Blockchain Basics :

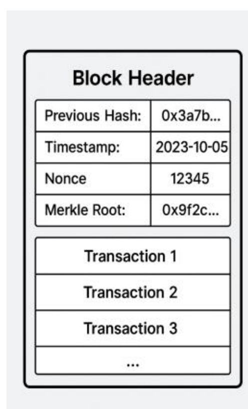
Blockchain is a **decentralized digital ledger** that records transactions across a peer-to-peer network. It stores data in cryptographically linked "blocks," creating an immutable chain. Each block contains verified transactions, a timestamp, and a unique hash. The network relies on **consensus mechanisms** (e.g., Proof of Work/Stake) to validate transactions without central authority. Key features include:

- **Transparency**: All participants view the same data.
- **Immutability**: Tampering alters a block's hash, breaking the chain.
- **Security**: Cryptographic hashing and decentralization prevent fraud. Blockchain enables trustless systems, eliminating intermediaries like banks or governments.

Real-Life Use Cases:

1. **Supply Chain**:
    - **Example**: Walmart tracks produce from farm to store using IBM's blockchain. Each step (harvesting, shipping, storage) is recorded, ensuring freshness and reducing fraud.
2. **Digital Identity**:
    - **Example**: Estonia's e-Residency program issues blockchain-based IDs, allowing secure access to government services, voting, and business registration.

Block Anatomy:



- **Previous Hash**: Cryptographic link to the prior block.
- **Timestamp**: Block creation time.
- **Nonce**: Random number miners adjust to solve the "puzzle."
- **Merkle Root**: Single hash summarizing all transactions.

Merkle Root & Data Integrity Example:

- Transactions are hashed in pairs → combined → rehashed until one root hash remains.
- **Verification**: To check if "Transaction X" is in Block 100, you only need:
    1. Transaction X's hash.
    2. The Merkle path (3–4 adjacent hashes).
- If recalculating the root hash matches Block 100's header, data is untampered. **Why it matters**: No need to download the entire block (e.g., 1 MB in Bitcoin) to verify a single transaction.

Consensus Conceptualization:

Proof of Work (PoW):
PoW requires miners to solve cryptographic puzzles by guessing a nonce to find a valid block hash (e.g., one starting with "0000"). This demands massive computational power, as miners compete in trial-and-error. Energy is needed because:

1. Solving puzzles requires trillions of hash calculations per second.
2. Specialized hardware (ASICs) consumes high electricity.
3. Difficulty adjusts to maintain ~10-minute block times (Bitcoin), escalating energy use.

Proof of Stake (PoS):
PoS selects validators based on their stake (coins locked as collateral). Validators propose blocks, and others attest to their validity. Differences from PoW:

- No mining: Validators don't solve puzzles; chosen algorithmically.
- Energy efficiency: Uses ~99.95% less energy than PoW.
- Security: Malicious validators lose their stake ("slashing").

Delegated Proof of Stake (DPoS):
DPoS is a PoS variant where token holder's elect delegates (e.g., 21 in EOS) to validate blocks. Validator selection:

1. Token holders vote using staked coins (1 coin = 1 vote).
2. Top-voted delegates become block producers.
3. Delegates take turns producing blocks; poor performers are voted out.