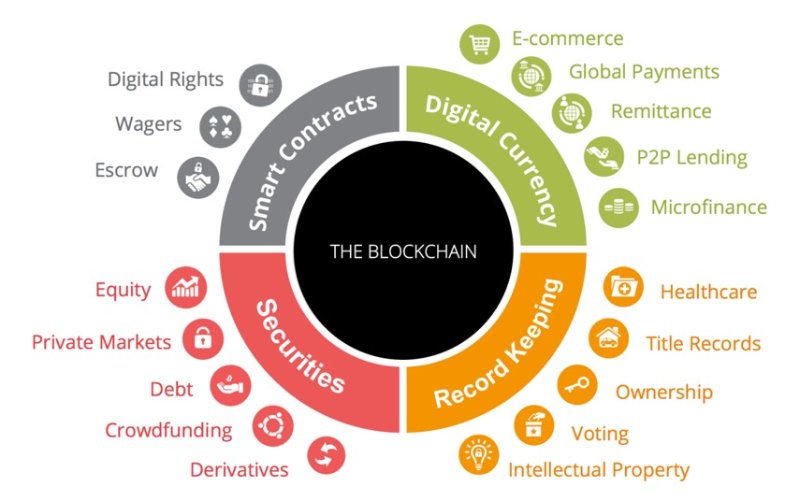
**What is the Blockchain and why is it So Important?**

Source: <https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam/>

Blockchain is growing in importance. Increasingly organisations have to explore what this revolutionary technology will mean for their business. Marc Andreessen from the well-known VC firm Andreessen Horowitz calls it as big an invention as the internet. Last year, in my [Big Data Trends](https://datafloq.com/read/7-big-data-trends-for-2016/1699) prediction for 2016, I already foresaw that 2016 would become the year of the Blockchain and now also Gartner has included in their [Hype Cycle for Emerging Technologies](https://datafloq.com/read/2016-hype-cycle-emerging-technologies-about-data/2243).

Many organisations are already exploring the possibilities of the Blockchain, although primarily still in the Financial Services industry. The R3 Partnership is a consortium of 45 of the biggest financial institutions, investigating what the Blockchain means for them. Next to the R3 consortium, four of the biggest [global banks](http://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147), led by Swiss bank UBS, have developed a “Utility Settlement Coin” (USC), which is the digital counterpart of each of the major currencies backed by central banks. Their objective is to develop a settlement system that processes transactions in (near) real-time instead of days. A third example is [Australia Post](https://delimiter.com.au/2016/08/23/australia-post-plans-blockchain-based-e-voting-system/), who have released plans for developing a blockchain-based e-voting system for the state of Victoria.

The possibilities of the Blockchain are enormous and it seems that almost any industry that deals with some sort of transaction, which would mean any industry, can and will be disrupted by the Blockchain. As a result, it is likely that many of these industries will face job losses since intermediaries will be needed a lot less.

Source: BTCS.com

## How Does the Blockchain Work?

So Blockchain is changing how we do business and will probably also affect our lives. But what is Blockchain and why is it so important? Since I am incorporating the Blockchain in my research for my PhD at UTS, I thought it was a good exercise to try to explain it to you, with the help of a great infographic I came across.

Simply put, the Blockchain is a shared single version of the truth of anything digital. It is a database technology, a distributed ledger that maintains and ever growing list of data records, which are decentralised and impossible to tamper with. The data records, which can be a Bitcoin transaction or a smart contract or anything else for that matter, are combined in so-called blocks. In order to add these blocks to the distributed ledger, the data needs to be validated by 51% of all the computers within the network that have access to the Blockchain.

