Bitcoin launched in 2009, the reward was **50 BTC per block**.
Every **4 years**, this reward becomes **half** — a scheduled event known as **Halving**.

Year	Block Reward	Meaning
2009	50 BTC	Start of Bitcoin mining
2012	25 BTC	First Halving
2016	12.5 BTC	Second Halving
2020	6.25 BTC	Third Halving
2024	3.125 BTC	Fourth Halving

With each halving, fewer new coins are released.
This slow and controlled supply keeps Bitcoin valuable over time.

After the Last Bitcoin is Mined (Around 2140)

Around the year **2140**, all **21 million coins** will be mined.
After this point, miners will **no longer receive new Bitcoins**.
They will earn **transaction fees only** for securing the network.