BITCOIN

02/01/2018

BITCOIN

Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like dollars or Euros – they're produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems.

It's the first example of a growing category of money known as cryptocurrency.

Bitcoin can be used to buy things electronically. In that sense, it's like conventional dollars, Euros, or yen, which are also traded digitally.

However, Bitcoins most important characteristic, and the thing that makes it different to conventional money, is that it is *decentralized*. No single institution controls the Bitcoin network. This puts some people at ease, because it means that a large bank can't control their money.

This currency isn't physically printed in the shadows by a central bank, unaccountable to the population, and making its own rules. Those banks can simply produce more money to cover the national debt, thus devaluing their currency.

Instead, Bitcoin is created digitally, by a community of people that anyone can join. Bitcoins are 'mined', using computing power in a distributed network. This network also processes transactions made with the virtual currency, effectively making Bitcoin its own payment network.

The Bitcoin protocol – the rules that make Bitcoin work – say that only 21 million Bitcoins can ever be created by miners. However, these coins can be divided into smaller parts (the smallest divisible amount is one hundred millionth of a Bitcoin and is called a 'Satoshi', after the founder of Bitcoin).

Conventional currency has been based on gold or silver. Theoretically, you knew that if you handed over a dollar at the bank, you could get some gold back (although this didn't actually work in practice). But Bitcoin isn't based on gold; it's based on mathematics.
Around the world, people are using software programs that follow a mathematical formula to produce Bitcoins. The mathematical formula is freely available, so that anyone can check it.

The software is also open source, meaning that anyone can look at it to make sure that it does what it is supposed to.

BITCOIN

Bitcoin has several important features that set it apart from government-backed currencies.

1. It's decentralized
The Bitcoin network isn't controlled by one central authority. Every machine that mines Bitcoin and processes transactions makes up a part of the network, and the machines work together. That means that, in theory, one central authority can't tinker with monetary policy and cause a meltdown – or simply decide to take people's Bitcoins away from them, as the Central European Bank decided to do in Cyprus in early 2013. And if some part of the network goes offline for some reason, the money keeps on flowing.

2. It's easy to set up
Conventional banks make you jump through hoops simply to open a bank account. Setting up merchant accounts for payment is another Kafkaesque task, beset by bureaucracy. However, you can set up a Bitcoin address in seconds, no questions asked, and with no fees payable.

3. It's anonymous
Well, kind of. Users can hold multiple Bitcoin addresses, and they aren't linked to names, addresses, or other personally identifying information. However…

4. It's completely transparent
Bitcoin stores details of every single transaction that ever happened in the network in a huge version of a general ledger, called the **blockchain**.
The blockchain tells all.

If you have a publicly used Bitcoin address, anyone can tell how many Bitcoins are stored at that address. They just don't know that it's yours.
There are measures that people can take to make their activities more opaque on the Bitcoin network, though, such as not using the same Bitcoin addresses consistently, and not transferring lots of Bitcoin to a single address.

***5.* Transaction fees are miniscule**
Your bank may charge you a £10 fee for international transfers. Bitcoin doesn't.

6. It's fast
You can send money anywhere and it will arrive minutes later, as soon as the Bitcoin network processes the payment.

BITCOIN MINING

In traditional fiat money systems, governments simply print more money when they need to. But in Bitcoin, money isn't printed at all – it is discovered. Computers around the world 'mine' for coins by competing with each other.

How does mining take place?

People are sending Bitcoins to each other over the Bitcoin network all the time, but unless someone keeps a record of all these transactions, no-one would be able to keep track of who had paid what. The Bitcoin network deals with this by collecting all of the transactions made during a set period into a list, called a block. It's the miners' job to confirm those transactions, and write them into a general ledger.

Making a hash of it

This general ledger is a long list of blocks, known as the 'blockchain'. It can be used to explore any transaction made between any Bitcoin addresses, at any point on the network. Whenever a new block of transactions is created, it is added to the blockchain, creating an increasingly lengthy list of all the transactions that ever took place on the Bitcoin network. A constantly updated copy of the block is given to everyone who participates, so that they know what is going on.

