What is Blockchain?

Here we are at the start of another new year, we are also told (by the pundits in the media) that we are at the beginning of a new technology that could be as important as the launch of the Internet all those years ago. The technology is something called Blockchain.

Is it really important? Yes.

Is it new? Not really.

The concept of Blockchain started back in 1991 with a group of researchers who came up with a way to digitally time stamp shared documents so they couldn't be backdated for fraudulent purposes. So why is it such a big thing today all of a sudden?

The reason is Bitcoin. Satochi Nakamoto used it as part of his new currency concept in 2009. But in 2017 Bitcoin finally became recognized as another viable currency for the world to accumulate its wealth along with money, gold, buildings, etc. and the rest of the "world" realized that Blockchain technology could be used as a concept to help in other ways besides Bitcoin.

That's the history over, what exactly is Blockchain technology?

I'm sure that most of you reading this will have no interest in the technology behind Blockchain, so I am limiting this paper to give an overview of what it is and how it might be used in the future. From this I hope you will see the possibilities and its implications and how it could affect your own businesses.

As the name suggests Blockchain is a chain of blocks that contain information.

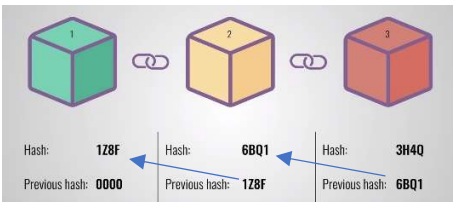
I Have to get just a little technical here to explain the concept. Using Bitcoin as our example, the format of each block is the same containing three parts: -

- Data
- Hash
- Hash of the previous block

The type of data contained in the block chain will vary according to what we want, but in the case of Bitcoin the data contains: -

- From (the sender's details)
- To (the recipient's details)
- Amount of coins in the transaction

The Hash can be compared to a fingerprint and is always a unique code. If anything in the block is changed at any time, the Hash code also changes. If the Hash changes, it is no longer the same block.



The third part of the block is the "Hash of the previous block" and is the link that connects all the blocks in the chain together and makes the chain secure.

The first block in the chain always has a Previous Hash = 000 as there is nothing previous to point to. This is called the Genesis block. If any block Hash is changed then any subsequent blocks cannot find the previous block and the chain is broken.

All sounds good so far?

The problem with this concept (and hacking in general) is that computers are now so powerful that they can make thousands of calculations per second. So, calculating new Hash codes (to validate the blocks in the chain to re-route to a different receiver for example) after the Genesis block, could take a matter of minutes down to a few seconds.

To combat this, Blockchain also uses something called "Proof-of-work". This is a mechanism intended to slow down the generation of new blocks in the chain with a time stamp. This ensures that if one block is tampered with, All the Proof-of-work codes need to be recalculated for every block in the chain and not just the Hash codes.

Blockchain has yet a 3rd level of security to the Hash and Proof-of-work security because it is distributed.

What? Surely that means the system is less secure by being distributed?

Let me explain, Blockchain uses a Peer-to-Peer (P2P) Network which anyone is allowed to join instead of relying on a centralized security system to validate the blocks of information. When someone joins the P2P Network they receive a full copy of the Blockchain. In network speak they are called a "node". When a new Block is generated it is sent out (distributed) to every node on the network and is checked by each node for validation. If everything checks out it is then added to each nodes copy of the Blockchain. The network then agrees a consensus of which Blocks in the chain are valid and which aren't. This means that the higher the number of nodes in a network, the more secure it is. Any Blocks identified as to have been tampered with are then rejected by everyone within the network.

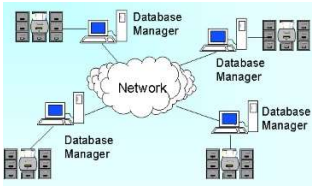
To successfully tamper and change a Blockchain you will need to update all the blocks in the chain, redo the Proof-of-work for each block and take control of more than 50% of the P2P Network. Only then will everyone accept a transaction that has been tampered with. This is almost impossible for anyone to do.

Remember that Blockchains are still in their infancy and continue to evolve. People are now beginning to think about how else this technology can be used. So far we have Bitcoin, but watch out for: -

- Other currency transactions
- Sharing Medical records
- Collecting taxes

Great, but that still doesn't affect my business I hear you cry. Well think about this.

At the moment we all use databases and they are currently held on a central server (I'm ignoring the cloud at the moment to keep things simple and introduce you to concepts). Because the database is crucial to our business, we surround them with a lot of security. But what would happen if they got corrupted for any reason? We have a backup – but this will only be as good as when the last backup was made and there is bound to be some data missing.



But what if the database is a blockchain? Every user, every computer, every node on the network has an exact duplicate copy of the database on their computer as a blockchain. There can be two, three, hundreds, thousands of nodes on a network anywhere in the world and all have got the same copy of the information on their computer as a secure Blockchain. In our example, if one or two copies of the database become corrupted, it wouldn't make any difference to anyone else in the network.

Now isn't that getting you thinking?

Ian Shufflebotham is a senior consultant of Total Business Solutions Inc. that partners clients with *Window Manufacturing software, ERP Solutions and Cyber Security*. Telephone : (UK) +44 07870 904144, (Canada) +1 416-508-7992, *or through our website at* http://www.total-biz.net