Foundations of Blockchain Technology

ECOM215: Blockchain Economics and Digital Assets

Dr Daniele Bianchi

Queen Mary, University of London

Semester B, 2025/2026

Today's Agenda

Why Blockchain Matters

What is Blockchain?

Cryptographic Foundations

Core Properties of Blockchain

Use Cases Beyond Cryptocurrency

Summary and Next Steps

Why Blockchain Matters

A Simple Problem: Sending Money Abroad

You want to send £1,000 to a relative in another country.

What happens with traditional banking:

1. Your bank verifies your identity and balance
2. Your bank contacts correspondent banks (often 2–3 intermediaries)
3. Each intermediary verifies the transaction and extracts a fee
4. Settlement takes 2–5 business days
5. Total cost: 5–10% of the transfer amount

The core problem: Each institution maintains its own ledger. Reconciling across ledgers requires **trust**, **time**, and **money**.

The Role of Intermediaries

Most economic transactions rely on **trusted third parties**:

- Banks verify balances and process payments
- Lawyers and notaries certify contracts
- Credit card networks guarantee merchant payments
- Governments maintain registries (land, identity, vehicles)

These intermediaries provide valuable services, but introduce:

Issue	**Example**
Costs	Processing fees, compliance overhead
Delays	Settlement times, reconciliation
Single points of failure	Outages, fraud, insolvency
Exclusion	1.4 billion adults lack bank access

The Blockchain Proposition

What if...

- A single shared ledger recorded all transactions
- Anyone could verify the ledger's accuracy independently
- No single party could control or manipulate records
- Transactions settled in minutes, not days
- The system operated 24/7 without institutional downtime

This is the core idea: replace **trust in institutions** with **trust in a transparent, decentralised system**.

The critical question for this course:
When does this proposition deliver real economic value—and when is it hype?

Blockchain: From Experiment to Infrastructure

Blockchain is no longer "emerging technology." Key milestones:

Year	Development
2009	Bitcoin launches (peer-to-peer electronic cash)
2015	Ethereum introduces programmable smart contracts
2017–20	Enterprise pilots (supply chain, trade finance)
2020–23	DeFi growth, stablecoins reach $100B+
2024	Bitcoin & Ethereum spot ETFs approved (US)
2024	MiCA regulation enters force (EU)

Today: crypto market cap >$2 trillion, institutional custody solutions, regulated investment products, comprehensive legal frameworks.

What is Blockchain?

Blockchain: A Definition

Definition

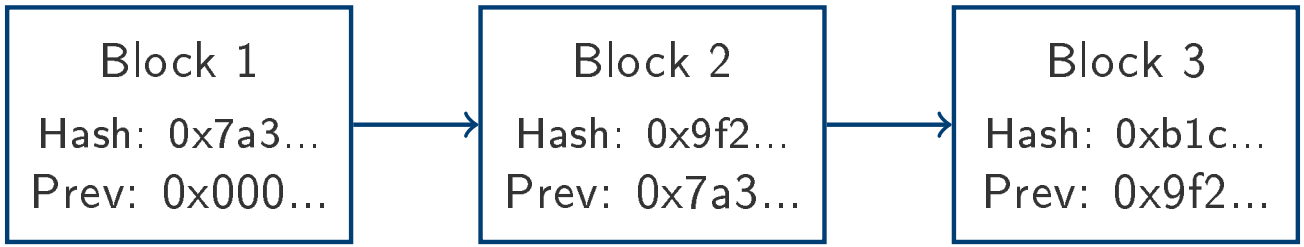
A **blockchain** is a distributed digital ledger that records transactions in linked groups (blocks), secured by cryptography, maintained by a network of computers without central control.

Four foundational components:

1. **Cryptography** — secures data and verifies identity
2. **Data structure** — organises transactions into linked blocks
3. **Distributed network** — replicates ledger across many nodes
4. **Economic incentives** — motivates honest participation

Think of it as a **cleverly designed bookkeeping system** where the bookkeepers don't need to trust each other.