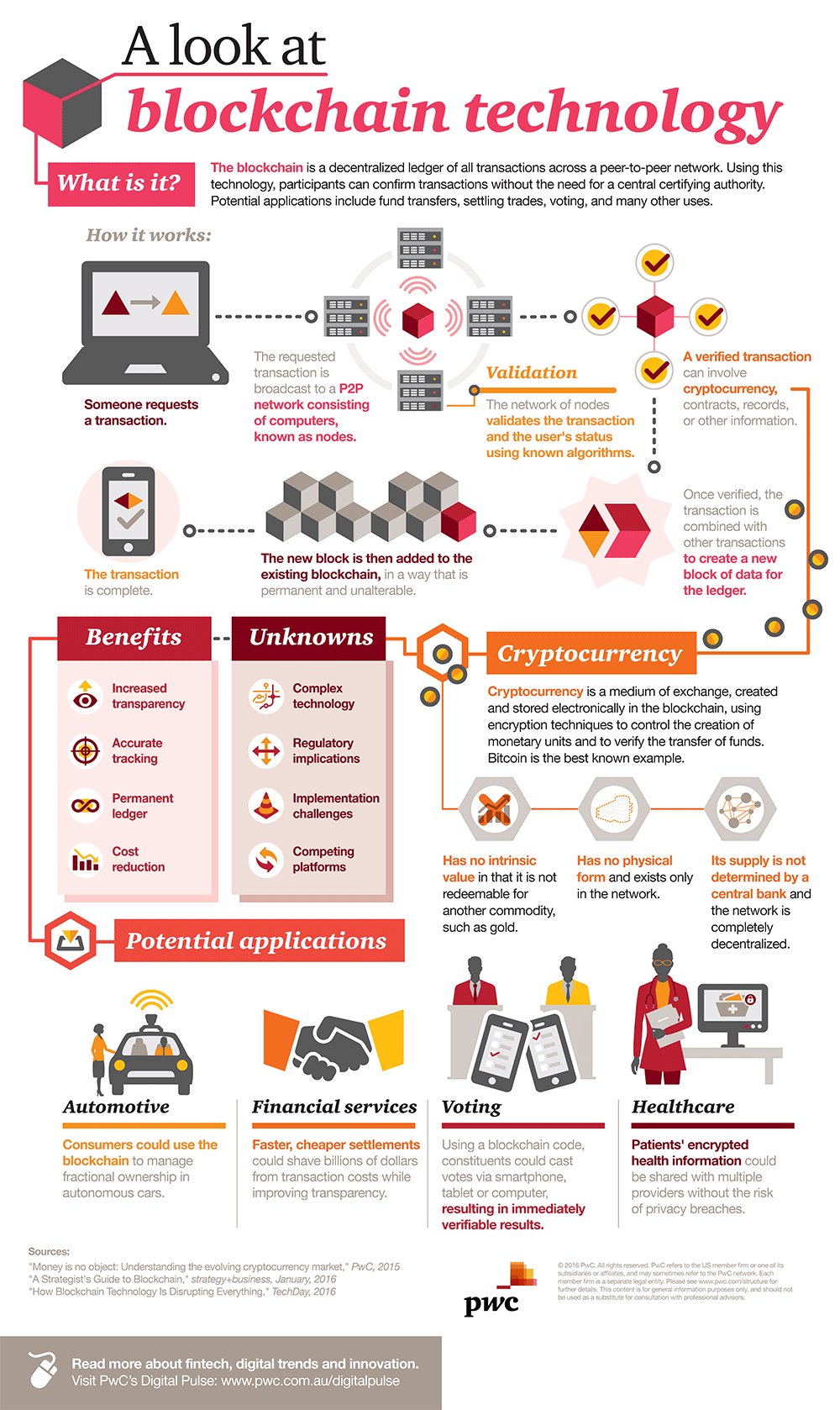
The validation is done via cryptography, which means that a mathematical equation has to be solved. Solving the mathematical equation is difficult and requires a lot of computing power. However, once it is solved it is immediately clear that the answer is correct. This can be compared to a crossword puzzle, which can be very difficult to solve, but once completed you immediately know that it is done correctly.

Once the validation is done, the Block will receive a timestamp and a so-called hash. This hash is then used to create the next block in the chain. If even one bit in the block changes, the hash will change completely and as a result, all subsequent blocks in the chain will change. Such a change has to be validated again by 51% of all the nodes in the network, which will not happen because they don’t have an incentive to work on ‘old’ blocks in the chain. Not only that, the blockchain keeps on growing, so you would require a tremendous amount of computing power to achieve that, which is extremely expensive. So it is simply not worth it to change any data. As a result, it is nearly impossible to change data that has been recorded on the Blockchain.

