

Executive summary

Blockchain is much more than Bitcoin.

Blockchain's first implementation as the technology underpinning Bitcoin has led many to associate Blockchain with Bitcoin. However, the potential use of Blockchain goes well beyond the world of cryptocurrencies. For some, it is a technology that will change our lives, while for others it is a pipe dream; no technology has stirred up so much debate since the advent of the internet. However, despite the numerous headlines on Blockchain, the technology remains difficult to apprehend for many.

Blockchain: a tamper-proof, decentralized and distributed digital record of transactions that creates trust and is said to be highly resilient.

A blockchain is a decentralized, distributed record or “ledger” of transactions in which the transactions are stored in a permanent and near inalterable way using cryptographic*¹ techniques. Unlike traditional databases, which are administered by a central entity, blockchains rely on a peer-to-peer network that no single party can control. Authentication of transactions is achieved through cryptographic means and a mathematical “consensus protocol”* that determines the rules by which the ledger is updated, which allows participants with no particular trust in each other to collaborate without having to rely on a single trusted third party. Thus, Blockchain is, as The Economist calls it, a “trust machine”. Participants in a blockchain can access and check the ledger at any time.

Blockchain therefore ensures immediate, across-the-board transparency, and as transactions added to the blockchain are time-stamped* and cannot easily be tampered with, blockchain technology allows products and transactions to be traced easily. Smart contracts* – i.e. computer programmes that self-execute when certain conditions are met – can be used to automate processes, further reducing costs. Because of their decentralized and distributed nature and the use of cryptographic techniques, blockchains are said to be highly resilient to cyber-attacks compared to traditional databases – although there is no such thing as perfect resilience.