Blockchain Economics and Digital Assets

Lecture 1: Foundations of Blockchain Technology

Dr Daniele Bianchi

Queen Mary, University of London

Semester B, 2025/2026

Contents

Overview

This lecture introduces the fundamental concepts of blockchain technology and sets the stage for understanding its economic implications. We begin by asking a simple question: why does blockchain matter? The answer lies in a fundamental problem that has shaped economic activity for millennia—the problem of trust.

Every day, we engage in transactions that require trusting strangers. When you send money abroad, you trust banks to transfer it correctly. When you buy something online, you trust payment processors to handle the transaction honestly. When you sign a contract, you trust legal systems to enforce it. These trusted intermediaries—banks, lawyers, notaries, governments—form the invisible infrastructure of modern commerce.

Blockchain proposes something radical: a system where this trust is not placed in institutions, but in a transparent, cryptographically-secured, decentralised network. Whether this proposition delivers genuine economic value, or merely shifts trust from one place to another, is the central question of this course.

This lecture is organised as follows. We first examine why intermediaries exist and what problems they create. We then define blockchain precisely and explore its core components: cryptographic building blocks, the chain-of-blocks data structure, and the distributed network that maintains it. Finally, we examine different types of blockchains and survey use cases beyond cryptocurrency.

1 Why Blockchain Matters

1.1 The Problem of Trust in Economic Exchange

Consider a simple problem: you want to send £1,000 to a relative in another country. What happens when you initiate this transfer through traditional banking?

Your bank first verifies your identity and checks your balance. It then contacts one or more correspondent banks—intermediaries that facilitate cross-border transactions. Each intermediary verifies the transaction, updates its own ledger, and extracts a fee for its services. The entire process typically takes two to five business days and costs between 5% and 10% of the transfer amount.

This inefficiency stems from a fundamental issue: each institution maintains its own private ledger, and reconciling information across these ledgers requires trust, time, and money. Your bank does not know the balance at the recipient's bank; correspondent banks do not know whether either party is creditworthy; everyone must trust everyone else to record transactions honestly.

This is not unique to international transfers. Most economic transactions rely on **trusted third parties** to function:

Intermediary	Function
Banks	Verify balances, process payments
Credit card networks	Guarantee merchant payments
Lawyers and notaries	Certify contracts
Governments	Maintain registries (land, identity, vehicles)

These intermediaries provide genuine value, but they also introduce costs: processing fees, compliance overhead, settlement delays, and the potential for single points of failure. Roughly 1.4 billion adults worldwide lack access to banking services entirely, excluded from formal economic participation.

1.2 The Blockchain Proposition

Blockchain offers an alternative architecture. What if a single shared ledger recorded all transactions? What if anyone could verify that ledger's accuracy independently, without trusting any particular institution? What if no single party could control or manipulate the records? What if transactions settled in minutes rather than days, and the system operated continuously without institutional downtime?

This is the core idea: replace **trust in institutions** with **trust in a transparent, decentralised system**. The question we will explore throughout this course is when this proposition delivers real economic value—and when it is merely hype.

1.3 From Experiment to Infrastructure

Blockchain is no longer an emerging technology confined to enthusiasts. Since Bitcoin's launch in 2009, the technology has matured considerably:

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

Today, the cryptocurrency market exceeds $2 trillion in capitalisation. Major financial institutions offer custody solutions. Regulated investment products trade on traditional exchanges. Comprehensive legal frameworks govern digital assets in major jurisdictions. Whatever one thinks of cryptocurrencies as investments, the underlying technology has achieved a level of institutional acceptance that was unthinkable a decade ago.

2 What is Blockchain?

2.1 A Precise 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.

This definition contains four foundational components that we will examine in turn:

1. **Cryptography**: Secures data and verifies identity
2. **Data structure**: Organises transactions into linked blocks
3. **Distributed network**: Replicates the ledger across many nodes
4. **Economic incentives**: Motivates honest participation

Think of blockchain as a cleverly designed bookkeeping system where the bookkeepers do not need to trust each other. The "cleverness" lies in combining existing technologies—cryptographic hash functions, digital signatures, peer-to-peer networks—in a way that creates new properties none could achieve alone.

