

Cambridge IGCSE · Computer Science 0478 · Notes

Digital currency

Read online at pastopic.com/cambridge/computer-science-0478/notes/digital-currency

Last checked 30 September 2026

Read first: [Encryption](#)

© 2026 Pastopic. Free for personal study. Please share the link, not the file.

What you need to know

By the end of this topic you should be able to:

1. **Say what makes a currency digital, and how people pay with one.** A digital currency exists **only electronically**: there are no coins or notes. People use it to pay for goods and services and to send money to each other, entirely through computers and networks.
2. **Describe how blockchain keeps a permanent record of every payment.** Blockchain keeps a shared record of every payment, called a **digital ledger**. Each entry carries the time it was made (a **time-stamp**), and entries can be **added but never changed**.

This is a small topic. It has been asked **only four times so far, once or twice a year in 2023, 2024 and 2025**, always on Paper 1 and for at most 4 marks at a time, so the exam evidence below is thin. Some worked examples below are worth more, on purpose, for extra practice. Expect short questions: a definition, the name "blockchain", a gap-fill, or an annotated diagram.

How the payment data is encrypted is in Encryption; how data travels across the internet is in The internet and the world wide web.

Understand it

What makes a currency "digital"

Ordinary money exists as coins and notes you can hold, as well as numbers in a bank's computer. A **digital currency** has **no physical form at all**. It exists only as data, so it can only be stored, spent and sent **electronically**.

How it is used:

- A person keeps their digital currency in a **digital wallet**, an app or account on their device.
- To pay a shop, or another person, their device sends the payment electronically across a network. Nothing physical changes hands.
- It can pay for anything the seller accepts: an online order, a service, even a car.

Features worth knowing (the mark schemes accept these):

- it **only exists electronically** (virtually), never physically;
- it can be **decentralised**: no single bank or government controls it, and the record of payments is held by many computers on the network (most cryptocurrencies work this way);
- it can also be **centralised**: issued and controlled by one organisation, such as a central bank;
- its data is usually **encrypted**, so a payment intercepted on the way is meaningless;
- its payments are usually recorded in a **digital ledger**, and the process that does this is **blockchain**.

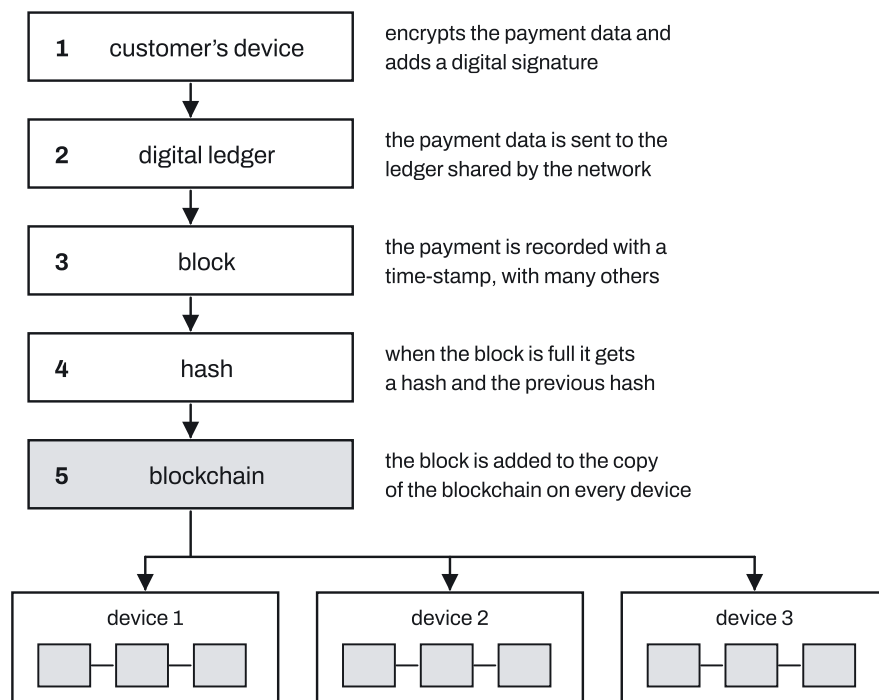
The ledger problem

Any money system needs a record of who paid whom. A bank keeps this record in its own database, and everyone trusts the bank. A decentralised digital currency has no bank, so it needs a record that:

- everyone on the network can see and check,
- nobody can secretly change (for example, to pretend a payment never happened or to spend the same money twice), and
- lets any payment be **traced** back through every earlier one.

