How Does Cryptography Protect Your Money?

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

Activity 1 — The Caesar Cipher

~7 min | pairs

Rule: Shift each letter 3 positions forward (`A`→`D`, `Z`→`C`).

Encrypt `BLOCKCHAIN` with shift 3. Write your ciphertext here: _____

(answer: `EORFNFKDLQ`)

Break it: Your partner encrypts a 6-letter word with an unknown shift and hands you only the ciphertext. Try all 25 shifts until you find the plaintext. Record the shift you found: _____

Kerckhoffs's principle: The algorithm is public; only the key is secret. *Why does Bitcoin's open-source code not compromise its security?*

_____

Activity 2 — Hash It Yourself

~7 min | individual

ASCII values: `a=97` `b=98` `c=99` `s=115` `t=116` `C=67` **Hash rule:** sum all values, take **mod 256**.

Input	Sum of ASCII values	Hash (mod 256)
`cat`	_____	_____
`Cat`	_____	_____
`cats`	_____	_____

Answers: `cat`→*56* `Cat`→*26* `cats`→*171*

Changing one character yields a completely different hash — the **avalanche effect**. Can you reconstruct the word from the number 56? Why not?

Activity 3 — The Envelope Analogy

~7 min | groups of 3

Paper exercise:

1. Write a short secret, fold the paper, seal it in an envelope. Write your **name** on the outside (your **public address**).
2. Classmates seal messages to you in separate envelopes addressed by name.
3. **Only you** open your envelopes.

Mapping: public key ≈ name on envelope (anyone can send); private key ≈ ability to open (only you decrypt). *Why is sharing your Bitcoin private key catastrophic?*

_____

Why Can't You Fake a Signature?

Digital signatures and key management are the last line of defence for your coins.

Activity 4 — Sign and Verify

~8 min | pairs

1. Write *"Send 2 BTC to Alice"* on a card and add your **unique personal mark** (distinctive doodle or symbol) — your "private key" signature.
2. Your neighbour examines it: genuine or fake?
3. Your neighbour now tries to **forge** your mark on a blank card. How convincing?

ECDSA connection: In Bitcoin every transaction is signed with the sender's Elliptic Curve Digital Signature Algorithm (ECDSA) private key. The network verifies against the public key — mathematically impossible to forge. Changing even one satoshi invalidates the signature.

Why must the message content be part of what is signed, not just the sender's identity?

Activity 5 — The Key Management Challenge

~8 min | individual → group

Scenario: You control 5 Bitcoin wallets, each with a separate private key.

Question	Your answer	Group answer
How many keys to back up?	_____	_____
What if one key is lost?	_____	_____
What if a backup is found?	_____	_____

Solution — HD Wallets & Seed Phrases: A Hierarchical Deterministic (HD) wallet derives *all* keys from one **seed phrase** (12–24 words). Back up once ⇒ recover everything. Lose the seed ⇒ lose all coins. *Order of words matters.*

Reflection Questions — Bring Your Answers to Class

1. SHA-256 is a *one-way* function: easy to compute, practically impossible to reverse. Why is this critical for Bitcoin mining and password storage? What would happen if SHA-256 were reversible?

---

2. Quantum computers could break the elliptic-curve cryptography protecting Bitcoin private keys (Shor's algorithm). What happens to Bitcoin then? What post-quantum solutions are being explored, and what trade-offs do they introduce?

---

3. *"Not your keys, not your coins."* Compare the trade-offs of **self-custody** (hardware wallet, seed phrase) versus funds on a **centralised exchange**. When is each option the wiser choice?