The Chain of Blocks



Key insight: Each block contains the cryptographic "signature" (hash) of the previous block.

- If someone modifies Block 1, its hash changes
- Block 2's "previous hash" no longer matches
- The tampering is immediately detectable

This creates **immutability**: changing history requires rewriting the entire chain.

Key Terminology

Distributed Ledger

An append-only database replicated across many network nodes. New records can be added; existing records cannot be modified or deleted.

Block

A batch of transactions recorded together. Block size and timing vary by blockchain (Ethereum: variable size every 12 seconds).

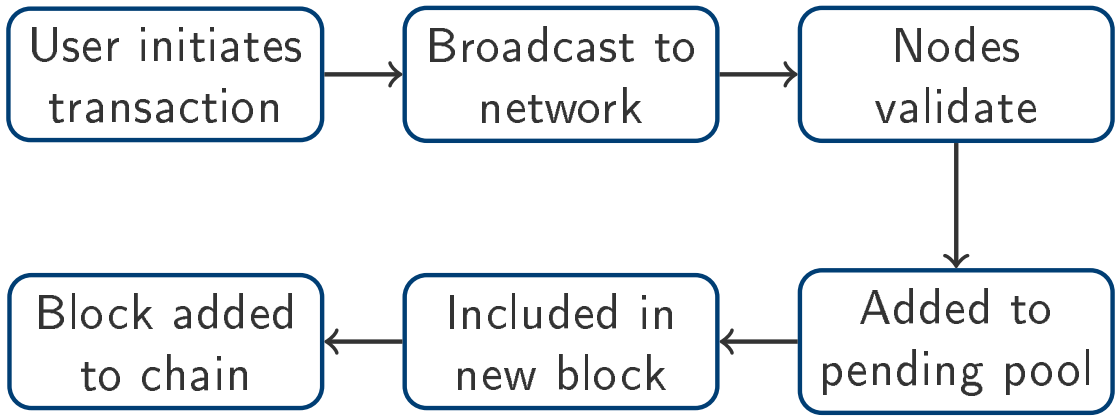
Node

A computer participating in the network. **Full nodes** store the complete ledger and independently validate all transactions. **Light nodes** store only block headers and query full transaction data as needed.

Consensus Protocol

The rules by which nodes agree on ledger updates. Examples: Proof-of-Work, Proof-of-Stake (covered in Topic 2).

How a Transaction Works



Critical points:

- Validation happens *before* recording (integrity)
- Once recorded, transactions cannot be reversed (irreversibility)
- All nodes receive the same updated ledger (transparency)
- No central authority approves transactions (decentralisation)

Cryptographic Foundations

Why Cryptography?

Blockchain relies on cryptographic tools to solve specific problems:

1. **Integrity** — Has the data been tampered with?
   - Hash functions produce a unique "fingerprint" of data
   - Any modification, however small, changes the fingerprint completely
2. **Authentication** — Who authorised this transaction?
   - Digital signatures can only be created with the sender's private key
   - Anyone can verify the signature using the sender's public key
3. **Transparency, not confidentiality**
   - Public blockchains do *not* encrypt transaction data
   - Anyone can see amounts and addresses (pseudonymous, not anonymous)

Hash Functions

Definition

A **hash function** takes input of any size and produces a fixed-length output (the "hash" or "digest"). Small input changes produce completely different outputs.

Example (SHA-256, used by Bitcoin):

```
"Hello" → 185f8db32271fe25f561a6fc938b2e26...
"Hello." → f52fbd32b2b3b86ff88ef6c490628285...
```

Key properties:

- **Deterministic**: Same input always gives same output
- **One-way**: Cannot recover input from output
- **Collision-resistant**: Practically impossible to find two inputs with the same hash
- **Avalanche effect**: Tiny input change $\rightarrow$ completely different hash

Hash Functions in Blockchain

Hashes serve multiple purposes:

1. **Linking blocks**
   - Each block header is hashed to produce a *block hash*
   - This block hash is included in the next block's header
2. **Identifying transactions**
   - Each transaction is hashed to produce a *transaction ID*
   - All transaction hashes in a block are combined into a *Merkle tree*
   - The Merkle root is included in the block header—so the block hash commits to every transaction
3. **Proof-of-Work** (Topic 2)
   - Miners must find inputs that produce hashes meeting specific criteria

Public-Key Cryptography

The Problem

How can two parties communicate securely without first meeting to share a secret key?

