Blockchain

Blockchain is like a record book that's shared across multiple computers instead of being stored in one place. Every time someone adds new information (like a transaction), it gets bundled with other transactions into a "block." This block is then linked to the previous block using cryptography, creating a chain - hence "blockchain."

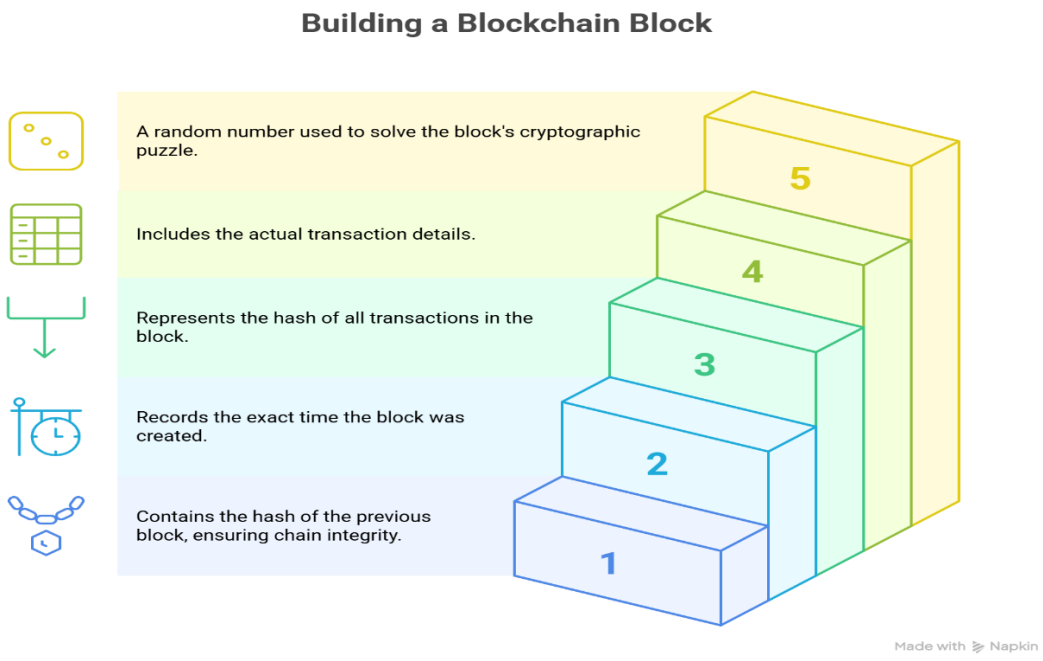
What makes it special is that once something is recorded, it's really hard to change or fake because everyone has a copy of the same records. If someone tries to cheat, the other computers will notice the mismatch. It's like having a group project where everyone keeps their own copy of the work, so no one can secretly edit the shared document without others knowing.

Real life use cases:

Real estate transactions - Instead of dealing with tons of paperwork and middlemen when buying a house, blockchain can store property titles and automate the transfer process. Smart contracts can automatically transfer ownership once payment is confirmed.

Digital identity verification - Some universities are starting to issue digital diplomas on blockchain, making it impossible for people to fake their degrees since employers can verify them directly on the blockchain.

Structure of a Blockchain



Merkel Root

The Merkle root serves as a cryptographic digest that enables efficient verification of data integrity within a block without requiring validation of every individual transaction.

Let's say a block contains 4 transactions:

- Transaction A: "Alice sends 10 units to Bob"
- Transaction B: "Charlie sends 5 units to Dave"
- Transaction C: "Eve sends 20 units to Frank"
- Transaction D: "Grace sends 15 units to Henry"

How it's calculated:

1. Each transaction gets hashed (turned into a unique code)
2. These hashes are paired up and hashed together
3. Keep pairing and hashing until you get one final hash - that's your Merkle root

Verification:

If someone tries to change Transaction B to "Charlie sends 500 units to Dave" instead of 5 units, the hash of that transaction changes. This makes the Merkle root completely different.

When you want to verify the data is unchanged, you just recalculate the Merkle root. If it matches the original, all transactions are intact. If it doesn't match, you know someone tampered with the data.

Consensus Mechanisms:

1. **Proof of Work** (PoW): Proof of Work is like a computational lottery where miners compete to solve complex math puzzles to add the next block to the blockchain. These puzzles require massive amounts of trial-and-error calculations, which is why it consumes so much energy - thousands of computers are running 24/7 trying different solutions. The first miner to solve the puzzle gets to add the block and earn cryptocurrency rewards.
2. **Proof of Stake** (PoS): Proof of Stake selects validators based on how much cryptocurrency they "stake" or lock up as collateral. It's like putting down a security deposit - the more you stake, the higher your chances of being chosen to validate the next block. This uses 99% less energy than Proof of Work because there's no energy-intensive mining competition. If a validator tries to cheat, they lose their staked coins as punishment, which keeps the system honest.

3. **Delegated Proof of Stake** (DPoS): Delegated Proof of Stake is like a representative democracy where coin holders vote for a small number of delegates (usually 21-101) who take turns validating transactions. Instead of everyone participating directly, the community elects trusted validators through voting, where your voting power depends on how many coins you hold. This makes the system much faster since only a few pre-selected validators need to reach consensus, rather than thousands of miners or validators competing simultaneously.