What Makes a Digital Ledger Trustworthy?

Work through the activities below *before* our first session. Bring your notes and answers to class.

Activity 1 — The Broken Telephone

~5 min | 3–5 students

Instructions:

1. One student writes a short sentence (e.g., *"Send 10 coins to Alice on Tuesday"*) and shows it only to the next student.
2. Each student reads the message silently and whispers it to the next, *without re-reading.*
3. The last student writes down what they heard.

Observe: Compare the original message with the final version. Even a single changed word can alter meaning completely.

Debrief question: *What mechanism could automatically detect whether a message was altered in transit?* Write your answer below.

Activity 2 — Hash It Yourself

~8 min | individual

Mini ASCII table: `A=65 B=66 C=67 ... Z=90 a=97 b=98 ... z=122 (space)=32`
Simple checksum rule: Add the ASCII values of all characters, then take the result **mod 256**.

Input string	Sum of ASCII values	Checksum (mod 256)
`HELLO`	_____	_____
`HELLP`	_____	_____
`hello`	_____	_____

Notice: Changing just one character (`O`→`P`) or the case changes the checksum entirely. This is the *avalanche effect* — a key property of cryptographic hash functions.

Activity 3 — Link the Chain

~10 min | pairs

Paper exercise: Create three "blocks" on index cards using the checksum from Activity 2.

Block #1	**Block #2**	**Block #3**
Data: *"Alice → Bob: 5"*	Data: *"Bob → Carol: 3"*	Data: *"Carol → Alice: 1"*
Prev. hash: *0000* (genesis)	Prev. hash: _____	Prev. hash: _____
This hash: _____	**This hash:** _____	**This hash:** _____

Tamper test: Change the data in Block #2 (e.g., *"Bob → Carol: 99"*). Recompute its hash. Does Block #3's "Prev. hash" field still match? *Why does tampering with one block "break" all subsequent blocks?*

How Do Strangers Agree?

Consensus is the heart of every blockchain. These activities explore why it is hard — and how it is solved.

Activity 4 — The Byzantine Generals

~10 min | 6 students

Setup: Five students are **loyal generals**; one student is secretly a **traitor**. Generals can only communicate by passing written notes. The traitor may send *different* messages to different generals. **Goal:** All loyal generals must agree on the *same* decision: **ATTACK** or **RETREAT**.

Round 1 (no majority rule): Each general writes their preference on a card and passes it to every other general. The traitor sends "ATTACK" to some and "RETREAT" to others. Try to reach agreement.

Round 2 (with majority rule): Each general collects all received votes and acts on the majority. Does agreement hold now?

Key result: A Byzantine Fault-Tolerant (BFT) system can tolerate up to $\lfloor (n-1)/3 \rfloor$ traitors. With $n = 5$ generals, the system tolerates at most **1** traitor.

Discussion: How does Bitcoin's Proof of Work translate this problem into a computational puzzle? Who plays the role of "general" in a blockchain network?

Activity 5 — Staking vs. Mining

~8 min | small groups

Two consensus mechanisms — one goal: select who gets to add the next block.

- **Proof of Work (PoW) — Mining:** Validators compete to solve a computationally hard puzzle (find a nonce such that `hash(block + nonce)` starts with enough zeros). The first solver wins the right to append the block and earns a reward. *Like a lottery where buying more "tickets" means running more hardware.*
- **Proof of Stake (PoS) — Staking:** Validators lock up (*stake*) cryptocurrency as collateral. The protocol pseudo-randomly selects a proposer weighted by stake size. Dishonest behavior is punished by *slashing* their stake.

Dimension	Proof of Work	Proof of Stake
Energy use	Very high (ASICs run 24/7)	Low (no computation race)
Equipment needed	Specialised hardware (ASICs/GPUs)	Cryptocurrency capital
Barrier to entry	High (hardware cost)	Moderate (capital requirement)
Security model	51% hash-rate attack	33% stake attack / slashing

Group question: Which mechanism is fairer? Which is more accessible to ordinary participants?

Reflection Questions — Bring Your Answers to Class

1. If you were designing a digital currency from scratch, would you choose Proof of Work or Proof of Stake? Justify your choice with at least two concrete reasons.

2. What real-world systems already rely on consensus among multiple independent parties? *(Consider: national elections, trial juries, scientific peer review, international treaties.)* What do they have in common with blockchain consensus?

---

3. Can a blockchain be "too decentralised"? Describe at least two trade-offs that arise when the number of independent validators grows very large. *(Hint: think about latency, coordination cost, and finality time.)*
