# #\*\*What is Blockchain and why do we need it?\*\*

## ##\*\*Contents\*\*

1. Introduction
2. Related Articles
3. What is Blockchain
   1. How does it work
   2. The benefits
4. The history of Blockchain
5. Why do we need Blockchain technology
6. Reference List

## ##\*\*Introduction\*\*

This article will explain what Blockchain is and how it works. It will then examine briefly the history of Blockchain technology, before considering why we need this technology.

## ##\*\*Related Articles\*\*

Smart Contracts.

## ##\*\*What is Blockchain?\*\*

At its simplest, a Blockchain is a connected series of blocks of data. However, unlike ‘traditional’ data blocks, which are created from a single origin or by an administrator, as a document may be written by a single user, Blockchain data is created by the consensus of a network of users. Blockchains can be used to record any kind of formatted data and are highly secure. [1] Blockchain technology however is a foundational technology, on to which applications are built. [2]

### ###\*\*How does it work?\*\*

As an example of how the Blockchain works, let us consider a financial transaction conducted on a Blockchain application. A person wishes to send some money to a friend overseas. The sender commences the transaction by entering the relevant details, which becomes a small piece of data. This data is then distributed to the network of users or computers controlling this Blockchain. These users compete to be the first to analyse the details of the transaction and either verifying or declining the transaction. If the transaction is verified and accepted, the decision is shared with all the other users and the transaction is carried out. The transaction data is linked to the data of the previous accepted transaction in an ongoing chain. Once a certain number of these transactions have occurred, they are bundled in to one large data block, a block in an ongoing Blockchain and a new block is commenced. [2 - 4]

Users who verify transactions and create new blocks are generally called miners, although there are different ways in which they can be selected and rewarded. [3] Blockchain verification is conducted by miners using algorithms or Smart Contracts - protocols which specify a set of requirements which must be met in order to accept the transaction. Smart Contracts can be set up to run automatically without human intervention and computational logic can be used to trigger new transactions when certain conditions are met. [3] For more information on this, see the chapter on Smart Contracts.

Blockchain is a foundational technology, onto which applications are built. [2] It is particularly well adapted to any situation where a record or ledger is needed. [1] For example, a marriage register application may be built upon this foundation, with specifications that not only must vital information of the participants be included, but also verification that neither party is currently in another marriage.

### ###\*\*The Benefits of Blockchain\*\*

This way of operating has various benefits, first and foremost it’s decentralisation. Blockchains do not require a single manager or controller, no intermediary needed, it is directly peer to peer. [2] As one example of how this may be of benefit, it has been suggested by Don Tapscott [cited in 1] that when it comes to charities or government spending, money can be sent directly to the beneficiary, rather than having to go through intermediaries, who may also take cuts of it. Another example is the entertainment industry, which could directly share their products with the public and be paid directly for their work.

Secondly, Blockchain technology is highly adaptive, the requirements and algorithms can be easily changed to meet a wide range of situations. While thus far Blockchain has mainly been used for financial transactions and associated with cryptocurrencies, it has potential in almost every other industry. It is already being used for public service records in Estonia. It could also be used for real estate records, supply chains, the entertainment industry, health records or prescriptions, and endless other records. [3]

Boucher also discusses it’s potential for voting in elections, with reduced costs, and the potential to increase engagement and turn-out with a simplified process. But they go on to point out that such a mechanism could be used in many other areas where attempts are made to involve large numbers of people in decision making, such as governmental policy making, or shareholder votes.

Blockchain technology also offers more security measures than are currently available with other technologies. As each transaction in a block is linked to the last, no one transaction can be tampered with. [2] Another benefit is that users do not have to reveal their identity, but can remain virtually anonymous. Users are allocated a unique code and may choose to reveal only that, or more of their information. [2] Blockchains can also be permissioned, to limit access to only certain selected people, or they can be public. [3]

The speed and cost of transactions varies between applications. Some fees may only be a few cents, or a percentage of the transaction amount. Other applications do not charge fees. The speed of the transaction can depend on the methods of verification. However there is great potential for Blockchain based transactions to be both cheaper and faster than current methods.

Figure 1: How Blockchains are created

## ##\*\*The History of Blockchain\*\*

The short version is that Blockchain technology was founded by Satoshi Nakamoto, a pseudonym used by an as yet unidentified person or persons. On October 31, 2008 Nakamoto published a paper entitled \*‘Bitcoin: A peer to peer electronic cash system’\* explaining Bitcoin and it’s foundation, Blockchain technology. On January 3, 2009 the first block of the Bitcoin Blockchain was created. [5]

The roots of the technology, however, can be traced back to World War 2, when the Nazi regime used Cryptography – encrypting information and sharing it among a range of sites. Famously, Alan Turing deciphered the codes of the Enigma machine the Nazis were using for this purpose. In the War in the Pacific, cryptography was used again by the Japanese, and again the codes were broken. Yet despite the failure of cryptography in these instances, governments around the world began to use it. [5]

Th next major steps in the development of the technology came in 1976, when Whitfield Diffie and Martin Hellman wrote a paper describing how the system could be broken into two parts. They described a Public Key, which could be used to encode a piece of information, and a Private Key, which was needed to decode the information. Although they described the process, they did not fully develop it. [5 - 6]

In 1977 three Americans, Ron Rifest, Adi Shamir and Leonard Adleman created the RSA algorithm, used for generating keys to encrypt and decrypt information. To publicise their algorithm and prove its strength, the three scientists posed a challenge in a magazine, that anyone who could decipher a message they presented would win $100. It was not until the mid-1990s that four men, Derek Atkins, Michael Graff, Arjen K. Lenstra and Paul C. Leyland, were able to decode the message, which they did by connecting several computers around the world to work on the puzzle jointly. [5 - 6]

Thus the foundations of Blockchain technology had been born - secure, decentralised information sharing using a two-step authentication process. A little over a decade later, Nakamoto completed the final steps of it’s development.

