WHAT IS BITCOIN AND HOW DOES IT WORK?

Bitcoin has been a bit of a buzzword in the news in the last couple of years, and is being widely talked about in technology and finance circles as a possible future alternative to normal currency. So what is it?

Bitcoin is a digital money system that allows people to send or receive financial transactions across the internet, with no requirement for traditional money. Your "normal" money can be converted into Bitcoin without it being linked to a real-world identity. The Bitcoin system does not keep track of the people who use it, it only keeps track of the addresses where the money is.

A Bitcoin address is a digital identifier, much like an IP address, that consists of 26 – 35 alphanumeric characters, normally beginning with the number 1 or 3. This identifier represents the destination for a Bitcoin payment. These digital addresses can be generated at no cost, by any user, at any time, using an account at a Bitcoin exchange or an online wallet service. The addresses are kept secure using the science of cryptography, which is essentially the maths behind secure communication on the internet.

Each Bitcoin address has two very important pieces of information, referred to as keys – a public key and a private key. The public key, which comes from the Bitcoin address mentioned above, is much the same as an email address – anyone can look it up and send Bitcoin to it. The private key, which you could consider similar to a password, is required for the owner to send Bitcoins from that address. It is essential that this key is kept secret otherwise anyone would be able to empty your account and send your money to themselves.

Bitcoin is not as anonymous as is widely reported. Websites or users using the Bitcoin system must go through a global database called the Blockchain. The Blockchain is a record of all Bitcoin transactions, almost like a public ledger that keeps track of everything that has ever taken place in the Bitcoin network. So while there is no obvious link between yourself and your digital Bitcoin address, every transaction to and from that address is publically available.

To purchase a Bitcoin, you first sign up to an online Bitcoin exchange. The exchange facilitates the conversion of your "real" bank account balance into electronic Bitcoin. You can then send your Bitcoin to an online wallet, which is used to keep track of your Bitcoin address, and your public and private keys. You then use the wallet to process transactions to and from whoever you please.

To generate a Bitcoin, a maths problem must be solved and the resulting solution is the Bitcoin. The difficulty of the maths problem depends on the number of people who are buying and selling Bitcoin at that particular moment versus the solution to the previous puzzle. Due to the complexity of the problems, the calculations are not solvable with a human brain and computers with very powerful processors are required. This process is called mining and the people who do it are called miners. Miners usually work together in groups to solve the puzzles and the first miner or group of miners who solve that particular puzzle is rewarded with new Bitcoin currency.

Due to the method of mathematics that Bitcoin uses, there is a finite amount of them, they are not endless. One of the main problems with the traditional money system is that whoever is in charge of the supply can simply print more blocks of cash, thus decreasing the value of the cash already in circulation and methodically driving up inflation. Bitcoin uses a more ethical approach, although this doesn't make their value any less volatile.