Blockchain Fundamentals

A Primer on Trust-less, Distributed Ledgers

What Is a Blockchain?

- Distributed, append-only ledger shared across a peer network
- Transactions grouped into timestamped blocks
- Each block hashes the previous one $\rightarrow$ tamper-evident chain
- Security comes from consensus (PoW, PoS, etc.) rather than a central authority
- Anyone can verify the full history independently

Why Blockchain Matters

- Trust minimisation: cryptography $>$ intermediaries
- Immutability: altering one block breaks every subsequent hash
- Transparency: open ledger $=$ audit trail for all participants
- Programmability: smart contracts $=$ self-executing business logic
- Incentives: native tokens reward honest behaviour (miners/validators)

Core Components (Part 1)

- Node: a computer running the protocol, holds a copy of the ledger
- Transaction: signed data package transferring value or invoking code
- Block: data container with header & body

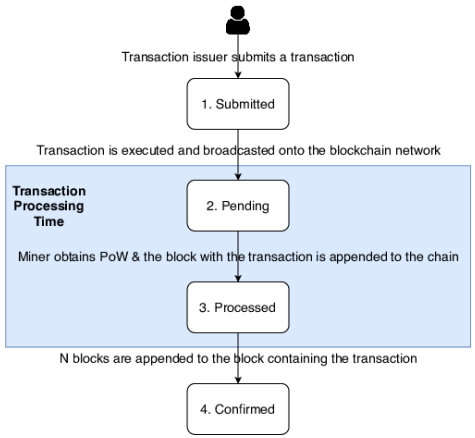

Figure: Transaction Lifecycle: 1. Submitted, 2. Pending, 3. Processed, 4. Confirmed

Core Components (Part 2)

- Consensus Engine: algorithm that decides which block is next

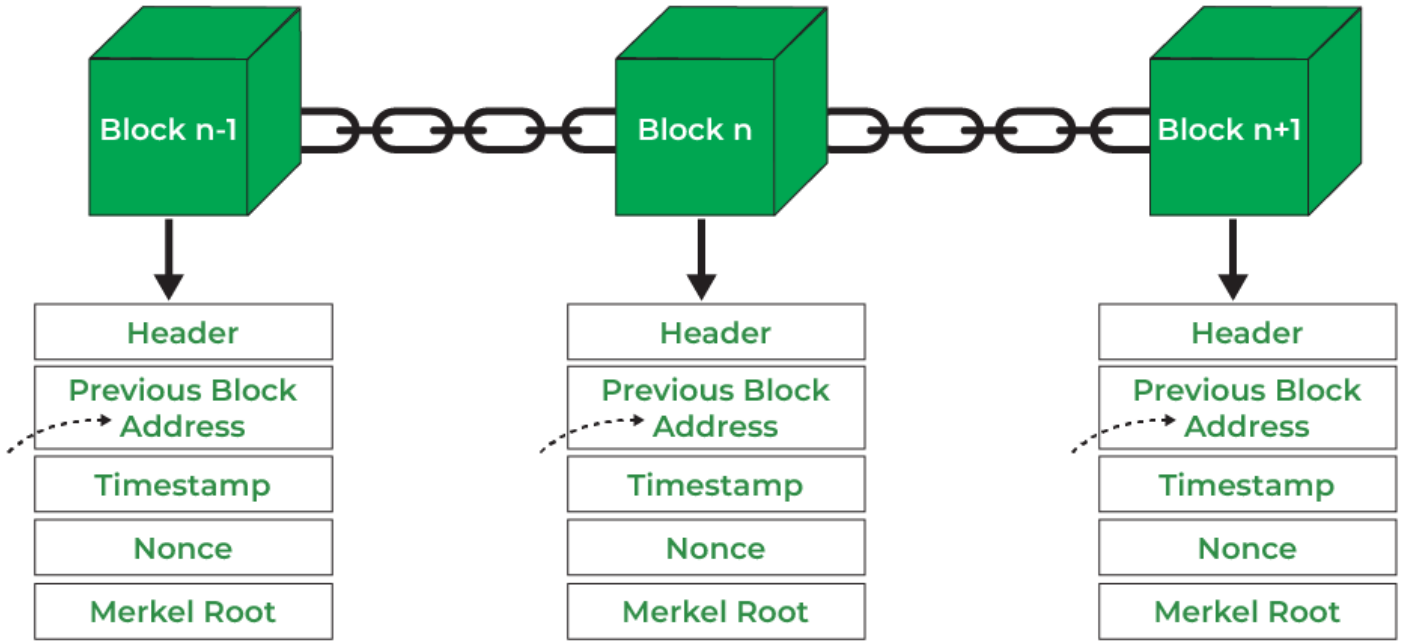

Figure: Block Structure: Block n-1, Block n, Block n+1 with headers (Previous Block Address, Timestamp, Nonce, Merkle Root) and Transaction Data in a Merkle Tree (hashes H1234, H12, H34, T1, T2, T3, T4)

- Peer-to-Peer Network: propagates transactions & blocks

Types of Blockchains (Part 1)

Public Blockchains Open to anyone with an internet connection

- Fully decentralized, no central authority
- Examples: Bitcoin, Ethereum, Solana, Avalanche

Private/Permissioned Blockchains Controlled by a single entity or small group

- Restricted access, often for enterprise use-cases
- Examples: Hyperledger Fabric, R3 Corda, Quorum

Consortium Blockchains Governed by a group of organizations

- Semi-decentralized, shared responsibility
- Examples: Energy Web Chain, Marco Polo Network

Types of Blockchains (Part 2)

Side-Chains Independent blockchains with their own consensus

- Connected to a main chain via bridges
- Examples: Polygon (Ethereum), Ronin (Axie Infinity)

Layer-2 Blockchains (Rollups) Offload computation and state storage to reduce main chain congestion

- Rely on the main chain for finality and security
- Types:
  - Optimistic Rollups (Arbitrum, Optimism) – assume validity, challenge with fraud proofs
  - ZK-Rollups (zkSync, StarkNet) – cryptographic validity proofs for instant finality
- Examples: Polygon zkEVM, Loopring

Plasma Chains Early form of L2 scaling; periodic state commitment to main chain

- Use "child chains" for high-throughput transactions
- Examples: OMG Network (formerly OmiseGo), Polygon Plasma (legacy)

TVL of Top 5 Blockchains (May 2025)

Blockchain	**TVL (USD)**	**Key Use-Cases**
Ethereum	$40B	DeFi, NFTs, DAOs
Binance Smart Chain (BSC)	$16B	DeFi, GameFi
Tron	$9B	Stablecoins, staking
Arbitrum	$7B	Rollups, low-cost DeFi
Optimism	$6B	L2 DeFi, NFTs

Table: Source: DeFiLlama (May 2025)

Key Use-Cases Snapshot

- Payments & remittances (Bitcoin, Lightning)
- Tokenisation of assets (stablecoins, RWA)
- Decentralised finance (DeFi) – lending, AMMs, derivatives
- Supply-chain provenance – track & trace goods
- Digital identity & credentials – verifiable claims