2.2 The Chain of Blocks

The name "blockchain" describes its fundamental data structure. Transactions are grouped into *blocks*, and each block contains a cryptographic link to the previous block, forming a chain.

More precisely, each block contains:

- A batch of transactions
- A timestamp
- The *hash* of the previous block (a cryptographic fingerprint)
- Its own hash (computed from all the above)

The critical property is that each block's hash depends on the previous block's hash. If someone attempts to modify an old transaction, the hash of that block changes. But this invalidates the reference in the next block, changing its hash as well. The tampering propagates forward, making any modification immediately detectable.

This creates **immutability**: changing the historical record requires rewriting the entire chain from the point of modification forward. As we shall see in Topic 2, this becomes computationally prohibitive on large networks.

2.3 Key Terminology

Several terms recur throughout discussions of blockchain:

A **distributed ledger** is an append-only database replicated across many network nodes. New records can be added, but existing records cannot be modified or deleted. A blockchain is one type of distributed ledger, distinguished by its block-based structure and cryptographic linking.

A **block** is a batch of transactions recorded together. Block size and timing vary by blockchain. Ethereum, for instance, produces blocks of variable size approximately every 12 seconds.

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

A **consensus protocol** defines the rules by which nodes agree on which blocks to add to the chain. Different consensus mechanisms—Proof-of-Work, Proof-of-Stake, and others—represent different approaches to this coordination problem. We examine these in detail in Topic 2.

2.4 How a Transaction Works

When a user initiates a blockchain transaction, the following sequence occurs:

1. The user creates and cryptographically signs a transaction (e.g., "send 1 ETH to address X")
2. The transaction is broadcast to the network
3. Nodes validate the transaction (checking signatures, balances, and format)
4. Valid transactions enter a "pending pool" (mempool)
5. A block producer includes the transaction in a new block
6. Other nodes verify and append the block to their copy of the chain

Several properties emerge from this process. *Validation happens before recording*, ensuring only legitimate transactions enter the ledger. *Once recorded, transactions cannot be reversed*—there is no "undo" button. *All nodes receive the same updated ledger*, creating transparency. And *no central authority approves transactions*; the network reaches consensus through its protocol rules.

3 Cryptographic Foundations

Blockchain relies on cryptographic tools to solve specific problems: ensuring data integrity, authenticating transaction authors, and linking blocks securely. Understanding these tools is essential for grasping both blockchain's capabilities and its limitations.

3.1 Hash Functions

A **hash function** takes input of any size and produces a fixed-length output called a *hash* or *digest*. Bitcoin uses SHA-256, which produces 256-bit outputs regardless of input length. Small input changes produce completely different outputs:

```
SHA-256("Hello")  → 185f8db32271fe25f561a6fc938b2e26...
SHA-256("Hello.") → f52fbd32b2b3b86ff88ef6c490628285...
```

A single character change—adding a period—transforms the hash entirely. This is the **avalanche effect**.

Cryptographic hash functions have several crucial properties:

- **Deterministic**: The same input always produces the same output
- **One-way**: Given a hash, you cannot recover the input (computationally infeasible)
- **Collision-resistant**: It is practically impossible to find two different inputs that produce the same hash
- **Avalanche effect**: Tiny input changes produce completely different hashes

In blockchain, hashes serve multiple purposes. Each block header is hashed to produce a *block hash*, which is then included in the next block's header—this is how blocks are cryptographically linked. Each transaction is hashed to produce a unique *transaction ID*. All transaction hashes in a block are combined into a *Merkle tree*, whose root is included in the block header, committing the block to every transaction it contains.

3.2 Public-Key Cryptography

Traditional cryptography requires parties to share a secret key before communicating securely. **Public-key cryptography** solves this with asymmetric key pairs.