The result is that peer-to-peer transactions become possible, without the need for a centralised certifying authority, such as a bank, which usually takes a small commission to carry out the work. If third parties are no longer necessary and organisations or consumers can do transactions peer-to-peer, which are also processed nearly instantly, that is a paradigm shift and that’s why the Blockchain is so important.

Of course, there is a lot more to the Blockchain than the brief description I have provided here. There are public and private Blockchains or Permissioned or Permissionless Blockchains. There are a wide variety of applications possible on the Blockchain, ranging from shopping, voting or renting out your house/boat/car/office to reputation systems. There are many different Blockchains ([Bitcoin](https://bitcoin.org/) Blockchain, [Ehtereum](https://www.ethereum.org/" \t "_blank), [Hyperledger](https://www.hyperledger.org/" \t "_blank), etc.) or cryptocurrencies (Bitcoin, Ether, [Steem Dollars](https://steem.io/" \t "_blank), etc.) and marketplaces to trade these cryptocurrencies. I’ll leave that for another [blog post](http://www.linkedin.com/pulse/what-blockchain-part-2-public-vs-private-proof-work-mark-van-rijmenam).

For now, the below infographic made by [PWC](https://www.digitalpulse.pwc.com.au/pwc-blockchain-infographic/), gives a good visual overview of what the Blockchain is and what the benefits are:



# What is the Blockchain – part 2 – Public vs Private, Proof of Work vs Proof of Stake & DApps

For the tech-savvy people among us, the Blockchain might be nothing new and it may be clear that it will have a big impact on the world. However, for many people, the Blockchain is still a mystery, a puzzle or an unknown unknown. Therefore, in a series of posts, I share with you what the Blockchain is, how it works and how it will completely change the world as we know it, if we get it right.

In my first post about the Blockchain, I explained [the basics of the Blockchain](http://datafloq.com/read/what-is-the-blockchain-and-why-is-it-so-important/2270) and in this post I will go a bit deeper and talk about the different types of Blockchains, some examples of dApps and talk about the most important part of the Blockchain; the consensus algorithms to validate the data.

## **Different Types of Blockchains**

The most well-known Blockchain is the Bitcoin Blockchain. The Bitcoin Blockchain was envisioned [by Satoshi Nakamato](http://bitcoin.org/bitcoin.pdf) in 2008 and this is a so-called Permissionless Blockchain, or public Blockchain. This means that anyone interested to join the Blockchain, can do so by simply hooking-up his/her computer to the decentralised Blockchain network, download the Blockchain and contribute to the processing of transactions. It is not required to have a previous relationship with the ledger and you don’t need to be approved to join. If you want to start mining Bitcoin and supporting the Bitcoin network, simply [click here](http://bitcoin.org/en/full-node) and get started. A permissionless Blockchain is not owned by anyone and everyone can contribute.

Next to public, permissionless, Blockchains, there are private, or permissioned, Blockchains. This means that only those that are identified and approved by the Blockchain network, can join the Blockchain and start processing transactions. A private Blockchain is commonly used by a group of companies that want to keep a shared ledger, like for example financial institutions. These Blockchains are owned by an organisation or a group of organisations and you have to be approved if you wish to join. A good example of a private Blockchain is the [Blockchain Settlement System](http://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147) developed by UBS and three other major banks. This Blockchain enables the four participating banks to drastically improve settlement times among them and no other party has access to the Blockchain or can contribute to it.

Private and public Blockchains are the two flavours that have been around and for both options, the main feature of the Blockchain is that once a transaction is approved and on the Blockchain, it cannot be changed or edited. Since this week, however, a third option has been developed. Accenture has patented an “editable Blockchain”, which means that the data in the Blockchain can be adjusted by a central authority. This is a bit of a contradiction since the power of the Blockchain is that data, once validated, cannot be altered. However, Accenture [claims](http://www.reuters.com/article/us-tech-blockchain-accenture-idUSKCN11Q1S2) that this type of Blockchain would only be for private, permissioned, Blockchains used for example by the banks, where a central authority can manage the network under agreed governance rules. It would offer a “safety button” that could, in fact, make the Blockchain more safe to use. If you want to read more about this editable Blockchain, you can read this [article on Forbes](http://fortune.com/2016/09/20/accenture-blockchain/).

