

Exercise walk-through

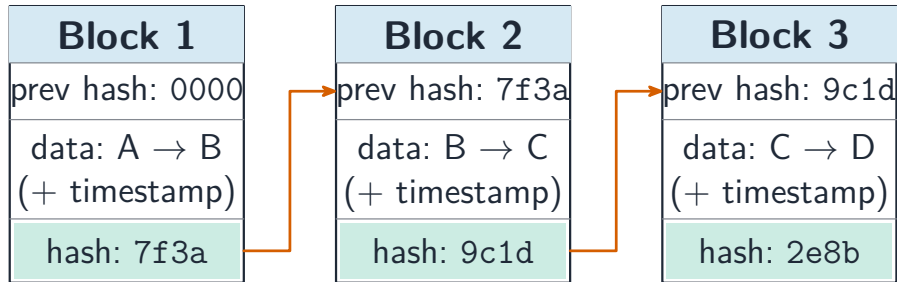
5.2

Digital currency

IGCSE Computer Science

Blockchain

each block stores the previous block's hash



A **blockchain** is a shared **digital ledger** of every transaction. Each block holds the data, a **timestamp**, a **hash**, and the hash of the block before.

Change one old block and its hash changes – breaking every block after it. That chained hash is what makes tampering **obvious**.

The malware types

virus

attaches to a file and needs a person to run it

worm

copies itself across a network with **no** human action

trojan horse

disguised as something useful, so you install it yourself

spyware

records what you do – often a **keylogger**
you type

capturing what

adware

floods you with unwanted adverts

ransomware

encrypts your files and demands payment for the key

These attacks **steal personal data, delete or change files, stop a service working, cost money, and make users lose trust in a company.**

How data is kept safe

firewall

checks traffic entering and leaving, and blocks what breaks the rules

anti-malware

anti-virus and **anti-spyware** – scan for and remove harmful software

authentication

proving who you are: a strong password, **two-step verification**, or **biometrics** (fingerprint or face)

encryption

scrambles data so an interceptor cannot read it – it does not stop theft, it makes theft useless

automatic updates

updates **fix weak points** in software, and automating them means they are not forgotten

reading carefully

bad **spelling or an urgent tone** marks a phishing message, and a strange **URL** marks an unsafe link

The last two cost nothing and stop the commonest attack there is. Technical defences cannot help a user who types their password into a fake page.

Exercises 2.1-2.2

2.1 Define digital currency.

[1]

2.2 State the three things stored in a blockchain block.

[3]

Exercises 2.1-2.2

2.1 Define digital currency.

[1]

2.1

- no physical coins or notes
- **money that exists only in electronic form**

2.2 State the three things stored in a blockchain block.

[3]

2.2

- a block stores three things
- **transaction data, a timestamp, a hash value**

Exercise 3.1

3.1 A blockchain is best described as a:

[1]

☐

A single private record

B shared digital ledger copied across many computers

C type of cookie

D web browser

Exercise 3.1

3.1 A blockchain is best described as a:

[1]

☐

A single private record

B shared digital ledger copied across many computers

C type of cookie

D web browser

3.1 B

- a blockchain is a **shared digital ledger copied across many computers**
- A is a private record; C is a cookie; D is software

Exercise 3.2 (a)

3.2 Blockchain makes records hard to change.

(a) Explain how the hash links the blocks together.

[2]

Exercise 3.2 (a)

3.2 Blockchain makes records hard to change.

(a) Explain how the hash links the blocks together.

[2]

(a)

- each block stores the **hash of the block before it**
- that **links the blocks into a chain**

Exercise 3.2 (b)

3.2 Blockchain makes records hard to change.

(b) Explain why changing one old block is detected.

[2]

Exercise 3.2 (b)

3.2 Blockchain makes records hard to change.

(b) Explain why changing one old block is detected.

[2]

(b)

- changing a block **changes its hash**
- it no longer matches the next block's stored hash, so the **chain breaks**