Solution: Asymmetric encryption
Each user has a **key pair**:

- **Public key**: Shared openly (like an email address)
- **Private key**: Kept secret (like a password)

Two uses:

Operation	Encrypt with	Decrypt with
Sending private message	Recipient's public key	Recipient's private key
Signing a transaction	Sender's private key	Sender's public key

Digital Signatures in Blockchain

When you send cryptocurrency:

1. You create a transaction message ("send 1 BTC to address X")
2. You sign it with your **private key**
3. The network verifies the signature using your **public key**

What this guarantees:

- **Authentication**: Only the private key holder could have signed
- **Integrity**: Any modification invalidates the signature
- **Non-repudiation**: Signer cannot deny the transaction

Critical implication:
If you lose your private key, you lose access to your assets.
If someone steals your private key, they control your assets.
There is no "forgot password" reset. This is a feature, not a bug.

Core Properties of Blockchain

The Five Properties

Different blockchains achieve these properties to different degrees:

1. **Immutability**: Recorded transactions cannot be altered
2. **Irreversibility**: Confirmed transactions cannot be undone
3. **Integrity**: Only valid transactions are recorded
4. **Transparency**: Transaction history is publicly auditable
5. **Decentralisation**: No single point of control or failure

The Blockchain Trilemma (Topic 2)

It is difficult to simultaneously maximise **decentralisation**, **security**, and **scalability**. Design choices involve trade-offs.

Immutability and Irreversibility

Immutability: The ledger's history cannot be rewritten.

- Guaranteed by hash-linking of blocks
- Changing old data requires re-mining all subsequent blocks
- Economically prohibitive on large networks

Irreversibility: Transactions cannot be "undone."

- Critical for preventing double-spending
- If you send funds to the wrong address, there is no reversal mechanism
- Contrast with credit cards (chargebacks) or bank transfers (recalls)

Implication: Blockchain is well-suited for situations where finality is valuable (settlement, proof of existence) but creates challenges for error correction.

Transparency and Decentralisation

Transparency: All transactions are visible to all participants.

- Anyone can audit the complete transaction history
- Builds trust without requiring trust in any single party
- Privacy trade-off: Pseudonymous, not anonymous

Decentralisation: No central authority controls the network.

- Thousands of independent nodes maintain the ledger
- No single point of failure or censorship
- Decisions made through protocol rules and consensus

Key insight: These properties are *emergent*—they arise from the system design, not from any guarantee by a trusted party. The system is only as robust as its weakest design assumption.

Public vs Private vs Consortium

We can distinguish different types of blockchains.

	Public	**Consortium**	**Private**
Access	Open to all	Invited orgs	Single org
Consensus	Permissionless	Pre-selected nodes	Centralised
Speed	Slower	Medium	Fastest
Decentralisation	High	Medium	Low
Examples	Bitcoin, Ethereum	R3 Corda, Hyperledger	Internal DBs

The trade-off:

- Public chains maximise trust minimisation but sacrifice throughput
- Private chains maximise efficiency but require trusting the operator
- Consortium chains attempt a middle ground

Public Blockchains

Definition: Open networks where anyone can participate, validate, and audit.

Examples: Bitcoin, Ethereum, Solana

Advantages:

- Maximum decentralisation and censorship resistance
- Trustless: security from protocol, not institutions
- Permissionless innovation: anyone can build on top

Disadvantages:

- Scalability constraints (throughput, latency)
- Energy consumption (Proof-of-Work) or capital requirements (Proof-of-Stake)
- Governance challenges for protocol upgrades

Note: Layer 2 solutions (Topic 2) address scalability by processing transactions off the main chain while inheriting its security.