A **digital ledger** is a record of transactions kept on computers. **Blockchain** is the process that makes this ledger impossible to alter.

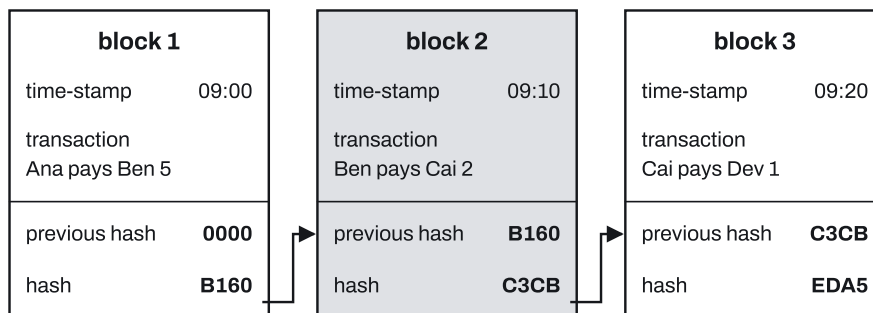
How a payment is made



1. The customer's device **encrypts** the payment data and adds a **digital signature**, which shows the payment really came from that customer.

- The payment data is sent to the **digital ledger**, which is shared by every device (computer) in the network.
- The payment is recorded as a **transaction**, with the **time and date** it was made (its **time-stamp**).
Transactions are collected together, many at a time, in a **block**.
- When the block is **full**, it is given its own **hash**, a unique identifier worked out from everything in the block. It also stores the **hash of the previous block**.
- The block is added to the end of the **blockchain**, and **every device** in the network adds it to its own copy.

Why the records cannot be altered



Each block stores the hash of the block before it.

Alter block 2 and its hash changes, so it no longer matches the previous hash stored in block 3: the change is spotted.

Each block stores the hash of the block before it, so the blocks form a **chain**:

block 1 $\xleftarrow{\text{hash of block 1}}$ block 2 $\xleftarrow{\text{hash of block 2}}$ block 3 $\xleftarrow{\quad} \dots$

The hash depends on everything inside the block, so changing even one transaction changes the hash. That creates two problems for anyone trying to cheat:

- the altered block's new hash no longer matches the "previous hash" stored in the next block, so the chain is broken and the change is spotted; and
- every device has its **own copy** of the blockchain. A changed copy no longer agrees with all the others, so it is rejected.

So the only thing anyone can do is **add new transactions** to the end. Old transactions stay exactly as they were, and because every block is linked to the one before, any payment can be **traced** back through the chain.

Key facts and formulas

There is no formula list for this subject, so you must learn all of these.

Formula	Status
Digital currency: exists only electronically, never physically	Learn it

Formula	Status
Features: electronic only; decentralised (or centralised); usually encrypted; tracked by a digital ledger	Learn it
Blockchain: a shared digital ledger of payments; each entry has a time-stamp, and entries can be added but never changed	Learn it
The process that uses a digital ledger to track digital currency: blockchain	Learn it
Payment steps: encrypt and sign → send to ledger → record with time-stamp in a block → full block gets a hash → added to the blockchain on every device	Learn it
Each block stores its own hash and the previous block's hash	Learn it
Records can't be changed or deleted, only added; every transaction can be traced	Learn it

How to do it

In the Paper 1 questions we have tagged for this topic (4 questions: 2023, 2024 twice and 2025), the types came up this often. 2 of the 4 questions mix two types, so the counts add up to more than 4.

Question type	Questions
Define a digital currency or give its features	2
Name the process that uses a digital ledger	2
Draw and annotate a payment made with blockchain	1
Complete a paragraph about digital currency	1

1. Define a digital currency or give its features (2 questions)

1. **"State what is meant by a digital currency"** (1 mark): "a currency that **only exists electronically**" (or virtually). That one idea is the mark.
2. **"Give two (other) features"** (1 mark each): pick two different ones from: only exists electronically; can be decentralised; can be centralised; usually encrypted.
3. Read the stem: if it already says digital currency is tracked by a digital ledger, that feature won't earn a mark again.

