What *is* a blockchain?

A blockchain is simply a special kind of ledger, a record-keeping system.

- **Ledger** : a book or database where you write down who paid whom, when, and how much.

The Problem with a Centralized Ledger

In the traditional world:

- **Single Authority** (e.g., a bank) keeps the master ledger.

- You **trust** that authority to (a) record honestly, and (b) keep your data safe.

But this comes with risks:

1. **Single Point of Failure**
   - If the bank's systems are hacked, your ledger could be altered or erased.
   - If the bank goes down, you lose access to your records.

2. **Trust and Control**
   - The bank can freeze accounts, reverse transactions, or charge hidden fees.
   - You have no direct control over your own data.

3: Solution Distributed Ledger

1. **Replication across many nodes**
    - Instead of just you and your friend, imagine hundreds or thousands of participants ("nodes") all holding their own copy of the ledger.

2. **Immutable entries**
    - You don't just "send a message"—you cryptographically lock each entry so it can't be changed without breaking the record.

3. **Agreement on order and validity**
    - Nodes need a way to agree on which transactions are real and in what order they happened.

4: Merkle Root: For hashing the transaction

5: Proof of work(Nonce)

SPV (Simplified Payment Verification) is a method that allows lightweight Bitcoin wallets (like mobile or hardware wallets) to securely verify transactions without downloading the entire blockchain.

Double spent problem

UTXOs: unspent transaction outputs

Bitcoin PDF: https://bitcoin.org/bitcoin.pdf

Bit: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

Second: https://blockchair.com/bitcoin