Private and Consortium Blockchains

Private blockchain: Controlled by a single organisation.

- Fast and efficient (fewer nodes, simpler consensus)
- Full control over access and governance
- But: Requires trusting the operator—arguably "just a database"

Consortium blockchain: Controlled by a group of organisations.

- Shared infrastructure without full public exposure
- Useful when multiple parties need a common record but don't fully trust each other
- Examples: Trade finance (we.trade), securities settlement (DTCC)

When do these make sense?
When you need auditability and coordination across organisations, but public transparency is undesirable or regulatory constraints apply.

Use Cases Beyond Cryptocurrency

Where Blockchain Adds Value

Blockchain is most useful when:

- Multiple parties need a **shared record**
- Those parties don't fully **trust each other**
- A trusted intermediary is **costly, slow, or unavailable**
- **Auditability** and **tamper-evidence** are valuable

Blockchain is *not* useful when:

- A single organisation controls all data
- Participants already trust each other
- Speed is critical and finality can wait
- Data needs to be frequently modified or deleted

Rule of thumb: If a traditional database solves the problem, use a database. Blockchain adds value through trust minimisation, not raw performance.

Supply Chain Management

Problem: Tracking goods across multiple parties (manufacturers, shippers, customs, retailers) with no single trusted record-keeper.

Blockchain solution:

- Shared ledger records provenance and chain of custody
- Each handoff is cryptographically signed
- Smart contracts can automate payments upon delivery confirmation

Examples:

- IBM Food Trust: Walmart traces produce from farm to shelf
- TradeLens (Maersk + IBM): Container shipping documentation
- De Beers (Tracr): Diamond provenance verification

Limitation: Blockchain guarantees data integrity *on-chain*, but cannot verify that off-chain inputs are accurate ("garbage in, garbage out").

Financial Services

Settlement and clearing:

- Traditional securities settlement: T+2 (trade date + 2 days)
- Blockchain-based settlement: potentially near-instant
- Reduces counterparty risk and capital requirements

Trade finance:

- Letters of credit, bills of lading still largely paper-based
- Consortium blockchains digitise and automate documentation

Cross-border payments:

- Correspondent banking is slow and expensive
- Stablecoins and CBDCs offer alternatives (Topics 4–5)

We will cover these in depth: DeFi (Topic 4), Stablecoins and CBDCs (Topic 5), Tokenisation of real-world assets (Topic 9).

Identity and Government Services

Digital identity:

- Self-sovereign identity: users control their own credentials
- Verifiable credentials without revealing underlying data
- Estonia's e-Residency programme uses blockchain-backed identity

Land registries:

- Immutable record of property ownership
- Reduces fraud and disputes in developing economies
- Georgia, Sweden, Dubai have piloted blockchain registries

Voting:

- Transparent, auditable vote records
- Significant security and privacy challenges remain
- Corporate shareholder voting more tractable than political elections

Summary and Next Steps

Key Takeaways

1. **Blockchain enables coordination without trusted intermediaries**
   - Useful when multiple parties need shared, tamper-evident records
2. **Core mechanism: cryptographically linked blocks**
   - Hash functions ensure integrity; digital signatures ensure authenticity
3. **Key properties: immutability, transparency, decentralisation**
   - But there are trade-offs (the blockchain trilemma)
4. **Different blockchains serve different purposes**
   - Public (trust minimisation) vs private/consortium (efficiency)
5. **Use cases extend beyond cryptocurrency**
   - Supply chain, financial settlement, identity, governance

What's Next

Topic 2: Blockchain Economics

- Consensus mechanisms: Proof-of-Work vs Proof-of-Stake
- The blockchain trilemma: decentralisation, security, scalability
- Economic incentives: mining, staking, fee markets
- Energy consumption and environmental concerns

Preparation:

- Review: What problem does consensus solve in a decentralised network?
- Think about: What incentives would motivate strangers to honestly maintain a shared ledger?

Questions?