## ##\*\*Why do we need Blockchain technology?\*\*

Technology must, and will, continue to advance to meet new or increased demands of our changing daily life. Contracts, transactions and records are the defining structures of most political, legal and economic systems, yet the technology behind these structures has not really kept pace with digital advancements. [2] Blockchain technology is a huge technological leap forward, which can make these things fairer, safer, faster, simpler. Many of the benefits listed earlier form the basis of why we need Blockchain, but we will elaborate here.

As Don Tapscott described when interviewed by Ron Kirkland [1], currently we create a lot of data, yet we do not own it, and in some cases we cannot even access it. Instead large corporations or government agencies own the data we create and can use it to spy on us, to influence our decisions, or can sell it to others for large sums of money. Blockchain technology has the potential to dramatically change this landscape and give our data, and it’s associated value, back to us.

This potential is not limited to our own social media data use or internet searches, but many other industries as well. Tapscott gives the example that recording artists could share their music on the Blockchain, with associated Smart Contracts limiting how it can be used and ensuring they are paid directly [1].

Such changes would eliminate the need for third party intermediaries who make money off the actions of others. This would cover an enormous array of people, including various finance workers, entertainment industry executives, various data collectors, and on and on. And while this potential loss of jobs is a large downside of Blockchain, the technology does open the door to other new types of jobs, such as Blockchain miners and programmers, as well as offering the abovementioned opportunities to profit from the creation of our own data. [1] Blockchain technology has the potential to change almost every industry we have, which will require large scale shifts and reshuffling, however as huge changes have occurred in the past, the workforce will likely adapt over time.

In the past several years we have seen dramatic increases in hacking events, identity and monetary thefts, data breaches and other technological crimes. While we should be hesitant to think that Blockchain technology can eradicate these events due to its absolute security, it does present greater security measures than are currently available with other technologies. As stated earlier, users of Blockchain based applications have control over what information about themselves they release to other users. [2] Smart Contracts ensure that specified requirements are satisfied before interactions occur. [4] This means that while you do not have to know all about who you are interacting with, you can use a variety of security requirements to ensure they are trustworthy. [4] Furthermore, if you send money to one person intentionally, but then accidentally also send the same instruction to another user, the algorithm will pick up the error and prevent the second transaction. [1] The distributed network means that multiple users on a network all hold an up to date copy of the ledger at all times, and changes in any one ledger must be confirmed by other users, making any corruption much more difficult. Furthermore, changing one entry in a Blockchain is impossible, as all entries are linked. This essentially means that to change one entry, you must change all of them, going back to the very beginning of the ledger, a virtually impossible task. [4] As the use of Blockchain based applications expands, some may find ways to exploit weaknesses in the technology, and certainly mistakes can be made when entering information on to the platform, however Blockchain applications are significantly safer than those based on other platforms.

While the task of building Blockchain based applications and setting up Smart Contracts with their specific requirements, may not be fast or easy, once these things are in place, industries can operate not only faster, but in a simpler way. The potential of Smart Contracts to initiate exchanges or record keeping without any human intervention makes many current tasks redundant.

It is impossible at this stage of Blockchain’s development to say where it will take us and exactly what tasks it may be called upon to perform in the future. It is possible to state that there is enormous potential for it to change our lives in positive ways. Thousands of people in hundreds of countries are investigating and developing uses for Blockchain and this is only likely to increase in the future as the world continues to embrace this revolutionary new technological landscape.

## ##\*\*References\*\*

1. Kirkland, R. \**How Blockchains could change the world*\* McKinsey & Co. May 2016. <https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world>
2. Iansiti, M. and Lakhani, K. R. \**The Truth about Blockchain*\* Harvard Business Review. January-February 2017. <https://hbr.org/2017/01/the-truth-about-blockchain>
3. Boucher, P. \**How Blockchain technology could change our lives: In depth analysis\** European Parliamentary Research Service, Scientific Research Unit. February 2017. <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf>
4. Church, Z. \**Blockchain, Explained\** MIT Sloan School. 25 May, 2017. mitsloan.mit.edu/newsroom/articles/blockchain-explained/
5. Anonymous*. \*From Alan Turing to Cyberpunk: The history of Blockchain\** Bank Bilbao Vizcaya Argentaria, S.A. 5 December 2017. <https://www.bbva.com/en/alan-turing-cyberpunk-history-blockchain/>
6. Milanov, E. \**The RSA Algorithm*\* 2 June 2009 <https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf>