Greater Manchester | Greater Security | Greater Business

# Cyber Foundry

# Blockchain: Cutting Through the Hype

## Does your business need to consider blockchain?

**Audience: General** **Reading Time: 15 Mins**

*"Don't be fooled by unrealistic predictions of returns and claims made through press releases, spam email, telemarketing calls, posts online or in social media threads. These actions may be signs of a classic 'pump and dump' fraud"*
*– Financial Industry Regulatory Authority*

## Key Points

- With all the talk surrounding blockchain and *Bitcoin* it is often hard to spot the hype from the reality. With every new technology there is a rush to implement it into your business model to show your business is on the cutting edge, however as history has often taught us, early adopters can sometimes be stung.
- Blockchain technology is based on four core principles. It is a *public distributed immutable ledger*. This means simply that it is a record of transactions (ledger) which is open to all (public); stored on several devices at once, rather than centrally (distributed); this can be added to, but not edited (immutable).
- Due to blockchain's four core principles, the potential applications are quite narrow. Subsequently, technical implementation of a blockchain is rarely required in a project.
- Blockchain technology can save a business time and money, but only when used appropriately.
- The primary advantage of blockchain is cutting out the middleman of a transaction. For *Bitcoin* that means cutting out a bank to verify your financial standing.
- A lack of a central regulator can be a significant business risk when using existing blockchain platforms.
- Due to the large sums of money made through Bitcoin, blockchain technologies are often seen as get-rich-quick schemes and in fact several companies are now being investigated for stock *pump-and-dump* schemes precisely because of their 'use' of blockchain.
- Blockchain's core technology has been around since the mid 90's, yet it only came to fame since Bitcoin was created by Satoshi Nakamoto. Who is that you ask? Well, no-one knows! Something perhaps to be cautious of when considering this technology for your core business practices.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

# The Background

**If you have kept your finger on the latest tech pulse, you will have no doubt heard the words *blockchain* or *bitcoin* thrown around. With so many articles and analysis, it's hard to simply understand what blockchain is, how it works, and whether you need it. This article looks to cut through the hype and explain the underlying principles that make the technology unique.**

## The History

Blockchain technology has been around since the mid 90's. However, it had little interest until *Bitcoin* was created in 2008. Bitcoin is built using blockchain technology with part of Bitcoin's intrigue being that its creator is unknown. In 2008, a paper called '*Bitcoin - A peer to peer electronic cash system*' was posted online, by someone calling themselves Satoshi Nakamoto.

Since then Bitcoin's value has soared and consequently many see it as a get-rich-quick scheme. In one year alone Bitcoin's value rose from nearly £700 to nearly £15,000. In fact, if you had invested £1,000 in the year it was first publicly available, in 2017 your investment would have been worth £36.7M.

Due to the amounts of money involved and stories of early investors, this has accelerated blockchain through the *Gartner Hype Cycle*. *(See figure 1)*

## The Hype

Bitcoin's underlying technology is blockchain and there seems to be a common misunderstanding that anything using blockchain technology will financially succeed

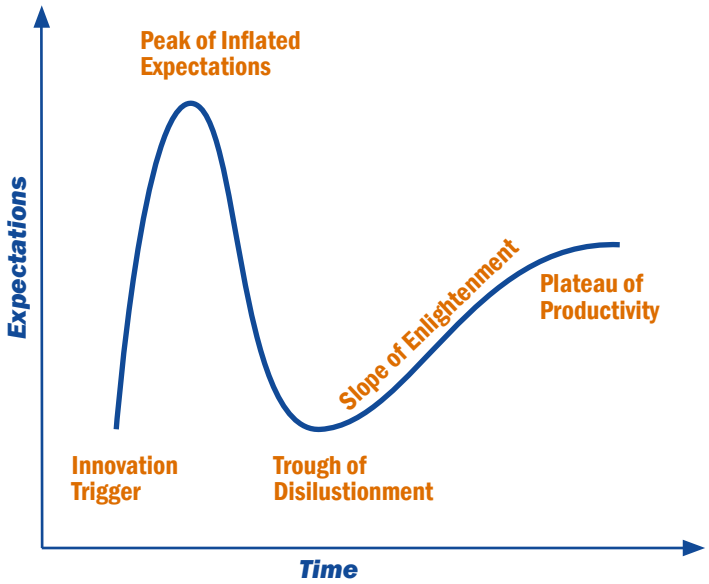



*Figure. 1 - Gartner Hype Cycle*

**Definition**

- **Innovation Trigger:** A technology is conceptualised with an early proof of concept. Usually commercially unproven, with no accesible products to test out.
- **Peak of Inflated Expectations:** Early publicity produces a number of success stories — often accompanied by scores of failures. Some companies take action; many do not.
- **Trough of Disillusionment:** As experiments and implementations fail to deliver, interest starts to decrease. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.
- **Slope of Enlightenment:** More instances of how the technology can benefit the enterprise start to crystallize and become more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.
- **Plateau of Productivity:** Mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology's broad market applicability and relevance are clearly paying off.

and create huge profits for a company. However, the stock market does not respond to technical logic, but to hype. It has been shown there is a link[1] between companies adopting blockchain technology publicly and their financial performance.

