BLOCKCHAIN



Blockchain

Blockchain was the hype of the second half of 2017. Bitcoin, just one of the many 'crypto-currencies', reached a peak of almost 17.000 euros in December 2017. This peak was driven by a hype in the underlying technology. Since then, the bitcoin and most other crypto-currencies with it, lost more than two-third of their value, and there are a lot less publications touting the Blockchain as a the technology of the future.

The hype seems to be over…

Maybe it is time to examine the real value of this technology… if any. Spoiler alert: it is my personal opinion there is, but much less than some claim.

Let's start by explaining what Blockchain is. First remark is that there is no such thing as THE Blockchain. 'Blockchain' is a type of technology of which there are many flavours. Compare it to a 'database' or an 'operating system'.
Depending on your needs, you can choose between the one or the other. For a smartphone, Android is a suitable option whereas a heavy server needs an optimised version of Linux. The same is true for blockchains. Although many of them offer similar functionalities, there are some distinctions. For the users this means that they have to choose one technology over another…

The most commonly used definition of Blockchain you will find is that it is a '*distributed ledger of transactional data*'.

- It is a **ledger**. Blockchain technology records data[1] in a sequential way. This means that once data is recorded, a change to that data is no longer possible, but needs to be made as another transaction. New transactions are added at the end of the ledger. Compare it to a bookkeeping ledger. Once an invoice is made, a correction to it should be made with another entry called a credit note.

- It is **distributed**, there is no central location where all data is kept. Many computers keep a copy of this database, and there are mechanisms in place to keep all these copies synchronised. This makes it is impossible to change the ledger once a transaction is recorded. Another advantage is that the technology is very robust to technological failures of one server.

- It keeps **transaction data**. The strength of the blockchain is that it registers transactions between different parties. In the best suited case these parties have no trusting relation with each other – for instance they both have other interests in the outcome of a transaction.

In order to use the blockchain, it is not necessary to understand its inner workings. It suffices to know that the technology collects 'blocks' of transactions that need to be registered. Once these are collected, a calculation is made to define the uniqueness of the block. The outcome of this calculation is then used as an additional input for the next block. Because of this, all the blocks are linked to each other. If you temper with data in one block, you must also change the data in all other subsequent blocks, or your change will be noticed. This characteristic, together with the fact that the ledger is kept on different servers worldwide, leads to the claim that blockchain is the best and safest available technology to keep an official record of transactions.

Playtime!

For your best understanding, you can play this blockchain simulation game with a group of five people or more (of which one is the facilitator):

1. Let everybody in the group come up with some numbers. These represent the transaction data. The facilitator writes these numbers on a whiteboard or flipchart.

2. After some time, the block is 'closed'. It is now time to calculate the 'hash' of this block. Instead of the complex cryptographic calculations of the real blockchain, we use a 'modulo-97' calculation. This means that we will add all the numbers of the block, divide by 97, and calculate the rest of the equation. Do this by using a basic calculator.

3. The first person that has a result shouts this out to the rest.

4. If this result is confirmed by the rest of the group, this person gets the 'transaction fee', and the block of data is added to the chain.

5. The result of the calculation (the rest of the division) is this first number in the next block, and new numbers can be added.

As you see, there is no way to change one number in the chain without breaking down the calculation. Changing a number will have an effect on the outcome of the hashing calculation (the mod-97 of the sum of numbers). In this simple example, there is a 1 in 97 chance that the result IS the same, but with the cryptographic calculations used in a real blockchain, this chance of getting the same hash is less than the number of atoms on earth.

1 There are some exceptions to this statement in which blockchains are also used to register small snippets of computer code. In order to keep this understandable, I will not elaborate on this.

1. Advantages

The main advantage is what is mentioned in the above characteristics: in the blockchain you can register transactions in such a way that they are indisputable. When you send a message to a business partner, he or she can't deny having received it. Such a message can also be a sending of crypto-currencies, see further in this article.

2. Shortcomings

The biggest shortcoming is that most of the blockchain technologies are not yet ready to deal with large amounts of transactions. Because of the increasing complexity of the hashing calculations, there is a need for very powerful computers. At the moment the energy consumption of the Bitcoin blockchain is already larger than that of several countries like Hungary or New Zealand. This raises questions to the long-term sustainability and scalability. Some other blockchain types have taken this issue into account as of their initial design. It remains to be seen which one of those will prevail.

