Blockchain Basics

A blockchain is a decentralized and immutable digital ledger that records transactions across multiple nodes in a secure and transparent way. Each transaction is grouped into a block ,linked chronologically using cryptographic hashes forming a chain. This structure ensures data integrity as altering one block requires changing all subsequent blocks which is computationally not apt in a distributed network. Blockchains eliminate the need for intermediaries by using consensus mechanisms to validate transactions to ensure trust among participants. They are secure due to cryptographic security and distributed consensus.

Real-Life Use Cases

1) Pharmaceutical Supply Chain
Fake medications cost the industry billions and endanger lives, especially in developing countries. Companies like Modum and IBM Blockchain are helping pharma companies track drugs from manufacturing to distribution using blockchain

2) Many people lack formal identification, making it hard to access healthcare, education, or banking. The ID2020 Alliance uses blockchain to give individuals a self-sovereign digital identity that is secure, portable, and privacy-preserving.

BLOCK:
Index: 1
Timestamp: 2025-06-07 07:40:00
Data: {transaction details}
Previous Hash: 0000abc...
Hash: 0000def...
Nonce: 12345
Merkle Root: 7890ghi...

The Merkle root is a hash of all transaction hashes in a block which is organized in a binary tree. It ensures data integrity by summarizing all transactions into a single hash. EG : if a block contains transactions T1 and T2, their hashes (H1, H2) are paired and hashed together (H12 = SHA256(H1 + H2)) to form the Merkle root. If T1 is altered, H1 changes, causing H12 to mismatch revealing tampering without checking every transaction.

Consensus Mechanisms

Proof of Work (pow): pow requires miners to solve complex mathematical puzzles to validate transactions and add blocks. This process consumes significant computational power and energy due to repeated hashing attempts. It ensures security by making attacks expensive as altering a block requires re-mining all subsequent blocks. EG: Bitcoin uses PoW to secure its network.

Proof of Stake (pos): pos selects validators based on the amount of cryptocurrency they hold and “stake” as collateral. It is more energy efficient compared to pow as no intensive computation is required and validators are chosen probabilistically based on stake size. EG: Ethereum uses PoS to reduce environmental impact.

Delegated Proof of Stake (DPoS): DPoS allows token holders to vote for a small number of delegates who validate transactions. Validators are selected based on the highest vote counts which are often weighted by voters’ stakes. This system is faster and more scalable than PoW or PoS but less decentralized due to reliance on elected delegates.