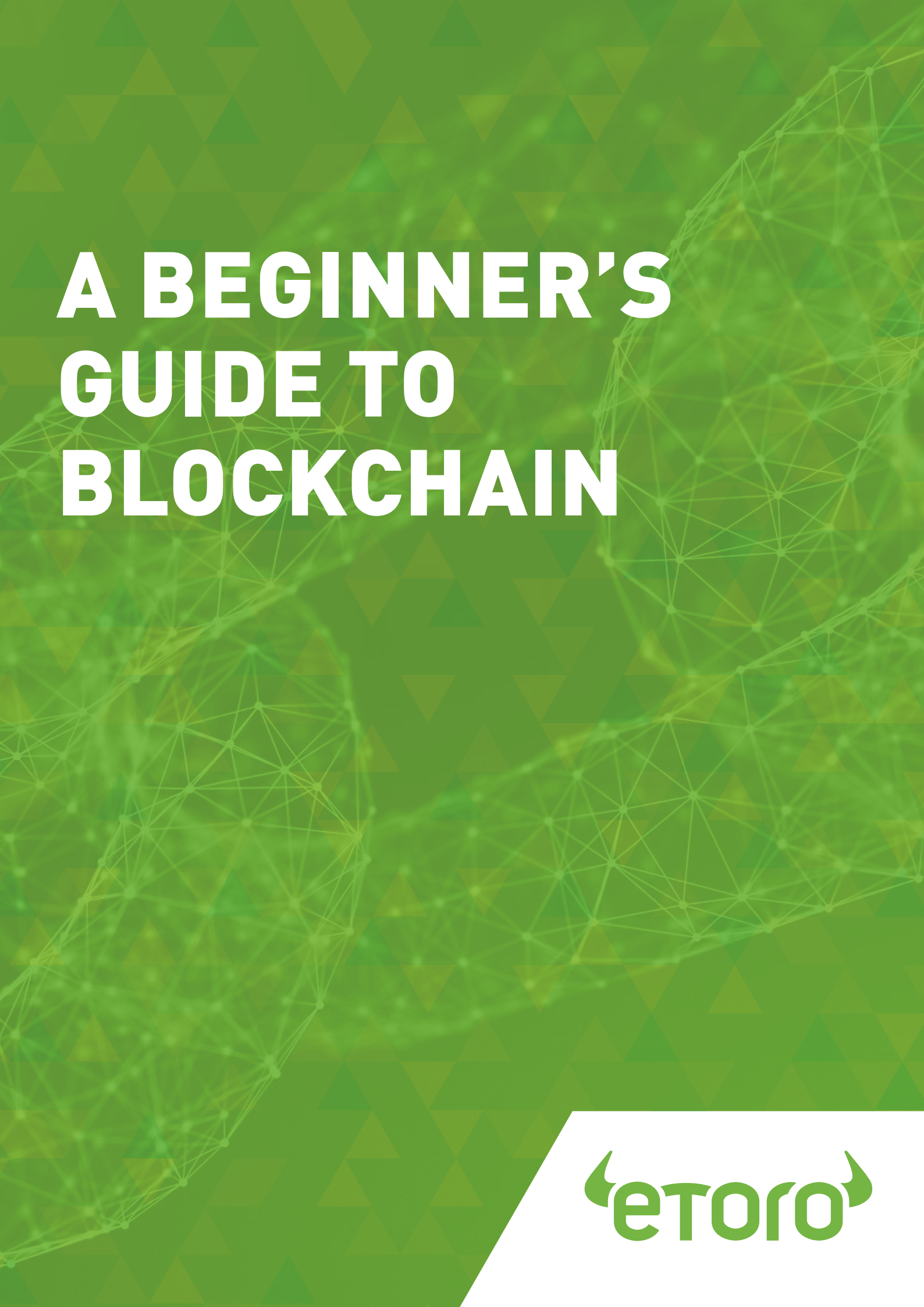
A BEGINNER'S GUIDE TO BLOCKCHAIN



Contents

Introduction

Cryptoassets, and particularly bitcoin or "digital gold" as some experts have labelled it, is a hot topic. Many believe they represent the future of money. Arguably, the most important and exciting element in the crypto space is the underlying blockchain technology.