2. Name the process that uses a digital ledger (2 questions)

The answer is **blockchain**, for 1 mark. The question may describe it without naming it: "a digital ledger", "time-stamped transactions that cannot be altered", "tracks the use of digital currency". Any of these points to blockchain.

3. Draw and annotate a payment made with blockchain (1 question)

Usually 4 marks, one for each correct point shown on the diagram. Draw boxes joined by arrows, as in the first diagram above, and write a short label on each box or arrow:

1. the customer's **device encrypts** the payment data;
2. the data is **sent to the digital ledger**;
3. the ledger entry shows the customer's **digital signature** and when the payment was made (its **time-stamp**);
4. transactions are **stored in a block**, many at a time;
5. every block is given its own **hash**, which identifies it and no other block;
6. **when the block is full**, it is **added to the blockchain on every device**.

Six points for 4 marks gives you spare marks in case one is judged too vague.

4. Complete a paragraph about digital currency (1 question)

1. Read the whole paragraph first, then fill each gap from the list.
2. Most gaps need a key term from this topic: where the currency exists, the name of the ledger process, what each record carries, or what the chain lets you do with old payments. Read the finished sentence back and check it states a true fact from this note.
3. **Watch for distractors**: words that sound right but make the sentence false, such as "edited" or "removed" (blockchain records can't be), "wallet" where the sentence needs the shared ledger, or "encryption" where it needs the process that tracks payments. Check the grammar too: after "a" or "the" the gap needs a noun, and after a verb it often needs a word ending in "-ly". Invented terms that sound technical are usually wrong.

Worked examples

The bold codes show where marks are earned, as in Cambridge mark schemes. The number is how many marks.

- **B1** mark for a correct result on its own, with no method needed.

Example 1

Use terms from the list to complete the paragraph about a digital currency. Not every term is needed. **[5]**

blockchain · copy · deleted · hash · physically · time-stamp · traced · virtually · wallet

Unlike cash, which you can hold in your hand, this currency is held only , on devices and networks. When someone pays with it, the network notes the exact date and time of the payment as a A block of payments can't be quietly edited later, because the next block holds its Every computer in the network keeps its own of the blockchain. An auditor can follow any payment backwards through every earlier payment, so the history of each payment can be

Answers in order, one mark each: virtually **B1**; time-stamp **B1**; hash **B1**; copy **B1**; traced **B1**.

"Physically" is wrong for the first gap: the sentence is about where the currency is held, and it has no physical form. "Deleted" fits nowhere, because nothing in a blockchain can be deleted.

Example 2

A gamer buys a headset with digital currency. These steps describe how the payment is recorded, but they are jumbled.

- **A** The block is added to every device's copy of the blockchain.
- **B** The payment is recorded in a block.
- **C** The gamer's device encrypts the payment data.
- **D** The block becomes full and is given its hash.
- **E** The payment data is sent to the digital ledger.

(a) Write the letters in the correct order. **[2]**

(b) Add one more detail to each of steps C, B and D. **[3]**

(a) C, E, B, D, A. **B2** for all five in order; **B1** if only one pair is swapped.

(b) One mark each:

- C: the device also adds a digital signature to the payment **B1**;
- B: the payment is recorded with a time/date stamp, and many other transactions are stored in the same block **B1**;
- D: the block also stores the hash of the previous block, which links it into the chain **B1**.

Together these give all six points a "draw and annotate" question rewards: encrypt, send to the ledger, record with signature and time-stamp, store in a block with others, give the block a hash, and add the full block to the blockchain on every device. Drawn as boxes and arrows with those labels, this is a full-mark diagram.

Example 3

Explain why a transaction stored in a blockchain cannot be altered without it being noticed. **[3]**

Any three of:

- each block has a hash worked out from its contents **B1**,
- ... so changing a transaction changes the block's hash **B1**;

- each block stores the hash of the previous block **B1**,
- ... so the altered block no longer matches the next block and the chain is broken **B1**;
- every device in the network holds a copy of the blockchain, so an altered copy disagrees with the others **B1**.

