Introduction to Blockchain

A Five-Minute Overview

BSc Blockchain Course

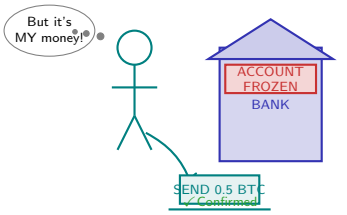
Why Would Anyone Trust a Network of Strangers with Their Money?

Throughout history, keeping money safe meant handing it to an institution you hoped would still exist tomorrow. Banks have frozen accounts during crises, governments have blocked cross-border transfers, and payment processors have cut off entire communities at a stroke. **Three recurring**

problems:

- **Frozen accounts** – your money, someone else's permission
- **Censored transactions** – a transfer blocked with no appeal
- **Single point of failure** – one institution, one outage, everyone loses

What if the network itself was the bank – with no one in charge?



Blockchain does not eliminate trust – it redistributes it from a single institution to a network of thousands of independent participants.

Source: Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." bitcoin.org/bitcoin.pdf

What Makes Blockchain Different from Every Other Database?

Four types of data store – four different trust models:

Property	Traditional Database	Cloud Database	Distributed Database	Blockchain
Control	One owner	One provider	Multiple owners	No single owner
Mutability	Editable	Editable	Editable	Append-only
Transparency	Private	Private	Partial	Fully public
Trust model	Trust operator	Trust provider	Trust admins	Trust protocol
Example	Bank ledger	Google Sheets	Airline booking	Bitcoin ledger

Pattern to notice:

Read across the rows from left to right. Control disperses with every step. Transparency increases with every step. By the time you reach blockchain, no single actor can edit history – and anyone can verify the full record. The trade-off is speed: a blockchain sacrifices throughput to achieve the last two properties simultaneously.

The key question each system answers:

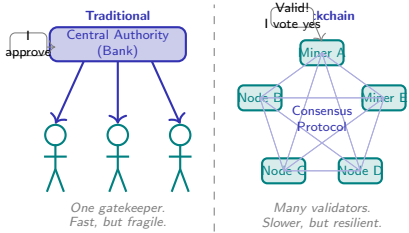
- **Traditional DB:** "Who manages this server?"
  You trust that person or organisation.
- **Cloud DB:** "Which company hosts this?"
  You trust their uptime and honesty.
- **Distributed DB:** "Who runs each node?"
  You trust the consortium agreement.
- **Blockchain:** "Is the protocol correct?"
  You trust mathematics and open-source code – verifiable by anyone.

Only blockchain makes "Trust, but verify" a literal property of the system.

A blockchain is the only database where the rules of record-keeping are enforced by the network itself – not by the organisation that created it.

Source: Buterin, V. (2014). "A Next-Generation Smart Contract and Decentralized Application Platform." ethereum.org/whitepaper

Who Validates Your Transaction – A Bank, A Miner, or the Crowd?



How consensus replaces central authority: In a traditional system, one institution holds the ledger and decides which transactions are valid. Fail that institution, and transactions stop. In a blockchain, hundreds or thousands of independent nodes each hold a full copy of the ledger. A transaction is accepted only when a majority of nodes agree it follows the rules. **What this changes:**

- No single node can forge or erase a record
- Removing one node does not stop the network
- Anyone may inspect the complete transaction history
- The rules are encoded in software, not in a contract with one company

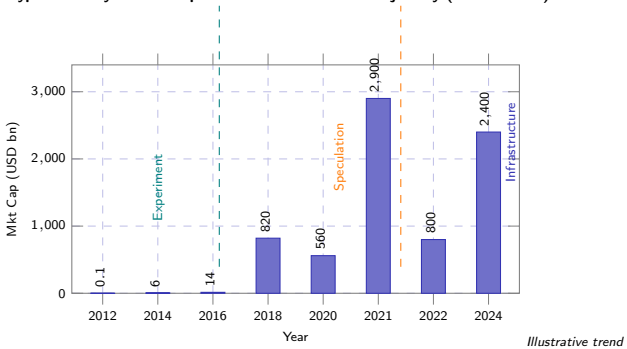
The crowd is the bank. The protocol is the rulebook.

Consensus is the mechanism by which strangers who do not trust each other can nonetheless agree on a shared truth – without a referee.

Source: Antonopoulos, A.M. (2017). Mastering Bitcoin, 2nd ed. O'Reilly. Chapter 10: Mining and Consensus.

Why Has the Crypto Market Grown from Zero to Three Trillion Dollars?

Cryptocurrency market capitalisation – illustrative trajectory (USD billions):



based on published market data. Log growth compressed to linear for readability.

Three eras of growth:

- **Experiment (to 2016):**
  A handful of developers building on the idea that digital scarcity was possible. Market cap measured in millions – ignored by mainstream finance.
- **Speculation (2017–2020):**
  Retail investors piled in on narratives. Prices ran far ahead of utility. Inevitable corrections followed. The infrastructure, however, kept building.
- **Infrastructure (2020–present):**
  Institutional portfolios, regulated exchanges, stablecoin payment rails, and central-bank digital currency research. Blockchain moved from hobbyist experiment to financial-system component.
- **The underlying driver:**
  Each wave brought developers, capital, and users who stayed after the speculation cooled – compounding the network effects each time.

Markets over-price blockchain in the short run and under-price the infrastructure it leaves behind in the long run.

Source: Illustrative trend based on CoinMarketCap historical data (coinmarketcap.com) and IMF Global Financial Stability Reports 2022–2024.

Three Questions That Reveal Whether a System Truly Needs Blockchain

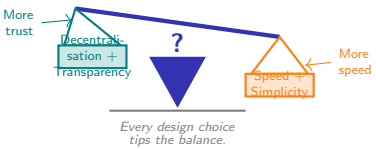
Before choosing blockchain, ask these three questions in order: **Q1 – Do**

multiple parties need to write the same record,
and do they distrust each other?
If a single organisation controls all writes, a conventional database is cheaper and faster. Blockchain earns its cost only when *no one* should have sole control. **Q2 – Must the history be auditable by**

outsiders
without relying on the system operator?
If the answer is yes – regulators, customers, or counterparties need independent verification – blockchain's public ledger is a genuine advantage. Opaque databases offer no such guarantee. **Q3 – Can the**

parties tolerate the trade-offs?
Blockchain is slower than a centralised database, uses more energy per transaction, and makes mistakes permanent (or very costly to reverse). If speed or easy correction matters more than decentralisation, choose a simpler tool. *If you answered YES, YES, YES – you have a genuine use case.*

If not – a shared spreadsheet may serve you better.



The

Blockchain Trilemma (simplified):
No system simultaneously maximises decentralisation, security, *and* speed. Every blockchain is a deliberate point on this balance.

Blockchain is not better or worse than a database – it is the right tool for a specific set of conditions. Knowing those conditions is the skill.

Source: Buterin, V. (2021). "Why sharding is great: demystifying the technical properties." vitalik.ca; Wust & Gervais (2018). "Do you need a blockchain?" IEEE Crypto Valley Conference.