CHAPTER 12

BLOCKCHAIN & FINTECH

Blockchain — the technology behind cryptocurrencies like Bitcoin — offers a **decentralised, secure and transparent** way to record transactions. **Fintech** (financial technology) uses cutting-edge technology to **enhance and automate financial services**. Together they are reshaping **banking, payments, lending, insurance and investment management**.

CHAPTER ROADMAP

1 What is blockchain? — components · features · types · uses
2 Distributed ledger technology — 5 types
3 What is fintech? — 5 areas · benefits

DEFINITION

Blockchain is a decentralised, distributed ledger technology (DLT) that records and verifies transactions across a network of computers in a secure, transparent and immutable manner.

Unlike central-authority databases, it runs on a **peer-to-peer (P2P) network** where each **node** keeps a copy of the ledger → **no intermediaries** (banks, clearinghouses). Recorded data cannot be changed **without approval of most of the network**.

Why the chain is tamper-proof



Each block stores the **hash of the previous block**. Change one block → its hash changes → the **link breaks** for every later block. Rewriting it would need **majority control (51% attack)** and recomputing all later hashes — practically impossible. **Consensus (PoW / PoS)** admits only valid transactions; **decentralisation** removes single points of failure.

1 KEY COMPONENTS OF BLOCKCHAIN

Blocks

Building units = list of transactions. **Header** (metadata: current hash, previous hash, timestamp, **nonce**) + **body** (verified transactions).

e.g. A Bitcoin block with 1,000 transfers.

Hashing

Converts data into a **fixed-size string** — a unique **digital fingerprint**. Does **not alter** the original data; slightest input change → **completely different** hash.

e.g. Altered transaction breaks the link to the next block.

Consensus

Protocols for the network to **agree on the ledger's state**; all nodes hold the same copy; prevents fraud.

PoW & **PoS** — see next page.

Nodes

Computers that **validate & store** the blockchain. **Full nodes** store everything & validate; **lightweight nodes** store part & rely on full nodes.

e.g. Ethereum nodes validate & run smart contracts.

Roles in a Blockchain Network

Nodes	Computers holding a copy; propagate transactions & blocks
Miners	Special nodes solving **mathematical puzzles** to validate & add blocks
Validators	Chosen to propose blocks based on **crypto staked**
Users	Initiate transactions — send / receive digital assets

PROOF OF WORK (PoW)

Miners compete to solve complex puzzles; first to solve adds the block. **High computing power**, high security.

Puzzle: find a **nonce** so the hash meets a strict condition — **hard to solve, easy to verify** (Bitcoin).

vs

PROOF OF STAKE (PoS)

Validators chosen by the number of coins they **hold / stake**. **More energy-efficient**; no expensive hardware.

Stake gives validators a **vested interest** in the network's integrity.

1 KEY FEATURES OF BLOCKCHAIN

Decentralisation
Control spread across the network; every node has a copy. *Bitcoin — no central bank.*

Transparency
Records visible to participants. *Etherscan shows all Ethereum transactions.*

Immutability
Cannot be altered/deleted; tampered version rejected. *Deployed smart contract can't change.*

Security
Public-private keys + hash links; resists **double-spending**. *51% attack unlikely.*

Consensus
All nodes agree before adding transactions. *PoS validators by coins held.*

Types of Blockchains

Type	Who controls / participates	Example
Public	**Open & decentralised** — anyone can join consensus & view; censorship-resistant	Bitcoin, Ethereum
Private	**Permissioned**; one organisation/group; access limited to authorised users	Hyperledger (supply chains, internal data)
Consortium	**Several organisations share control**; semi-decentralised	R3 Corda (interbank settlements)
Hybrid	Mix of public & private — choose **what is public vs private**	Dragonchain

How Blockchain Works — Alice sends 5 BTC to Bob

① **Transaction initiation** — Alice sends 5 BTC
› ② **Broadcast to network** — nodes check Alice has enough BTC
› ③ **Block creation** — grouped into a block, linked by hash
› ④ **Chain propagation** — all nodes update → irreversible

1 USES OF BLOCKCHAIN

trust · transparency · secure data

Beyond cryptocurrencies — valuable wherever **decentralisation, immutability, transparency and security** matter.