Secondly, there is the fact that transactions do not happen in real-time as is the case with a credit card payment.

Another shortcoming is one that lies in the strength of the blockchains: transactions can never be forgotten. This is good for certain information – like the registration of how a certain piece of real estate changed owners over the years – but can be detrimental for the use in other types of information. Keeping a penal record on the blockchain would be a nice application, but even the worst offender has the legal rights that his crimes are forgotten a number of years after he served his sentence.

3. Applications

Examples

The fact that there are very few real-life examples of large-scale blockchain use is an indication of the inflated expectations. On the other hand, there are a lot of ongoing proof-of-concepts. An interesting observation is that these pilots are executed in sectors that are traditionally rather conservative like banking and government.

As mentioned above, blockchain technology can be used for transactions between parties which do not have a mutual trust relation. To give a counter example: when a certificate of a clean penal record is given to a job candidate for a potential employer, blockchain has little sense as the employer trusts the government which delivers the document.

I recently heard that when telephone lines, canals or highways were build, builders had no idea what types of goods and services would be transported on them. This was also the case at the emergence of the Internet, and is now the case in the creation of the blockchain. The technology is there, and the application of it is only limited by the imagination of the users.

Architecture

Allow me to go a little bit more technical for one paragraph.

When you want to start a blockchain-project, it is necessary to realise that the blockchain is just the data repository. Like in traditional system architecture, there is not only the 'database', but also a layer with business logic, and a user (or machine) interface. This is important to realize as the value of a blockchain project will be encoded in the layer on top of the ledger. This layer of intelligence can for instance unscramble an encrypted message.

Another possibility is that the hash of a file is saved on the blockchain, but that the file itself remains on another database. When the other party consults the file, his user interface will at the same time consult the file hash to certify the validity of it. This would be a potential solution to sensitive data that should be removable. When it is time to remove the penal record from the earlier example, it suffices to delete the record in question. When it doesn't exist anymore, it mustn't be validated no longer as well. The validation hash that remains on the blockchain has no meaning any longer.

4. Crypto-currencies

The main reason for the media attention on blockchain late last year was the stellar rise of the Bitcoin crypto-currency. The future of crypto-currencies, or crypto's as they are called in the jargon, is hard to predict. Some fierce advocates claim this way of exchanging assets will become the future of payments, others are more sceptical, and think the whole blockchain technology is a passing fad.

The following paragraphs are hence a very personal interpretation, and should by no means be considered as investment or de-investment advice.

What is known at the moment is that the current infrastructure is not scalable enough to implement payments on a large scale. Transaction volumes are too small and the confirmation time of transactions is too long. This makes it impractical to implement the technology for in-store payments. However, there still is a fierce evolution and this issue may well be solved in the future.

This raises another point as to what technology will 'win' the largest market share. As is the case with social networks, there are large network effects. This means that the value of a crypto-currency increases when there are more people or organisations that have their 'wallet' on this blockchain. Currently there are literally hundreds of blockchains claiming they are the best alternative, it remains a gamble which technology will prevail.

However, as described above, there is a real-life value for organisations and individuals in the registration of transaction data on the blockchain. As such, these people will be willing to pay some kind of transaction fee for the service offered. The way blockchains are set up today, is that these transaction fees are paid in the crypto-currency of that blockchain. Some easy exchange from fiat currency to crypto will therefore remain needed. The exchange rate at which this will happen is hard to predict, and will depend on various factors like the speed with which new coins are mined and the future popularity of blockchain.

If we have inspired you, please contact us.



Peter Snoeckx
+32 497 53 35 07
peter.snoeckx@mobius.eu

Möbius Ghent
Kortrijksesteenweg 152
9830 Sint-Martens-Latem
Belgium
+32 9 280 74 20

Möbius Brussels
Rue des Colonies 11
1000 Brussels
Belgium
+32 2 517 60 19

Möbius Utrecht
Atoomweg 50
3542 Utrecht
The Netherlands
+31 030 73 71 197

möbius
business consulting. profoundly different.