But a general ledger has to be trusted, and all of this is held digitally. How can we be sure that the blockchain stays intact, and is never tampered with? This is where the miners come in. When a block of transactions is created, miners put it through a process. They take the information in the block, and apply a mathematical formula to it, turning it into something else. That something else is a far shorter, seemingly random sequence of letters and numbers known as a hash. This hash is stored along with the block, at the end of the blockchain at that point in time.

Hashes have some interesting properties. It's easy to produce a hash from a collection of data like a Bitcoin block, but it's practically impossible to work out what the data was just by looking at the hash. And while it is very easy to produce a hash from a large amount of data, each hash is unique. If you change just one character in a Bitcoin block, its hash will change completely. Miners don't just use the transactions in a block to generate a hash. Some other pieces of data are used too. One of these pieces of data is the hash of the last block stored in the blockchain.

Because each block's hash is produced using the hash of the block before it, it becomes a digital version of a wax seal. It confirms that this block – and every block after it – is legitimate, because if you tampered with it, everyone would know.

If you tried to fake a transaction by changing a block that had already been stored in the blockchain, that block's hash would change. If someone checked the block's authenticity by running the hashing function on it, they'd find that the hash was different from the one already stored along with that block in the blockchain. The block would be instantly spotted as a fake.

Because each block's hash is used to help produce the hash of the next block in the chain, tampering with a block would also make the subsequent block's hash wrong too. That would continue all the way down the chain, throwing everything out of whack.

BITCOIN MINING

Competing for coins

So, that's how miners 'seal off' a block. They all compete with each other to do this, using software written specifically to mine blocks. Every time someone successfully creates a hash, they get a reward of 25 Bitcoins, the blockchain is updated, and everyone on the network hears about it. That's the incentive to keep mining, and keep the transactions working.

The problem is that it's very easy to produce a hash from a collection of data. Computers are really good at this. The Bitcoin network has to make it more difficult, otherwise everyone would be hashing hundreds of transaction blocks each second, and all of the Bitcoins would be mined in minutes. The Bitcoin protocol deliberately makes it more difficult, by introducing something called 'proof of work'.

The Bitcoin protocol won't just accept any old hash. It demands that a block's hash has to look a certain way; it must have a certain number of zeroes at the start. There's no way of telling what a hash is going to look like before you produce it, and as soon as you include a new piece of data in the mix, the hash will be totally different.

Miners aren't supposed to meddle with the transaction data in a block, but they must change the data they're using to create a different hash. They do this using another, random piece of data called a 'nonce'. This is used with the transaction data to create a hash. If the hash doesn't fit the required format, the nonce is changed, and the whole thing is hashed again. It can take many attempts to find a nonce that works, and all the miners in the network are trying to do it at the same time. That's how miners earn their Bitcoins.

BITCOIN TRANSACTIONS

Bitcoin transactions are sent from and to electronic Bitcoin wallets, and are digitally signed for security. Everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the Bitcoins were produced.

Holding onto Bitcoins is great if you're a speculator waiting for the price to go up, but the whole point of this currency is to spend it, right? So, when spending Bitcoins, how do transactions work?

There are no Bitcoins, only records of Bitcoin transactions

Here's the funny thing about Bitcoins: they don't exist anywhere, even on a hard drive. We talk about someone having Bitcoins, but when you look at a particular Bitcoin address, there are no digital Bitcoins held in it, in the same way that you might hold pounds or dollars in a bank account. You cannot point to a physical object, or even a digital file, and say "this is a Bitcoin".

Instead, there are only records of transactions between different addresses, with balances that increase and decrease. Every transaction that ever took place is stored in a vast public ledger called the block chain. If you want to work out the balance of any Bitcoin address, the information isn't held at that address; you must reconstruct it by looking at the blockchain.

What does a transaction look like?

If Alice sends some Bitcoins to Bob, that transaction will have three pieces of information:

•An input. This is a record of which Bitcoin address was used to send the Bitcoins to Alice in the first place (she received them from her friend, Eve).
•An amount. This is the amount of Bitcoins that Alice is sending to Bob.
•An output. This is Bob's Bitcoin address.

How is it sent?