Use	What blockchain does	Study-text example
Cryptocurrencies	Decentralised P2P payments, no banks	Bitcoin — global payments, minimal fees
Supply chain	Real-time tracking, authenticity, anti-counterfeit	**Walmart** tracks food farm → store
Smart contracts	**Self-executing** agreements; enforce terms when conditions met	Real estate ownership transfer on payment
Cross-border payments	Fast, low-cost; cuts middlemen	**Ripple (XRP)** instant bank transfers
Healthcare	Unified, tamper-proof patient records	Medicalchain
Voting systems	Secure, transparent, anonymous votes	West Virginia pilot for overseas military
Digital identity	**Self-sovereign identity** — users control their data	Civic
IP protection	Register rights; track use/sale of digital assets	Ascribe.io (digital art)
Real estate	Automate contracts & title transfers	Propy
Energy trading	P2P sale of surplus solar energy	Brooklyn Microgrid
Tokenisation of assets	**Fractional ownership** → more liquidity	$1m property → 1,000 tokens on Ethereum
Insurance	Automated claims; less fraud	Flight delay > 2 hours auto-pays
AML & KYC	Store & verify customer identity across institutions	Shared KYC across branches → faster onboarding

Trade-Based Money Laundering (TBML)

Disguising **illicit funds** by manipulating trade transactions — hard to detect in complex, opaque global trade.
Common techniques:

- **Over/under-invoicing** of goods
- **Multiple invoicing** for the same shipment
- **Phantom shipments** (no goods move)
- **Misrepresentation** of goods or services

How blockchain helps:

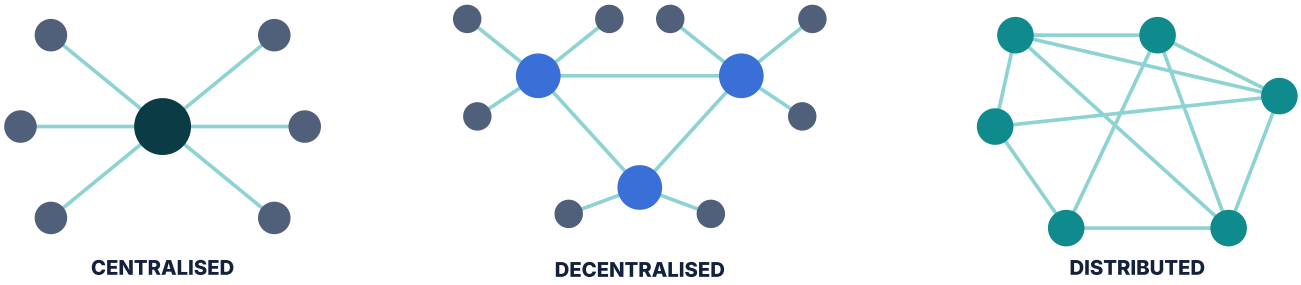
Transparency & immutability
End-to-end traceability **Smart contracts**
Visibility of shipping movements **Shipment tracking**

2 DISTRIBUTED LEDGER TECHNOLOGY (DLT)

DEFINITION

DLT is a digital system for recording asset transactions where data is distributed across multiple locations, not stored on a central server.

No central authority; all participants access the records. **Blockchain is the most well-known form of DLT** — but not the only one.



Centralised = one hub · Decentralised = several hubs · Distributed = every node connected (study-text figure, redrawn)

2.1 Types of DLT

① Blockchain

Transactions grouped into **blocks linked in a chain**; each holds the previous block's hash → immutability.

e.g. Bitcoin — first blockchain cryptocurrency.

② Directed Acyclic Graph (DAG)

Non-linear, graph-like structure; **no mining** → faster, more scalable.

e.g. IOTA's **"Tangle"** for IoT.

③ Hashgraph

Gossip protocol spreads transaction info; consensus by **"virtual voting"** — fast & fair.

e.g. Hedera Hashgraph (dApps).

④ Holochain

Decentralised computing **without consensus mechanisms**; each agent keeps its **own chain** of interactions.

e.g. Decentralised social media, P2P apps.

⑤ Private & Consortium Ledgers

Private = restricted, **one authority**. Consortium = governed by a **group of organisations**.

e.g. R3 Corda (financial institutions).

Remember

Every blockchain is a DLT, but **not every DLT is a blockchain**.

3 WHAT IS FINTECH?

DEFINITION

Fintech (financial technology) refers to the use of advanced technologies in financial services to improve processes, enhance efficiency and elevate customer experience.

Makes financial activities **faster, more accessible, secure and customer-friendly** → a more **inclusive** financial ecosystem. Spans digital payments, P2P lending, robo-advisors, blockchain and **RegTech**.

3.1 Key Areas of Fintech

① Digital Payments
e.g. PayPal

Mobile wallets (Apple/Google/Samsung Pay) — encryption & **tokenisation**. **Cryptocurrencies** — P2P cross-border, enabling **DeFi**. **Contactless** — **NFC** & QR codes.

Benefits: instant, no intermediaries · encrypted · convenient

② Lending & Credit
e.g. LendingClub

P2P lending (LendingClub, Prosper) — borrow directly from individuals/investors, bypassing banks. **Alternative credit scoring** — social media, transaction history, **utility bills**.

