HOW DOES THAT WORK?

BLOCKCHAIN

Blockchain technology records secure online transactions through a shared and continually reconciled database. Originally created in 2009 to manage the digital currency bitcoin, it is now being considered for applications as diverse as online voting and cloud storage.

A blockchain is a distributed database, meaning that each participant can access the whole database and its complete history. This means that no single person or group controls the data, and everyone can verify the records, which are permanent. A blockchain is made up of nodes, computers that connect to the blockchain network and receive a copy of the blockchain. These nodes communicate with each other, storing and updating information rather than being updated through one central computer.

The concept was invented to ensure that bitcoin could work in the same way as cash, able to move about without being spent multiple times by the same person, without the use of a bank. The database contains the payment history of every bitcoin, so can provide proof of who owned it at any given time.

Every transaction on a blockchain can be viewed by anyone with access to the system, with each user or node having a unique address. After confirming that the transaction is legitimate, the blockchain database puts the record, along with a number of other verified transactions, into a block and timestamps them before chaining them together using a cryptographic signature. These new encrypted blocks are added to the previous blocks, creating a chain that shows the entire history of the blockchain.

Once a transaction has been added to the database, the accounts are updated and records cannot be altered, as they are linked to all previous transactions.

Blockchain databases are not stored in one single location, but are hosted by many computers simultaneously. This means that a blockchain database contains the history of all of its records, protected from being revised, deleted or tampered with. Consequently, hackers cannot corrupt the information without targeting all computers that the blockchain is held on, as well as all the previous blocks, creating a secure online system.

The databases can be created with a group of preselected participants, or they can be 'unpermissioned' and open to everyone, meaning that anyone can contribute data and everyone that has a copy of the ledger has an identical version.

In the future, blockchain technology could be used for most financial transactions. The Bank of England has said that blockchains or digital ledger technology may be a useful platform to power a central bank digital currency, something that is currently being researched. In 2014, blockchain was used by a Danish political party for electronic voting at its annual meeting, laying the foundations for blockchain use in general elections. There are also multiple startups that are currently looking into creating blockchain-based cloud storage systems, which would eliminate hacking and data loss problems that often arise in traditional cloud storage.

Someone requests a transaction

The requested transaction is broadcast to a network of computers

Validation
The network validates the transaction and the user's status using known algorithms

A verified transaction can involve cryptocurrency, contract, records or other information

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger

The transaction is complete

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

The cycle of a blockchain transaction