To send Bitcoins, you need two things: a Bitcoin address and a private key. A Bitcoin address is generated randomly, and is simply a sequence of letters and numbers. The private key is another sequence of letters and numbers, but unlike your Bitcoin address, this is kept secret.

Think of your Bitcoin address as a safe deposit box with a glass front. Everyone knows what is in it, but only the private key can unlock it to take things out or put things in.

When Alice wants to send Bitcoins to Bob, she uses her private key to sign a message with the input (the source transaction(s) of the coins), amount, and output (Bob's address).

She then sends them from her Bitcoin wallet out to the wider Bitcoin network. From there, Bitcoin miners verify the transaction, putting it into a transaction block and eventually solving it.

BITCOIN TRANSACTIONS

Why must I sometimes wait for my transaction to clear?
Because your transaction must be verified by miners, you are sometimes forced to wait until they have finished mining. The Bitcoin protocol is set so that each block takes roughly 10 minutes to mine.

Some merchants may make you wait until this block has been confirmed, meaning that you may have to make a cup of coffee and come back again in a short while before you can download the digital goods or take advantage of the paid service.

On the other hand, some merchants won't make you wait until the transaction has been confirmed. They effectively take a chance on you, assuming that you won't try and spend the same Bitcoins somewhere else before the transaction confirms. This often happens for low value transactions, where the risk of fraud isn't as great.

What if the input and output amounts don't match?
Because Bitcoins exist only as records of transactions, you can end up with many different transactions tied to a particular Bitcoin address. Perhaps Jane sent Alice two Bitcoins, Philip sent her three Bitcoins and Eve sent her a single Bitcoin, all as separate transactions at separate times.

These are not automatically combined in Alice's wallet to make one file containing six Bitcoins. They simply sit there as different transaction records.

When Alice wants to send Bitcoins to Bob, her wallet will try to use transaction records with different amounts that add up to the number of Bitcoins that she wants to send Bob.

The chances are that when Alice wants to send Bitcoins to Bob, she won't have exactly the right number of Bitcoins from other transactions. Perhaps she only wants to send 1.5 BTC to Bob.

None of the transactions that she has in her Bitcoin address are for that amount, and none of them add up to that amount when combined. Alice can't just split a transaction into smaller amounts. You can only spend the whole output of a transaction, rather than breaking it up into smaller amounts.

Instead, she will have to send one of the incoming transactions, and then the rest of the Bitcoins will be returned to her as change.

Alice sends the two Bitcoins that she got from Jane to Bob. Jane is the input, and Bob is the output. But the amount is only 1.5 BTC, because that is all she wants to send. So, her wallet automatically creates two outputs for her transaction: 1.5 BTC to Bob, and 0.5 BTC to a new address, which it created for Alice to hold her change from Bob.

BITCOIN TRANSACTIONS

Are there any transaction fees?
Sometimes, but not all the time.

Transaction fees are calculated using various factors. Some wallets let you set transaction fees manually. Any portion of a transaction that isn't picked up by the recipient or returned as change is considered a fee. This then goes to the miner lucky enough to solve the transaction block as an extra reward.

Right now, many miners process transactions for no fees. As the block reward for Bitcoins decreases, this will be less likely.

One of the frustrating things about transaction fees in the past was that the calculation of those fees was complex and arcane. It has been the result of several updates to the protocol, and has developed organically.

Updates to the core software handling Bitcoin transactions will see it change the way that it handles transaction fees, instead estimating the lowest fee that will be accepted.

Can you trade Bitcoin instead of owning it?
Of course. Just like currencies and equity markets, Bitcoin is available to buy or sell via various exchanges. On these exchanges you are able to buy and sell Bitcoin as well as multiple other crypto currencies just as you would a normal FX Currency pair such as EURUSD.

Exchanges:

- GDAX
- POLONIEX
- BitMEX
- BITFINEX
- BITSTAMP

These exchanges can be used just like your normal trading platforms provided by your brokers such as IG Markets and Interactive Brokers.

Information obtained from CoinDesk

DISCLAIMER

This report is for research and educational purposes only and the opinions expressed throughout are of Toroso. We do not have a crystal ball that sees into the future therefore our opinions are pure calculated speculations which on occasion will be wrong resulting in losses due to the market being unpredictable.

02/01/2018