Benefits: faster approval · credit for underserved · less reliance on credit scores

③ Wealth Mgmt (Robo-Advisors)
e.g. Betterment, Wealthfront

Automated, algorithm-based advice & portfolios by goals, **risk tolerance**, horizon; auto-rebalancing; **tax-loss harvesting**.

Benefits: lower fees · personalised strategies · automated rebalancing & tax optimisation

④ Insurance (InsurTech)
e.g. Lemonade

AI-driven personalisation (IoT driving data → dynamic pricing); **automated claims** via AI chatbots.

Benefits: faster, accurate claims · real-time personalised policies · better engagement

⑤ RegTech
e.g. ComplyAdvantage

Helps comply with regulations (**AML, KYC**) & manage risk: **compliance automation** · **risk management** (predictive) · **name screening** (sanctions lists, watchlists, **PEPs**, adverse media).

Benefits: lower cost · real-time monitoring · accurate detection

3.2 Benefits of Fintech

- **Improved accessibility** — underserved & remote
- **Enhanced efficiency** — automation
- **Cost reduction** — fewer intermediaries
- **Personalisation** — data analytics & ML
- **Transparency** — real-time balances & history

NAME SCREENING A key RegTech component and a **first line of defence** against financial crime — avoids dealing with sanctioned / high-risk parties and shows **due diligence** to regulators.

EXAM FOCUS · MCQ TRAPS

commonly confused points

1 Hashing doesn't change data
It produces a fingerprint; tiny input change → totally different hash.

2 Header vs body
Header = hashes, timestamp, **nonce**. Body = transactions.

3 PoW vs PoS
PoW = **miners** solve puzzles (energy-heavy). PoS = **validators** by coins staked (energy-efficient).

4 51% attack
Controlling a majority of computational power — needed to alter a public blockchain; highly unlikely.

5 Double-spending
Spending the same crypto twice — prevented by **consensus**.

6 Blockchain types
Hyperledger = **private** · R3 Corda = **consortium** · Dragonchain = **hybrid** · Bitcoin = **public**.

7 DAG & Hashgraph
DAG (IOTA Tangle) = **no mining**. Hashgraph = **gossip protocol + virtual voting**.

8 Holochain
Works **without** consensus mechanisms — each agent has its own chain.

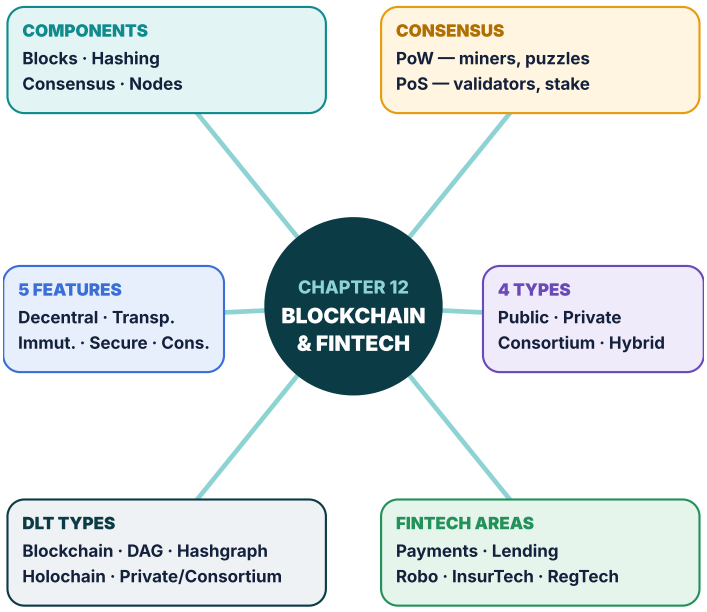
9 Full vs lightweight node
Full = entire chain + validates. Lightweight = part only, relies on full nodes.

10 Fintech area match
Robo-advisors = wealth mgmt · Lemonade = InsurTech · name screening / AML = RegTech.

CLASSIFY IT

1	Find a nonce by trial & error	Proof of Work
2	Validator picked by coins held	Proof of Stake
3	Banks share control of ledger	Consortium
4	IOTA Tangle	DAG
5	Flight-delay payout auto-triggers	Smart contract
6	Fake shipment, no goods moved	TBML — phantom
7	Loan scored on utility bills	Alt. credit scoring
8	Screening a PEP before onboarding	RegTech

REVISION MAP



Blockchain
Decentralised, hash-linked, immutable ledger.

Agree
PoW (work) or PoS (stake) consensus.

Use
Crypto, supply chain, smart contracts, KYC, TBML.

DLT
Blockchain is one type of distributed ledger.

Fintech
Tech making finance faster, cheaper, inclusive.