In late 2017, the New York based beverage maker *Long Island Iced Tea* changed its name to *Long Blockchain Corp* and announced it was focusing to invest in blockchain technologies - namely Bitcoin. Their stock consequently leaped 200% and closed up 183%.

In fact, so many companies have started doing this that in December 2017 the Financial Industry Regulatory Authority issued a warning to investors stating:

*"Do your research before purchasing shares of any company offering investment opportunities in cryptocurrency. And don't be fooled by unrealistic predictions of returns and claims made through press releases, spam email, telemarketing calls or posted online or in social media threads. These actions may be signs of a classic 'pump and dump' fraud."*

## What is Blockchain?

Blockchain is a cryptographic way to store data securely. In simple terms it is a fancy database. The way it differs to previous database technologies is it removes the trust needed in a governing authority, for instance a bank or hospital. Rather than trusting the governing authority to verify the accuracy of information it is done democratically.

### A Simple Analogy

You decide to play a game of football with your friends. There are 22 of you, which is enough for 11 per team, but no referee. Instead of not playing or teams being uneven, you decide that on any referee decision will be decided as a group on a case by case basis. Whatever decision the majority votes for, you will follow.

This analogy demonstrates the distributed and democratised nature of blockchain technologies. There is no single governing body as every decision is made by the group as a whole. Although some may act dishonestly for their own personal gain, if the majority are honest then the integrity of the truth is maintained.

To apply this to a cryptocurrency like BitCoin, when a user wants to know how much another user has in their *BitCoin wallet*, they ask the group to verify what is in said wallet. The majority then rules.

> *A blockchain removes the need for a trusted governing middleman*

**Definition**

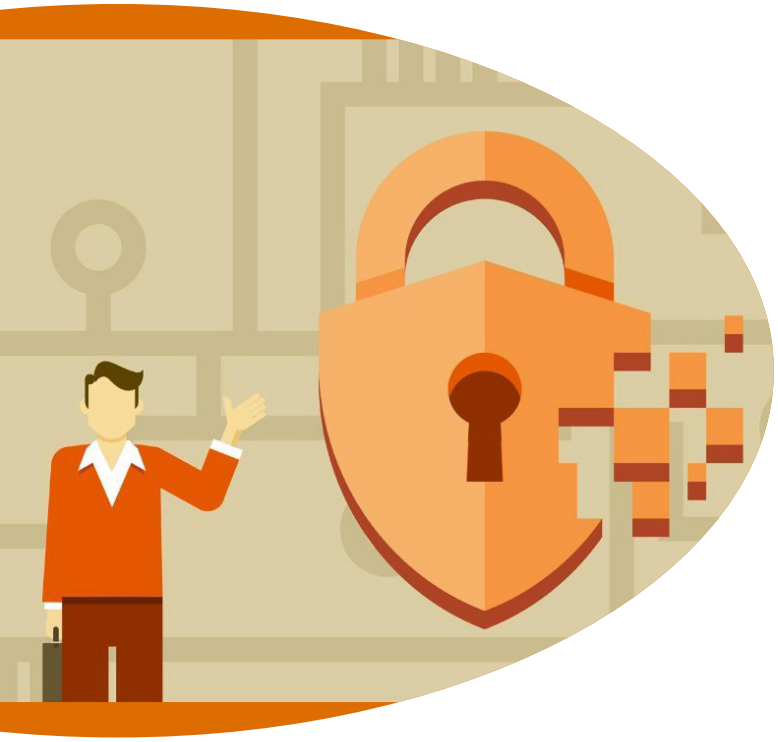
- **Bitcoin** - a type of digital currency in which a record of transactions is maintained and new units of currency are generated (mined) by the computational solution of mathematical problems, and which operates independently of a central bank.
- **Blockchain** - a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.
- **51% Attack** - 51% attack refers to an attack on a blockchain by a group of miners controlling more than 50% of the network, or computing power.

[1] https://www.finra.org/investors/alerts/dont-fall-cryptocurrencyrelated-stock-scams

### A More Complex Analogy

You want a new ukulele, so you go to your local music shop to buy one. There are rumors that the shop owner will take money from his customers without actually having the items in stock. Unfortunately for you, this is the only music shop in town and you want the ukulele.

