

Exercise walk-through

Digital currency ■ 5.2

eXercise

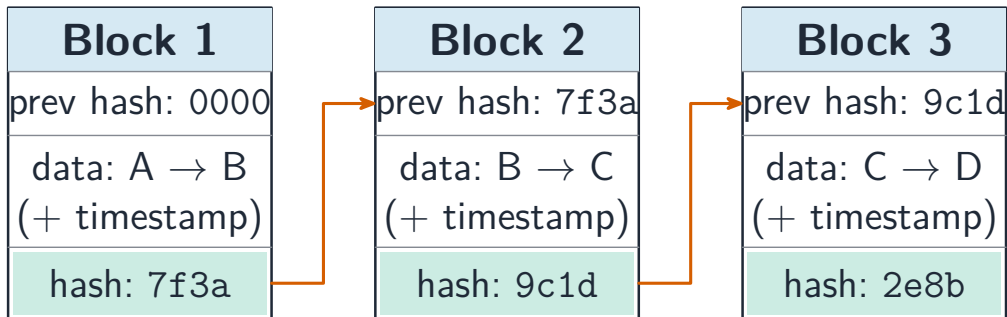
You must be able to

- describe digital currency
- describe a blockchain (a digital ledger of transactions)
- explain how the hash chain detects tampering

Method — Blockchain

- **digital currency:** money in electronic form only (no coins/notes).
- changing an old block changes its hash, so it no longer matches the next block — the change is spotted.

each block stores the previous block's hash



Blocks chained by storing the previous block's hash

Practice 2.1 ■ 1 mark

Define digital currency.

Solution 2.1

Method: Blockchain

Worked steps

money that exists only in electronic form (no physical coins or notes) **B1**.

Practice 2.2 ■ 3 marks

State the three things stored in a blockchain block.

Solution 2.2

Method: Blockchain

Worked steps

the transaction data; a timestamp; a hash value **B1** **B1** **B1**.

Exam-style 3.1 ■ 1 mark

A blockchain is best described as a:

- A** single private record
- B** shared digital ledger copied across many computers
- C** type of cookie
- D** web browser

Solution 3.1

- A single private record
- B shared digital ledger copied across many computers** 
- C type of cookie
- D web browser

Worked steps

- B.** A blockchain is a shared digital ledger copied across many computers.

Exam-style 3.2 ■ 2 marks

Blockchain makes records hard to change.

- (a) Explain how the hash links the blocks together.
- (b) Explain why changing one old block is detected.

Solution 3.2

Method: Blockchain

Worked steps

- (a) each block stores the hash of the block before it **M1**, linking the blocks into a chain **A1**.
- (b) changing a block changes its hash **M1**; so it no longer matches the next block's stored hash, breaking the chain **A1**.