Each user generates two mathematically related keys:

- A **public key**: Shared openly, like an email address
- A **private key**: Kept secret, like a password

These keys enable two operations:

Operation	Use with	Verify/Decrypt with
Encryption	Recipient's public key	Recipient's private key
Signing	Sender's private key	Sender's public key

3.3 Digital Signatures in Blockchain

When you send cryptocurrency, you create a transaction message ("send 1 BTC to address X") and sign it with your private key. The network verifies this signature using your public key.

This provides three guarantees:

- **Authentication**: Only the private key holder could have created the signature
- **Integrity**: Any modification to the transaction invalidates the signature
- **Non-repudiation**: The signer cannot later deny having authorised the transaction

The critical implication is that private keys are the sole proof of ownership. If you lose your private key, you lose access to your assets permanently. If someone steals your private key, they control your assets completely. There is no "forgot password" mechanism, no customer service to call, no way to reverse fraudulent transactions. This is a feature of the system, not a bug—but it represents a fundamental shift in how we think about asset security.

4 Core Properties of Blockchain

Different blockchains achieve these properties to varying degrees, but the following represent the ideals the technology aspires to:

4.1 Immutability and Irreversibility

Immutability means the ledger's history cannot be rewritten. Hash-linking ensures that changing any historical data requires re-computing all subsequent block hashes. On large networks with substantial computational resources devoted to maintaining the chain, this becomes economically prohibitive.

Irreversibility means confirmed transactions cannot be "undone." Unlike credit card payments (which allow chargebacks) or bank transfers (which can sometimes be recalled), blockchain transactions are final. This is valuable for settlement finality but creates challenges when errors occur. If you send funds to the wrong address, no mechanism exists to reverse the transfer.

4.2 Transparency and Decentralisation

Transparency means all transactions are visible to all participants. Anyone can audit the complete transaction history of a public blockchain. This builds trust without requiring trust in any particular party—you can verify rather than trust.

The privacy trade-off is significant: public blockchains are *pseudonymous*, not anonymous. Transactions are linked to addresses (public keys), not legal identities. But once an address is linked to a real identity—through an exchange, a payment, or data analysis—all associated transactions become attributable.

Decentralisation means no single party controls the network. Thousands of independent nodes maintain the ledger, with decisions made through protocol rules and consensus rather than central authority. This eliminates single points of failure and censorship, but introduces coordination challenges for upgrades and dispute resolution.

4.3 The Blockchain Trilemma

These properties exist in tension. Vitalik Buterin, Ethereum's co-founder, articulated this as the **blockchain trilemma**: a blockchain can optimise for at most two of three properties—decentralisation, security, and scalability.

More decentralised networks (with more nodes validating transactions) achieve greater censorship resistance but slower throughput due to communication overhead. Higher security (requiring more computational work or economic stake) provides stronger guarantees against attacks but consumes more resources. Greater scalability (processing more transactions per second) typically requires either larger blocks (which price out smaller validators) or fewer validators (which reduces decentralisation).

We will examine this trilemma in depth in Topic 2, along with Layer 2 solutions that attempt to work around these constraints.

5 Types of Blockchains

Not all blockchains are created equal. They differ fundamentally in who can participate, who validates transactions, and what trade-offs they accept.

5.1 Public Blockchains

Public blockchains are open networks where anyone can participate, validate transactions, and audit the ledger. Bitcoin and Ethereum are the primary examples.

Advantages:

- Maximum decentralisation and censorship resistance
- Trustless operation: security derives from the protocol, not institutional reputation
- Permissionless innovation: anyone can build applications on top

Disadvantages:

- Scalability constraints (Bitcoin processes roughly 7 transactions per second)
- Resource consumption (Proof-of-Work) or capital requirements (Proof-of-Stake)
- Governance challenges when protocol changes are needed

5.2 Private and Consortium Blockchains

Private blockchains are controlled by a single organisation. They offer speed and efficiency—fewer nodes mean simpler consensus—but require trusting the operator. Critics argue that a private blockchain is "just a database" since it lacks the trust-minimisation properties that make public blockchains distinctive.

Consortium blockchains are controlled by a group of organisations. They represent a middle ground: shared infrastructure without full public exposure. Examples include R3 Corda for financial services and Hyperledger Fabric for enterprise applications.

