Bitcoin made easy

Bitcoin: Is it real, will it last, is it safe, what is it?

Bitcoin is the invention of one Satoshi Nakamoto, whose true identity is still somewhat in doubt. In 2008/9 he posted the design on the internet, together with the software to coordinate it. His aim was for people to feel secure and safe about exchange money online without the services and interference a third party like banks governments. In short, the internet currency had to be as good as cash.

Surprisingly most internet dwellers have never even heard the word Bitcoin. Not knowing myself I googled it, but the more I read, the more it confused me and so my resolve to solve this puzzle in layman's terms.

The first thing I learned was that a Bitcoin was 'An experimental, decentralized, digital Cryptocurrency that enables instant payments to anyone, anywhere in the world. It uses peer-to-peer technology to operate, with no central authority. The transaction management and issuing of money is carried out collectively by the network.

Now isn't that just too plain and simple.

A guy by the name of Tom Peters once said: "If you're not confused, you're not paying attention".

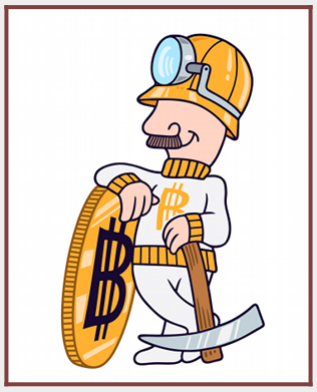
What on earth is Cryptocurrency, or for that matter digital currency?

The value of any item is determined by its demand and its practical use. The value of gold will for instance never drop to $0.00, even if the world financial markets crash. Gold has more than a monetary value. It can be used to make jewellery etc. Your house will similarly always retain some value because its main purpose is to be a roof over your head, something you will always have a need for.

The value of a Bitcoin is determined solely by the demand and need for an online currency with which to buy and sell, similar to cash. It has no other practical value and at a glance it's difficult to understand

how it can maintain its value when there's nothing to back or support it.

To understand Bitcoin you need to forget all about how conventional money works. It is not a coin or paper shaped article with a value written on it.



So how does it all happen? The Bitcoin software includes a special computerized technique that creates very complex mathematical problems on the network of servers stemming from ***anyone*** who wishes to become a miner of Bitcoins. The search for the answers to these complex riddles is known as **mining**. Anyone can mine for Bitcoins by using a computer with a high speed graphic card and special mining software. The complex mathematical formula generates a 64 digit number, and 'cracking' this algorithm (known as hashing) generates a bitcoin with its own unique number and also entitles the miner to 50 bitcoins as a reward. Hashing is the transformation of a string of numerals or letters into values of shorter length that represents the original string.

As already explained, the value of the Bitcoin lies in its need (demand) for an online currency. To ensure that the demand for Bitcoins remains high, Satoshi Nakamoto stipulates in his rules that only 21 million coins should ever be created and that new coins must be produced at an ever decreasing rate until the target is reached. It is estimated that the 20 million mark will be reached in about 2030. The system must thus controls the number of Bitcoins that are allowed to be 'mined' every year. If the deviation from the rate that the network needs coins to be produced is to big, the difficulty level of the mathematical problems is moved up or down in order to maintain the required quota. The current Bitcoin quota is 50 every 10 minutes.

Every individual computer ***on the network*** runs a software program that keeps track of ALL Bitcoin transactions ever made. For example when someone buys bitcoins or pays for something online there is a process by which the validity of the bitcoins used in the transaction are verified. This public log is collectively maintained by every 'miner' and contains all the information needed to validate (certify) every Bitcoin transaction that takes place. The system is so geared that

riddles for new Bitcoins will only be generated and released to a miner if he fulfills his obligation of validating transactions. The system thus monitors itself.

Understandably that's a lot of on-going, ever changing activity with the result that mining has become a major internet industry. Solving the riddles is extremely complicated. Individual miners are a thing of the past and they are now pooling their efforts.

Bitcoin Denominations

A Bitcoin can be divided into 8 decimals. 0.00000001 BTC is currently the smallest amount possible and is aptly named the 'Satoshi' in honour of Satoshi Nakamoto the pseudonym of the inventor of Bitcoin.

Coins can be obtained in 1 of 3 ways:

1. You can mine them
2. You can buy them
3. You can earn them

Most people's involvement with Bitcoins is simply to transact online and the easiest option is therefor to buy coins. For that you need a Bitcoin Wallet. Your wallet is what allows you to transact online and it is where you store your Bitcoin addresses that you need to send and receive coins and have transactions validated. All wallets are compatible and just like emails your wallet and addresses are fully functional even though you are off line.

So the next question – what is a Bitcoin address? It's exactly what it says. Just like an email address is needed to send and receive emails, a Bitcoin address is needed to send and receive Bitcoins. Bitcoin addresses are between 27 & 34 characters. The number includes 'checksums' so it is impossible to present a wrong number by accident. A Typical number will look as follows:

31sAAFguRuphBVTewXYtYbMv5Tndxhfrkn

Every Bitcoin address (not the wallet) has a matching private key which is a secret piece of data that proves your right to spend the bitcoins you have received from another specific Bitcoin address. The private key is mathematically related to the Bitcoin address, and is designed so that the Bitcoin address can be calculated from the private key, but importantly, the same cannot be done in reverse. It is also needed to create the transactions to spend the funds sent to the address. If the private key is lost (your drive crashes) all Bitcoins linked to that number are lost forever, no exceptions.
Only the user with the private key can sign a transaction to give some of their bitcoins to somebody else. Every user also has a public key attached to the public log (referred to earlier on) through which anyone can validate the signature.

Lets take an example:

• Mr. X owes you money and so you send him your Bitcoin address to which your public key is attached.
• Mr. X sends the instruction message and attaches the Bitcoins and your public key.
• Mr. X signs the transaction with his private key and broadcasts the agreement on the Bitcoin network for all to see. This last step is automatically done by the Bitcoin clients software that is downloaded when you open your wallet.
Anyone checking is able to see that the message is authentic. The complete history of transactions kept on the public log makes it possible for anyone to verify who is the current owner of any particular group of coins. They can see that Mr. X has personally agreed to transfer the coins to you. Only Mr. X knows his private key, unless he was foolish enough to give it to someone else.

To set your mind at ease, it is impossible to work out someone's Private key by using his public key.

Ok, summing up. Do bitcoins qualify as a **cryptocurrency?** Let's check:

1. It's a 'currency' where whoever possesses it owns it
2. The owner is anonymous and no records are kept as to who the owner

is.
3. It does not have physical properties and if lost or stolen it’s GONE ! !
4. It is based on trust and it’s value is determined by supply and demand.
5. It is not attached to any country or bank i.e. no middle man.
6. It’s a peer to peer currency i.e. created by people and not a bank.
7. It has its origin in cryptography using mathematical properties.

What is cryptography? – The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

There you have it. You are now a fairly knowledgeable Bitcoin creature, but there’s still lots more to learn if for some reason you decide you want to be a Bitcoin digital cryptocurrency guru.

Till next time!

Steve