Blockchain technology will revolutionise the way we interact with each other. It is a technological advancement that could have wide-ranging reverberations that will not only transform financial services but countless other organisations and industries, such as healthcare and security. Why? Due to the way it allows information to be tracked and stored in a trustworthy and transparent way.

Interest in crypto has grown with the rise of bitcoin, and the hundreds of other cryptoassets the original cryptocurrency has spawned since it was launched in 2009. In fact, the idea of a blockchain has been around for almost 30 years, since the early 1990s. Bitcoin is simply the first successful application of blockchain technology, which has become integral to the popularity of the ever-expanding cryptoasset world.

This relationship between blockchain and cryptoassets is similar to the one between the internet and email. Much like email is just one use case of the internet, the first cryptocurrency – namely, bitcoin – is the original use case of blockchain technology.

This guide refers to the bitcoin blockchain.

"This relationship between blockchain and cryptoassets is similar to the one between the internet and email."

So what is blockchain?

A blockchain is a secure, distributed database. For example, normally in an office all the computers are connected to one common server. However, with blockchain technology the computers are linked to many different devices and processors. Within this database there is an ever-growing list of blocks. Upon entry, each block is time-stamped and 'attached' to the previous block to create a 'record'.

A good metaphor for blockchain is 'the internet of value'. Anyone can produce and publish information on the internet and others can access that content wherever they are in the world. Likewise, a blockchain allows someone to send value anywhere around the globe where the blockchain can be accessed. It is crucial to have a public-private, cryptographically-created key pair in order to access the blocks you own.

In summary, a blockchain is a shared, inflexible database for recording the history of all transactions using a system that encourages transparency and trust, minimising the need for trust by distributing it across the network users. In the words of the father-and-son authors of Blockchain Revolution, Don and Alex Tapscott, a blockchain is defined as an "incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value".

Perhaps the most impressive feature of blockchain technology is that it provides security in an unsecured internet – where phishing and malware can compromise the data of individuals and jeopardise the way business is done around the world.

"A good metaphor for blockchain is 'the internet of value'."

How does blockchain work?

Blockchain securely stores data in batches – or blocks – that are linked together chronologically, forming a continuous chain. Unlike the old ledger method, whereby a book or database would be used to store information, the blockchain was designed to be decentralised and distributed across a large network of computers. This clever decentralising of data limits the ability to tamper with the information, building trust in the system.

How is it tamper-proof? The way a block links with previous blocks, and then the next block appends itself to the chain, meaning it is impossible to change any information without impacting the whole chain.

To add a block to the certain blockchains, a computer must provide a code or 'hash' in order to create a batch of data that forms the next block. That computer will then share the solution to all the other computers in the network, providing a 'proof-of-work'. Once entered, the network will verify the proof-of-work and a block will be added to the chain.

To find the hash, computers use a process of trial and error to guess the cryptographic signature – a combination of the record of the most recent crypto transactions along with a proof-of-work and the signature for the previous blocks. Once the combination has been found and verified by the network, a new block is added to the blockchain. The race for the next hash then begins. This is known as mining.

Imagine each block is a Word document. And the filename of that document is 'Crypto needn't be cryptic'. The file needs to become a "hash", a sort of fingerprint for a file or block. A hash is a combination of letters and numbers that must start with a predetermined number of zeros (at the time of writing, it was 18 zeros), for example 000000000000000006dbfjls8676fbsT3k4j88.

In order to create this hash we have to start with the filename of the document, for example, eToro2018, and see what hash it produces. For example, if the filename 'Crypto needn't be cryptic' created the hash 0009ehk5lki6bnm7hgf2srt7fk9, we know it is incorrect as it doesn't start with the correct number of zeros. This process is called "mining" and is done by trial and error.

"To add a block to the blockchain, a computer must provide a code or 'hash' in order to create a batch of data that forms the next block."