Example 4

A market stall that has always taken cash starts accepting a digital currency as well.

- (a) Describe how paying the stall with the digital currency is different from paying with coins. **[2]**
- (b) The digital currency is decentralised. Explain why a decentralised currency needs a ledger that is shared by the whole network. **[2]**
- (c) The stall owner says: "The payments are encrypted, so encryption is how the currency keeps track of who paid whom." Explain why the owner is wrong. **[2]**
- (a)** Coins are physical objects handed over to the stall **B1**; the digital currency only exists electronically, so the payment is sent from the customer's device across a network and nothing physical changes hands **B1**.
- (b)** No bank or single organisation keeps the record of payments **B1**, so every device holds a copy of the ledger, letting everyone check who paid whom and stopping anyone changing the record in secret **B1**.
- (c)** Encryption only makes the payment data meaningless if it is intercepted **B1**; the process that tracks the payments is blockchain, which records them in a time-stamped ledger that cannot be altered **B1**.

Common mistakes

- **Saying digital currency is "money in a bank account" or "online banking"**. Ordinary money also exists as coins and notes. The key idea is that digital currency exists **only** electronically.
- **Writing "virtually" where the sentence says "does not exist ..."**. Digital currency does not exist **physically**; it *does* exist virtually.
- **Calling the process "encryption" or "a digital ledger"**. Encryption protects the data and the ledger is the record; the process that tracks the currency is **blockchain**.
- **Saying blockchain records can be deleted or edited by the owner**. They can't be altered at all; new transactions are only ever added.
- **Drawing a diagram without annotations**. Marks are for the points written on it (encrypt, ledger, time-stamp, block, hash, added on every device), not for the boxes.
- **Repeating a feature the question already gave**. "Give two other features" after the stem mentions digital ledgers means ledgers don't count again.

The June 2025 report found that many candidates could define a digital currency and name blockchain, so these are marks you are expected to get.

How to get the marks

- **Use the key words:** electronically, physically, digital ledger, blockchain, time-stamp, block, hash, encrypted, decentralised, traced. The mark schemes look for these.
- **"State what is meant by"** (1 mark): one precise definition, "only exists electronically".
- **"Give" / "Identify"**: a word or a short phrase is enough. "Blockchain" on its own earns the mark.
- **"Give two features"**: two **different** ideas. "Exists online" and "exists electronically" are the same idea and earn one mark.
- **"Draw and annotate"**: the marks are for the annotations, one per correct point. Put the steps in order with arrows, and write a short, specific label for each.
- **"Explain"**: give a reason and its effect, such as "changing a block changes its hash, **so** it no longer matches the next block".
- **Gap-fills**: one mark for each term in the right place. Read the sentence both sides of the gap, and check whether the gap needs a noun ("a time-stamp") or an adverb ("physically").

Quick check

1. True or false: a digital currency can be withdrawn from a cash machine as notes. Explain.
2. True or false: "blockchain" is another name for encryption. Explain.
3. What is added to each transaction to record when it was made?
4. Where is a copy of the blockchain kept?
5. Tick one true statement about blockchain: (A) the owner of a record can edit it later; (B) each block stores the hash of the previous block; (C) it is stored on one central server only; (D) old blocks are deleted when the chain gets too long.

Answers

1. False. A digital currency only exists electronically; it has no coins or notes.
2. False. Encryption makes data meaningless if it is intercepted; blockchain is the process that records transactions in a time-stamped digital ledger that cannot be altered.
3. A time-stamp (the time and date of the transaction).
4. On every device (computer) in the network, so there are many identical copies.
5. B. A is wrong because records cannot be altered; C is wrong because every device has a copy; D is wrong because nothing is ever deleted.

Past questions to try

- [0478/12/O/N/23 Q12](#): features of digital currency and the name of the process.
- [0478/12/F/M/24 Q5](#): complete a description of digital currency and blockchains.
- [0478/11/O/N/24 Q8](#): draw and annotate a payment made with digital currency and blockchain.
- [0478/11/M/J/25 Q9](#): part (c), define a digital currency and name its ledger process.