You go to the cashier and ask to buy a £10 ukulele. The cashier claims to have one in stock but refuses to show you until you have paid. This is due to a lot of people who have asked for ukuleles, taking them, and leaving the music shop without paying. As a result, you are asked to pay upfront. However, you do not trust this shop as you have not seen the product, and you are not sure if they even have one in stock. You are both stuck in a stalemate, with neither trusting the other. You offer a solution of bringing a middleman to give the money to, and for the shop to give ukulele to make sure both people have what they say they have. However, the shop does not trust anyone you pick, for fear they are part of an attempted theft. The shop owner offers up a middleman of his own, however you also do not trust this choice, for fear they may be a staff member and not impartial.



Finally, you suggest a different idea: You show the contents of your wallet to every customer in the shop and then they all tell the owner how much money you have in your wallet. Then the owner takes every customer in the shop into the room where the ukuleles are stored, for them to verify whether he actually has ukulele in stock. This means that even if there is a biased thief or employee in the mix, the majority will tell the truth.

> *At least five cryptocurrencies have been hit by '51% attacks'*

The owner agrees and you show everyone the contents of your wallet - you have £0. The cashier takes everyone into the storeroom and they confirm that there are three ukuleles. One customer tells the cashier you have £10 in your wallet, but all the others verify you have £0. The cashier therefore knows not to trust you and that single customer, and avoids a situation of not having a ukulele paid for.

This analogy is much fuller in explaining a blockchain environment. Again, this highlights the technologies core purpose of replacing trust; a blockchain removes the need for a trusted governing middleman.

Every time you use your bank card, the bank tells the cashier that you have enough money to buy the item. This works because everyone trusts the banks. Yet, what if you did not trust the bank? How could you prove to someone that you had enough money? You could use a blockchain.

# Publicly Verifiable

The reason for its name is that every piece of information is contained within a block, that block is then chained to the previous block. This creates a growing chain which cannot be broken. The official technical description of this system is a *public distributed immutable ledger*.

## Public

In the examples above the system works because of the public nature of the information. Every team member is privy to the football information, everyone in the shop got to see both inside your wallet and the ukulele store. Had only one person been trusted then their bias may influence the trust. The more people you ask to verify, the more trustworthy the answer. For instance, if there were only one other customer in the shop, you could go along with two 'thieves' and the majority would be lying.

Technically, this is called a *51% attack*: when you 'own' at least 51% of the involved parties, you rule the majority. In our example, the more people in the shop, the harder it is to own the majority. In the real world, the more public the blockchain, the more secure. At the time of writing, at least five cryptocurrencies have been hit by such attacks. This includes *Ethereum* the second largest cryptocurrency after Bitcoin.

**Distributed**

To distribute responsibility means to share responsibility amongst the many not the few. We distribute the responsibility from a single person to many. No single person has a swaying vote, no single person can influence the information. Every person has equal say.

**Immutable**

Once the majority has decided, that cannot be changed. It can be appended to, but not changed. For instance, in the shop scenario if you were to try again the next day with £10 in your wallet and you polled the shop, they would not say that *'the day before your wallet did not have £0'* instead but they would say that *'today you have £10'.*

Immutability is maintained through process calling hashing. We are not going to unpack that in this article, however you can find plenty of other articles online which breakdown the block contents in more detail.

**Ledger**

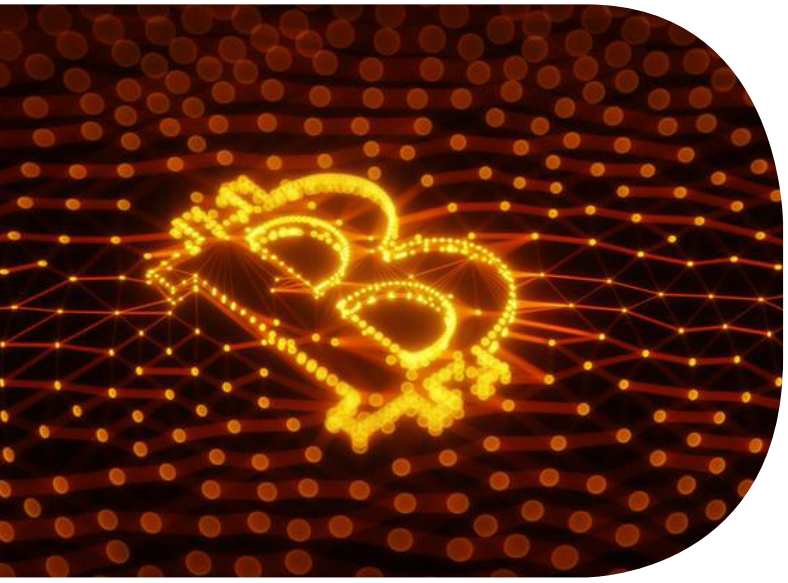
> *... anyone can potentially store anything within a public blockchain, including some more nefarious information.*

This is where the analogies start to fall down, but broadly speaking a ledger in this sense is a historical record of transactions. If you were to transfer anything of value, the record of that transactions is recorded in a ledger.