Features & differences

For many, blockchain – rather than bitcoin and the crypto stampede it triggered – is by far the bigger game-changing innovation introduced by Satoshi Nakamoto, the name given to the anonymous person (or persons) who published the famous white paper, *Bitcoin: A peer-to-peer electronic cash system* on 31 October 2008.

This is because blockchain technology, which laid the foundations on which a vast majority of cryptos now operate, has the potential to transform numerous industries outside the crypto sphere. These include healthcare, financial services, and housing, to name but three. Experts are queuing up to proclaim its potential to be as revolutionary as the internet.

However with an electronic payment system, and if money takes the form of a digital file, you may think that it might be possible to replicate it. This is not the case with the blockchain. The bitcoin blockchain secures the cryptocurrency by making it impossible for it to be counterfeited.

Let's imagine George has a bike that he wishes to sell online. Peter has viewed the bike and is keen to buy it. Rather than requiring a third party, such as PayPal, to process the transaction, bitcoin and other cryptoassets that use a peer-to-peer payment system can make it much more straightforward. Peter initiates a transaction by sending George the agreed amount of cryptos and, once processed, the bike is exchanged. If George then fails to give Peter the bike, the transaction will be reversed.

This is why blockchain technology is central to cryptos, and sets them apart from other currencies, by:

- Decentralising data and allowing information to be shared;
- Building trust in the data through peer-to-peer verification;
- Allowing people to interact with the data without the need for an administrator or intermediary using cryptography.

Cryptography – as mentioned above – ensures that those who use the blockchain can just edit the parts they effectively 'own' by possessing the private keys needed to access their record. This also means that everyone's version of the blockchain is synchronised at all times.

For example, MedicalChain is the first healthcare organisation to employ blockchain technology to facilitate the storage and utilisation of electronic health records to deliver a complete telemedicine experience. Only certain people can view these records and they cannot be edited.

With an inbuilt safeguard against fraud and false identity, greater transparency, lower fees for cross-border transactions, and freedom from government interference, cryptos have started transforming payment systems around the world.

"Blockchain has the potential to transform numerous industries outside the crypto sphere."

Is there more than one blockchain?

Yes. Blockchain is a technology, and not a single network, meaning it can be implemented in many different ways. Some blockchains are completely public, Bitcoin, for example, and open for anyone to view, while others are only visible to a select group of authorised users and called a private blockchain in a network. The latter group is used by banks, government agencies, and similar.

There is a third type: a hybrid blockchain, sometimes called a federated blockchain. This is a fusion of the public and private approaches, where some data is accessible to all with a fraction of it held back for the eyes of only a few. Certain members of a hybrid blockchain can determine what transactions remain public and what information should be confined to a smaller group, protecting digital assets – the best of both chains, if you will.

For instance, Lucy has a blockchain-backed digital medical record. Every time-stamped entry is a block, meaning every appointment Lucy attends is recorded. This shows Lucy's medical history, and is invaluable to a doctor who is in possession of the private key that allows him or her to access the data. As blockchain travels in one direction, by design it is impossible to alter the record retroactively. The information is shared with a third party – such as a specialist – only when Lucy or the doctor allows it.

While blockchain's original purpose was to power bitcoin, society is now beginning to benefit from its many applications. For example, verifying the providence of diamonds, tracking contaminated food, or even paying the dentist. How? By being transparent and digitally accessible to all.

For example, when you buy a football shirt, how do you know it's a real one and not counterfeit? From the manufacturer to the club to the shop, you can keep record on the blockchain. Since it's immutable, you know that nobody can edit it. It is possible that in the near future football fans will be able to scan a barcode on an item of merchandise and be reassured that it's an official product. Similarly, it could bring transparency to the sale and resale of tickets.

In the food industry, OriginTrail allows consumers to know where their purchases came from and how they were produced. Tampering with sell-by dates and adding secret ingredients cannot happen.

