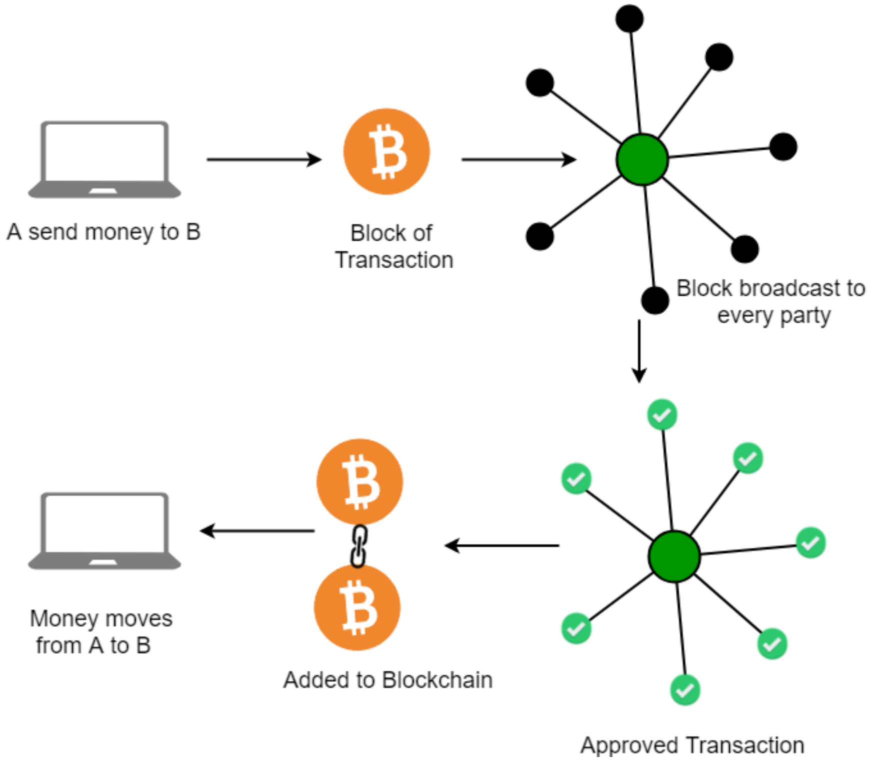
Mini Task 1: Build & Explain a Simple Blockchain

1. Blockchain Basics

Define blockchain in your own words (100–150 words).

Blockchain is like a digital notebook that is shared with many computers around the world. Everyone in the network can see and check this notebook, which makes it very secure and trustworthy. You might have heard of blockchain because it powers **cryptocurrencies** like Bitcoin, where it keeps track of who owns what. But blockchain isn't just for digital money. It can do a lot more! In **supply chains**, it helps track where products come from and where they go. In **healthcare**, it can safely store patient records. In **finance**, it makes sending money or making deals faster and more reliable. The cool part is that no single person controls the blockchain — **it's decentralized.** This means everyone has a copy of the data, and no one can secretly change it. It helps create trust without needing a middleman, like a bank or big company.



- List 2 real-life use cases (e.g., supply chain, digital identity).

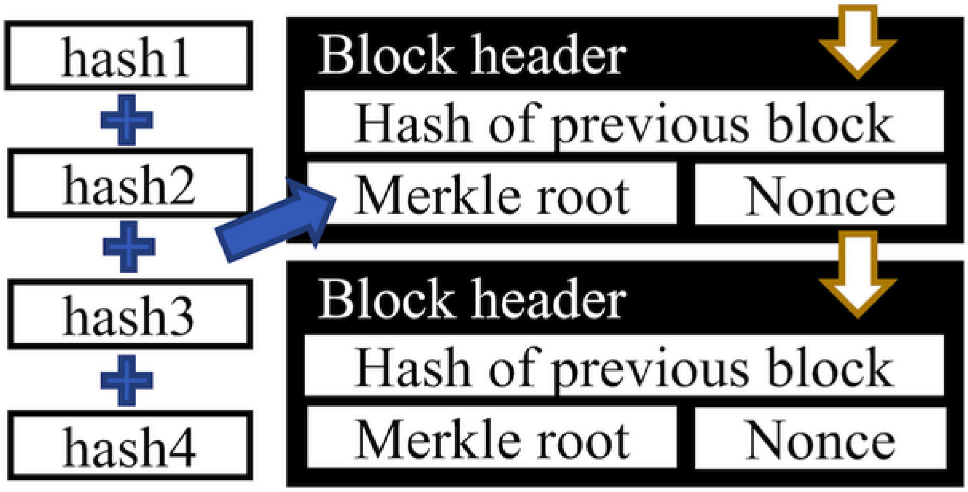
Here are **2 real-life use cases** of blockchain:

1. **Supply Chain Management**
Blockchain helps track products at every stage — from manufacturing to delivery. For example, food companies use blockchain to trace where ingredients come from and ensure freshness. If there's a recall (like contaminated lettuce), they can quickly find the exact source.

2. **Digital Identity**
Blockchain can store secure, tamper-proof digital identities. This allows people to prove who they are online without needing paper documents or centralized databases. It can be used for passports, driver's licenses, or online logins — reducing fraud and making processes faster.

2. Block Anatomy

- Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.



- Briefly explain with an example how the Merkle root helps verify data integrity.

The **Merkle root** helps verify data integrity by summarizing all transactions in a block into a single hash. Even a tiny change in any transaction will change the Merkle root, making tampering easy to detect.

Example:
Imagine a block contains 4 transactions: T1, T2, T3, T4.

1. First, each transaction is hashed: H1, H2, H3, H4.
2. Then, pairs of hashes are combined and hashed again: H12 = hash(H1 + H2), H34 = hash(H3 + H4).
3. Finally, H12 and H34 are combined into the **Merkle root** = hash(H12 + H34).

If someone tries to change T2, H2 will change → H12 will change → Merkle root will change.

This allows quick verification: just compare the stored Merkle root with a newly calculated one. If they match, the data is intact; if not, something was altered.

3. Consensus Conceptualization

1. Explain in brief (4–5 sentences each):

What is Proof of Work and why does it require energy?

What is Proof of Stake and how does it differ?

What is Delegated Proof of Stake and how are validators selected?

- **Proof of Work (PoW)**

  Definition:

  Proof of Work is a method used by some blockchains where computers compete to solve difficult puzzles to confirm transactions and add new blocks. The first one to solve the puzzle gets rewarded, ensuring network security through this competitive work.

  Daily Life Example:

  Imagine a classroom where students race to solve a hard math problem. The first student to finish correctly gets a prize. Because everyone tries hard and uses a lot of energy and time to win, it's like miners in PoW competing with lots of computer power.

- Proof of Stake (PoS)

  Definition:

  Proof of Stake chooses who confirms transactions based on how many coins they own and lock up as a "stake." The more coins you stake, the higher your chance to be picked as a validator, which saves energy compared to PoW.

  Daily Life Example:

  Think of a club where members who have paid more membership fees get a better chance to be chosen as leaders to organize events. They don't have to race or compete hard; their commitment (stake) decides their chance.

- **Delegated Proof of Stake (DPoS)**

Definition:

Delegated Proof of Stake is a system where coin holders vote to elect a small group of trusted people (delegates) to validate transactions and secure the network on their behalf.

Daily Life Example:

It’s like a group of neighbors voting for a few representatives to handle community tasks, such as managing the neighborhood watch. These representatives do the work for everyone, and if they don’t perform well, they can be voted out.