## **Proof of Work vs Proof of Stake**

In order to add data to the Blockchain, it needs to be validated and accepted by the network. Validating the data is done using cryptography and via consensus, meaning that 50% +1 of the network need to agree. There are two ways to achieve this consensus, being Proof of Work and Proof of Stake:

### Proof of Work Consensus Algorithm

Proof of Work is used in the Bitcoin Blockchain and it refers to participating users (or nodes) solving difficult mathematical problems to validate the blocks. The node that publishes the solution first, ‘wins’ and receives Bitcoins as a reward. The mathematical problem works like a crossword puzzle; it is difficult to solve, but once it is completed, you instantly know if it is correct. Once accepted by the majority of the network, all the nodes in the network will start working on the next block, thereby repeating the process.

The disadvantage of Proof of Work is its inefficiency in terms of computing power. It requires real-world resources to validate transactions and it requires a lot of it. However, this is also what makes the Blockchain immutable, as it requires a tremendous amount of computing power (a.k.a. as money), meaning 51% of all resources in the Blockchain, to alter transactions.

### Proof of Stake Consensus Algorithm

Proof of Stake solves a major problem of the Proof of Work consensus algorithm, which is the computing power that is required to keep the Blockchain working. The most important difference is that with a Proof of Stake consensus algorithm, the amount of computing power is not the requirement for validation, but the amount of cryptocurrency owned. In order to validate, 51% of the digital currency in the network needs to agree on the current state. As a result, the more digital currency you own, the higher your stake in the success of the Blockchain. The [rationale](http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf) is quite simple; the higher your stake in the system, the higher your incentive to maintain a secure network, because of the pain felt when the reputation and price of the cryptocurrency is damaged due to attacks.

As a result, Proof of Stake requires significant less energy and can be seen as a greener option. The problem, however, with Proof of Stake is, that it becomes easier for a small group of people owning a majority in the currency, to alter the Blockchain. Especially in new Blockchains, where the digital currency is yet to be owned by many people, this can pose a problem.

## **DApps on the Blockchain**

An application on the Blockchain is called a Decentralised Application, or DApp. DApps offer a lot of benefits for the end-user in terms of increased security, transparency and automation of operations thanks to smart contracts. DApps can be a lot cheaper to run, because of the automation, resulting in reduced overhead costs and faster time-to-market once developed. Basically, any application that’s out there, can be turned into a Decentralised Application. When removing a centralised governing body as well as removing as much as governance by management and employees as possible, and instead include governance by code through smart contracts, DApps offer a new way of doing business. In order for a DApp to be a DApp, it needs to have [four characteristics](http://bitcoinmagazine.com/articles/how-decentralized-applications-could-bring-the-blockchain-to-new-industries-1455324259):

1. The code needs to be open-source and any changes to the code must be done via consensus;
2. Data has to be stored on a public Blockchain, to avoid a centralised governing body;
3. There must be a cryptocurrency, or App Coin, to access and use the application;
4. A cryptographic algorithm needs to be in place to ensure either Proof of Work or Proof of Stake.

There are already quite a few examples of DApps, of which Bitcoin is of course the most well-known. To view an extensive list of DApps, here is a list of all known DApps at the moment: [dapps.ethercasts.com](http://dapps.ethercasts.com/). To have a detailed explanation of DApps, please visit [Bitnation](http://blog.bitnation.co/what-are-dapps/" \t "_blank).

## **Changing How the World Works**

The Blockchain, and with it the hundreds of DApps that have already been developed, offer a glimpse of what the future beholds. The Blockchain is still in its early development and a lot of development work is still to be done. However, decentralised applications that are run by smart contracts, without the need for a centralised governing power that generally takes a large commission, offer tremendous advantages. They are cheaper and more efficient to run, more difficult to control by governments or organisations and more secure and transparent than existing applications.