- are used in online financial transactions
- allow progress in online games and quizzes to be stored
- allow social networking sites to recognise certain preferences and browsing histories
- allow different languages to be used on the web pages automatically as soon as users log on.

## Activity 5.1

1 A URL being entered is: **http://www.urlexample.co.ie/sample_page**

Identify:

a the domain name

b the domain type

c the file name

d which protocol is being used.

2 a Give two differences between session cookies and persistent cookies.

b Describe three uses of cookies.

3 The following table shows five features of the internet and the World Wide Web. Tick (✓) the appropriate box to indicate which feature refers to the internet and which feature refers to the World Wide Web:

| Feature | Internet | World Wide Web |
|---|---|---|
| it is possible to send and receive emails | | |
| makes use of http protocols | | |
| uses URLs to specify the locations of websites and web pages | | |
| resources can be accessed by using web browsers | | |
| makes use of TCP and IP | | |

4 Why do you think persistent cookies are sometimes referred to as ***tracking cookies***? Give at least two pieces of evidence to support your answer.

# 5.2 Digital currency

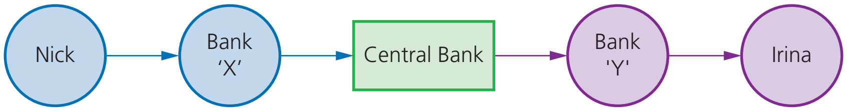
## 5.2.1 What is digital currency?

**Digital currency** exists purely in a digital format. It has no physical form unlike conventional **fiat currency** (for example, $, £, €, and ¥).

(Note: Fiat is a Latin word meaning 'let it be done'; since conventional currency is backed by governments and banks rather than being linked to gold or silver reserves, it is referred to as fiat currency.)

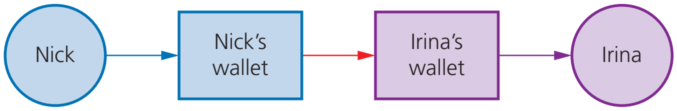
Digital currency is an accepted form of payment to pay for goods or services. As with cash or credit/debit cards, digital currency can be transferred between various accounts when carrying out transactions. It has made it possible to bank online (for example, using *PayPal*) or via a smartphone app (for example, *Apple Pay*). This is all possible because money only exists as data on a computer system, but it can be transferred into physical cash if we need it.

Digital currency relies on a **central banking system**. For example, suppose Nick wishes to send Irina some money; Nick uses bank 'X' and Irina uses bank 'Y':



▲ **Figure 5.6** Digital currency

The problem with centralisation is maintaining confidentiality and security; these have always been issues with digital currency systems. However, one example of digital currency, known as cryptocurrency, has essentially overcome these issues by introducing decentralisation:



▲ **Figure 5.7** Cryptocurrency and decentralisation

- Cryptocurrency uses **cryptography** to track transactions; it was created to address the problems associated with the centralisation of digital currency.
- Traditional digital currencies are regulated by central banks and governments (in much the same way as fiat currencies). This means all transactions and exchange rates are determined by these two bodies. Cryptocurrency has no state control and all the rules are set by the cryptocurrency community itself.
- Unlike existing digital currencies, cryptocurrency transactions are publicly available and therefore all transactions can be tracked and the amount of money in the system is monitored.
- The cryptocurrency system works by being within a **blockchain** network which means it is much more secure.

## 5.2.2 Blockchaining

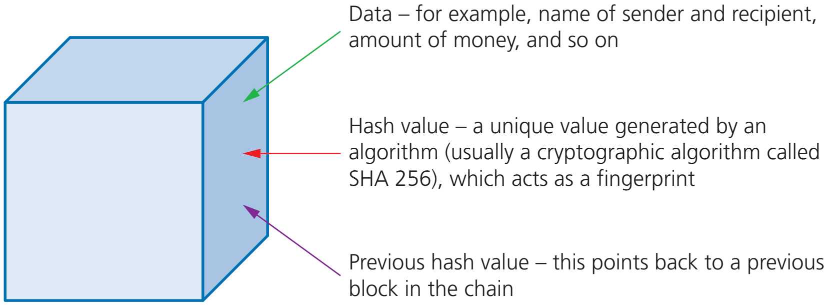
Blockchain is a decentralised database. All the transactions of networked members are stored on this database. Essentially, the blockchain consists of a number of interconnected computers but they are **not connected** to a central server. All transaction data is stored on **all** computers in the blockchain network.

Whenever a new transaction takes place, all the networked computers get a copy of the transaction; therefore **it cannot be changed without the consent** of **all** the network members. This effectively removes the risk of security issues such as hacking. Blockchain is used in many areas, such as:

- cryptocurrency (digital currency) exchanges
- smart contracts
- research (particularly within pharmaceutical companies)
- politics
- education.

## How blockchain works

Whenever a new transaction takes place, a new **block** is created:



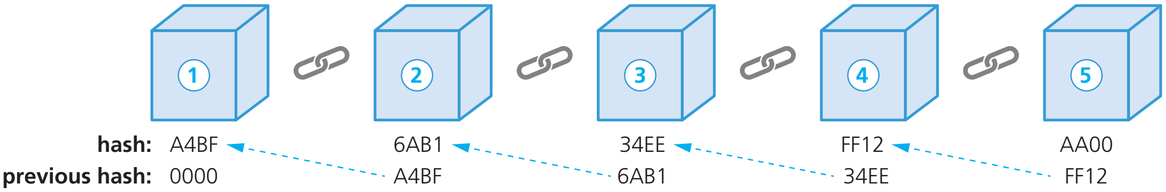
Data – for example, name of sender and recipient, amount of money, and so on

Hash value – a unique value generated by an algorithm (usually a cryptographic algorithm called SHA 256), which acts as a fingerprint

Previous hash value – this points back to a previous block in the chain

▲ **Figure 5.8** Block description

A new hash value is created each time a new block is created. This hash value is unique to each block and includes a **timestamp**, which identifies when an event actually takes place. We will now consider what happens when a chain of blocks is created. Figure 5.9 shows part of a typical blockchain:



▲ **Figure 5.9** Part of blockchain (showing 5 blocks)

It is clear from Figure 5.9 how these blocks are connected. Block ‘1’ is known as the ***genesis block*** since it doesn’t point to any previous block. Now suppose block ‘2’ is changed in some way. Any changes to the data within block ‘2’ will cause the value of the hash to change (it will no longer have the value 6AB1). This means that block ‘3’ and beyond will now be invalid since the chain was broken between block ‘2’ and ‘3’ (previous hash 6AB1 in block ‘3’ is no longer valid).

This will prevent tampering (for example, by a hacker). However, it may be crossing your mind that computers are now so fast that it should be possible to quickly create a whole new string of blocks, and therefore recreate a new chain before the problem has been discovered. This is prevented by **proof-of-work**, which makes sure it takes ten minutes to determine the necessary proof-of-work for *each* block **before** it can be added to the chain. This is ‘policed’ by **miners**, which are special network users that get a commission for each new block created. Thus, the whole process of creating new blocks is slowed down which foils hackers and also means that the currency is regulated by all the network computers.

Consequently, this makes it almost impossible to hack into the blockchain since it would be necessary to attack every single block in the chain at the same time. It only takes one block to break the link for any transaction to be terminated. When a new block is created, it is sent to each computer in the blockchain and is checked for correctness before being added to the blockchain. If a new network user is created, they get a copy of everything in the whole blockchain system.