	Public	**Consortium**	**Private**
Access	Open to all	Invited organisations	Single organisation
Consensus	Permissionless	Pre-selected nodes	Centralised
Speed	Slower	Medium	Fastest
Decentralisation	High	Medium	Low
Trust model	Protocol	Consortium members	Operator

The choice depends on the use case. Public chains maximise trust minimisation but sacrifice throughput. Private chains maximise efficiency but require trusting the operator. Consortium

chains attempt a middle ground suitable for scenarios where multiple parties need coordination but full public transparency is undesirable.

6 Use Cases Beyond Cryptocurrency

6.1 When Does Blockchain Add Value?

Blockchain is most useful when:

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

Conversely, blockchain adds little value 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

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

6.2 Supply Chain Management

Supply chains involve tracking goods across multiple parties—manufacturers, shippers, customs officials, retailers—with no single trusted record-keeper. Blockchain can provide a shared ledger recording provenance and chain of custody, with each handoff cryptographically signed.

Examples include IBM Food Trust (Walmart tracing produce from farm to shelf), TradeLens (container shipping documentation), and De Beers' Tracr platform (diamond provenance verification).

The limitation is significant: blockchain guarantees data integrity *on-chain* but cannot verify that off-chain inputs are accurate. If someone falsely records that goods were inspected, the blockchain dutifully preserves this false record. The principle of "garbage in, garbage out" applies—immutably.

6.3 Financial Services

Several financial applications benefit from blockchain's properties:

Settlement and clearing: Traditional securities settlement operates on T+2 (trade date plus two days). Blockchain-based settlement could be near-instant, reducing counterparty risk and capital requirements.

Trade finance: Letters of credit and bills of lading remain largely paper-based. Consortium blockchains can digitise and automate this documentation.

Cross-border payments: Correspondent banking is slow and expensive. Stablecoins and central bank digital currencies offer alternatives, which we examine in Topic 5.

6.4 Identity and Government Services

Blockchain enables new approaches to digital identity. *Self-sovereign identity* allows users to control their own credentials without relying on centralised identity providers. Verifiable credentials can be shared without revealing underlying data—proving you are over 18 without revealing your birthdate, for instance.

Land registries benefit from immutable records of property ownership, reducing fraud and disputes. Georgia, Sweden, and Dubai have piloted blockchain-based property registries, particularly valuable in jurisdictions with unreliable traditional record-keeping.

Voting applications remain more speculative. While transparent, auditable vote records are appealing, significant security and privacy challenges remain. Corporate shareholder voting may be more tractable than political elections, where the stakes and attack surfaces are higher.

7 Summary and Looking Ahead

This lecture has covered substantial ground. The key takeaways are:

Blockchain enables coordination without trusted intermediaries. Its value proposition is clearest when multiple parties need shared, tamper-evident records and no single party can be trusted to maintain them.

The core mechanism is cryptographically linked blocks. Hash functions ensure integrity; digital signatures ensure authenticity; the chain structure ensures that historical modifications are detectable.

Key properties are immutability, transparency, and decentralisation. But these exist in tension with each other and with scalability—the blockchain trilemma.

Different blockchains serve different purposes. Public chains maximise trust minimisation; private and consortium chains trade decentralisation for efficiency.

Use cases extend beyond cryptocurrency. Supply chain, financial settlement, identity, and governance all represent potential applications—though the "oracle problem" (verifying off-chain data) limits what blockchain can guarantee.

In the next lecture, we turn to the economics of blockchain: how consensus mechanisms work, why they consume resources, and what trade-offs different approaches embody. We will examine Proof-of-Work and Proof-of-Stake in detail, understand the blockchain trilemma more precisely, and explore how Layer 2 solutions attempt to circumvent scalability constraints.

Readings

Required:

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Read Sections 1–5 for the original articulation of blockchain's core concepts.

Supplementary:

- Catalini, C., & Gans, J. S. (2020). "Some Simple Economics of the Blockchain." *Communications of the ACM*, 63(7), 80–90. An accessible economic perspective on blockchain's value proposition.

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press. Chapters 1–2 provide excellent technical background.