A ledger is just an event log over time. In a financial sense it records the changes in your bank balance over time, this principle is the same in a digital wallet. In the ukulele shop scenario, if you had £10 and then paid for a ukulele, that transaction would be verified and recoded and your balanced changed. For example, if everyone knew you had £10 in your wallet and then you paid £10 for a ukulele, everyone would then know you have £0. Unlike a financial ledger which only would store financial data, a blockchain ledger can store any kind of data. Furthermore, due to the public nature of the technology anyone

can potentially store anything within a public blockchain, including some more nefarious information. In fact, a German team of researchers have found that within Bitcoin's blockchain contains links to child pornography.

Technically, if you run a Bitcoin node you will inadvertantly be downloading links to child pornography. This is unfortunately one of the perils of buying into a unregulated ecosystem with immutable records.



## How do People Make Money?

Blockchains are like complex mathematical puzzles which get solved to secure each block, a process known as *mining*. In the case of cryptocurrencies you could invest your computational resources to assist in this process and be rewarded with parts of the currency as a result.

Early pioneers who had ammased stocks of Bitcoins got lucky as they traded their Bitcoins for fiat currencies as the value skyrocketed. As the Bitcoin blockchain grows larger, the mining requires more resources to complete. Though the same applies to every other cyrptocurrency, none have had as succsessful take up on the scale of Bitcoin.

Presently, the main ways in which people and businesses are profiting through blockchain is through *mining* the coins to trade; *trading* coins like stocks and shares; or selling computational hardware to *mine* cryptocurrency. However, if you currently have a business which doesn't involve crypto trading, or cryptography it's unlikely your business will be suited or geared towards these ways of making money from blockchain technologies.

## So, does My Business Need It?

The levels of hype for *blockchain* is becoming comparable to level of hype for *the Internet* in the late 90's and early 00's. Consequently, some have predicted that blockchain will be as ubiquitous as the internet in 20 years time. However, there is one factor the Internet has, which blockchain has not: millions of practical applications.

The Internet solved one problem; to communicate anywhere with anyone. This has millions of applications from sport, to entertainment, to jobs, to trade, the list is almost literally endless. The Internet lived up to its hype. However, blockchain has very limited applications and consequently may struggle to live up to its hype at any time.

Due to the hype from Bitcoin, there is a perception – though not based in any reality – the technology itself is valuable and thus if applied to any problem, it will make money. This is simply not true. In fact, a recent study of 43 blockchain use-cases, from a range of companies claiming to reduce operational costs by 90% using blockchain, found little or no evidence of any results. With the exception of Bitcoin, there has been very few – if any – successful blockchain implementations so far.

So, to answer the question, *does your business need to consider blockchain?* Almost certainly not.

*[2] https://mashable.com/2018/03/21/bitcoin-child-pornography/?europe=true*

# Further Reading

**About the Author**

Geraint Harries is a technical manager on the Greater Manchester Cyber Foundry project. Before starting at Lancaster University over 2 years ago, Geraint had worked in software development roles in both IBM and the Civil Service. In addition to being a qualified teacher, Geraint has worked freelance with a varied client base as a software developer and graphic designer.

Lancaster University

**READ MORE**


Forbes. 2019. *A Short History Of Bitcoin And Crypto Currency Everyone Should Read.* [ONLINE] Available at: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#553dbefa3f27 [Accessed 8 July 2019].

CNBC. 2019. *$24 million iced tea company says it's pivoting to the blockchain, and its stock jumps 200%.* [ONLINE] Available at: https://www.cnbc.com/2017/12/21/long-island-iced-tea-micro-cap-adds-blockchain-to-name-and-stock-soars.html [Accessed 8 July 2019].

FINRA. 2019. Don't Fall for Cryptocurrency-Related Stock Scams. [ONLINE] Available at: http://www.finra.org/investors/alerts/dont-fall-cryptocurrency-related-stock-scams [Accessed 8 July 2019].

Coindesk. 2019. Blockchain's Once-Feared 51% Attack Is Now Becoming Regular. [ONLINE] Available at: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular [Accessed 8 July 2019].

Sky News. 2019. Ethereum Classic: Hackers hijack blockchain in rare '51% attack'. [ONLINE] Available at: https://news.sky.com/story/ethereum-classic-hackers-hijack-blockchain-in-rare-51-attack-11601786 [Accessed 8 July 2019].

Merl Tech. 2019. Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps. [ONLINE] Available at: http://merltech.org/blockchain-for-international-development-using-a-learning-agenda-to-address-knowledge-gaps/ [Accessed 8 July 2019]





European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER