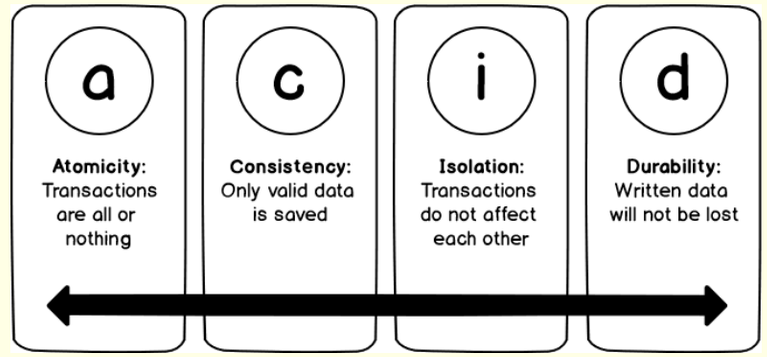
How are transactions entered?

- **Forms** – Used to collect structured data from users, often in digital or paper format. Can include text fields, checkboxes, and dropdowns.
- **OMR (Optical Mark Recognition)** – Scans and detects marks on paper (e.g., multiple-choice exam sheets) to quickly process large amounts of data.
- **OCR (Optical Character Recognition)** – Converts printed or handwritten text into digital format, allowing for text processing and editing.
- **Sensors** – Devices that collect data from the environment (e.g., temperature, motion, light) and convert it into a digital format for processing.
- **Barcodes** – Encoded data stored in a series of lines or squares, scanned by barcode readers for quick identification (e.g., product labels in stores).
- **Data Mining** – The process of analysing large datasets to identify patterns, trends, and useful insights for decision-making.

What is a transaction?
A **transaction** in databases is a sequence of one or more operations (such as inserting, updating, or deleting data) that are executed as a single unit.

A transaction must follow the **ACID** properties to ensure data integrity.



Atomic A transaction should either succeed or fail but never partially succeed.

Consistent: The transaction should only change the database according to the rules of the database.

Isolation Each transaction shouldn't affect/overwrite other transactions concurrently being processed. (**Concurrency**: When multiple transactions are executed simultaneously, they might try to access or modify the same data, leading to inconsistencies)

Record locking can be used to ensure that the ACID principle of isolation is achieved when carrying out multiple transactions. Record locking allows one user/process to access/modify record level data at any one time

Durability Transaction is not lost in case of power / system failure. Completed transactions stored in secondary storage.

Transaction Processing

Data entered must be accurate in the first place.

Data entered should be validated (automatically checked it is sensible) and verified (checked that the data entered matches the original).

Security measures need to be in place to prevent malicious tampering of data.

Record Locking
Records should be locked when in use. If one transaction is amending a record, no other transaction should be able to until the first transaction is complete.

Transactions should maintain **referential integrity.**

Ensuring that changes are consistent across a database. if a record is removed all references to it are removed A foreign key value must have a corresponding Primary key value in another table.

Changes to data in one table must take into account data in linked tables.