When it comes to precious stones, as with food, blockchain can help to build confidence by providing a complete and transparent record of providence. De Beers, which mines, trades and markets more than 30 per cent of the world's supply of diamonds, has plans to use a blockchain ledger for tracing its precious stones from the mine to the customer purchase. This transparency will help the industry as a whole and individuals in particular who wish to verify that the diamonds they are buying are free from conflict.

"Blockchain is a technology, and not a single network, meaning it can be implemented in many different ways."

Blockchain transforming industries

When it comes to music, films and books, the advent of the internet, and streaming sites such as Soundcloud, Mixcloud, and Spotify, has made digital music more accessible to everyone. This comes at a cost to the artists, insofar as they are not remunerated for physical sales of albums or singles in the way they used to be. Blockchain has the potential to put an end to that.

In the same way bitcoin can make a token that cannot be replicated, the Recording Industry Association of America (RIAA), for example, could sign every digital copy of a song to a single buyer. This applies for films and books, too, and would return entertainment to the days when purchasing an album, hardback novel, or DVD would mean exactly that.

Moreover, Estonia – "the most advanced digital society in the world", according to Wired – began experimenting with blockchain technology in 2008, a year before it was used to underpin bitcoin. It is used to help with the country's healthcare database, and its voting system. All of which can be accessed digitally by any resident. In these days of fake news and fears of election rigging, blockchain technology could be the answer.

Elections require authentication of the identity of those voting, in addition to secure record keeping, and trustworthy tallies to identify the election winner. Blockchain tools can be used to ensure vote casting, tracking, and counting is correct and tamper-proof. Follow My Vote is one example of a blockchain voting startup. Using this, for example, Sally can vote with the reassurance that her decision is made available on the blockchain for all to see, and cannot be altered.

Iqbal V. Gandham, UK Managing Director at eToro, is positive blockchain technology will change the world for the better. "Many experts predict that blockchain will become as revolutionary, transformative and important in our daily lives as the internet is today," he says. "I believe blockchain could be even bigger than that. However, we are still at a very early stage of the technology's life cycle, and that is crucial to bear in mind.

"If you consider that the first elements of the internet were put together as far back as the 1960s, and Hotmail, which launched in July 1996 and offered the world's first user-friendly electronic-mail platform, I would suggest that blockchain is currently at about 1994 – the year the world's first internet café [Cafe Cyberia in Whitfield Street, London] opened – by comparison: therefore, blockchain is on the cusp of mass-scale adoption."

"The Recording Industry Association of America (RIAA), for example, could sign every digital copy of a song to a single buyer."

Glossary

Bitcoin
The first and largest cryptocurrency (by market cap). Bitcoin was launched in 2009 as a decentralised currency, built on blockchain technology. It's the first real-world application of blockchain. Bitcoin was created by a person (or group of people) under the pseudonym Satoshi Nakamoto.

Blockchain
A decentralised network, built from a continuous chain of blocks. All transactions on the network are stored on a public ledger, which exists throughout the network, meaning there is no need for a central server to authorise transactions.

Cryptocurrency
A digital currency that uses cryptography to verify transactions and provide security. The first major application of blockchain, a cryptocurrency is a currency designed to have no central ownership. Blockchain technology is the infrastructure that enables cryptocurrencies to be stored on the network to change hands.

Cryptoasset
An umbrella term used to describe cryptocurrencies, tokens, cryptocollectibles, and crypto fiat currencies.

Private key
A string of numbers and letters known only to the user. Each user on the network holds a private key. It equates to a 'password'.

Public key
A string of number and letters that is used to encrypt data on the blockchain. If the private key can be equated to a password, the public key is a username of sorts, as it is available for all to see on the public ledger.

This guide is provided for information and educational purposes only and should not be considered to be investment advice or a recommendation. The information and opinions contained in this guide are based on sources believed by eToro to be reliable.No guarantees or warranties are made to its accuracy, completeness or suitability for any purpose. Cryptocurrencies can widely fluctuate in prices and are not appropriate for all investors. Trading cryptocurrencies is not supervised by any EU regulatory framework.