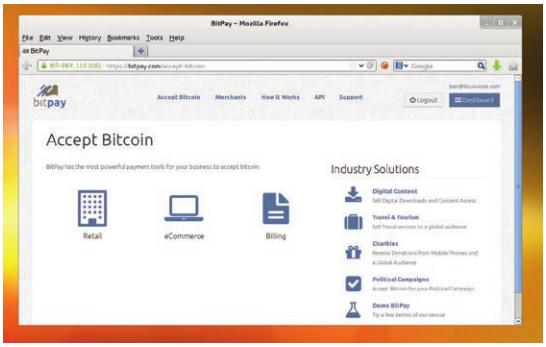
bitcoin

What in the name of Zeus is it?

Bitcoin is a digital currency that became popular in 2013. It's not controlled by governments, banks, or anyone. It's a decentralised currency designed to free our money from those who would oppress us. But how does a digital currency work? How can it be valid if there's no one to say who has what?
Ben Everard investigates.



Sellers can receive money in Bitcoin without having to deal with the currency itself, using services such as BitPay (www.bitpay.com).

There are, roughly speaking, three parts to Bitcoin: the block chain, mining network, and wallets. In order to understand how Bitcoin works, you have to understand how each of these works. Make a cup of tea and settle in.

The block chain is a list of every single Bitcoin transaction that's ever taken place. Until a transaction is on the block chain, it hasn't happened. It is quite literally a chain of blocks – each block is a list of new transactions, and a link back to the previous block. Anyone can then validate the block chain by following it all the way back to the very first transaction when Satoshi Nakamoto created the first Bitcoins.

At this point, you're probably wondering who's responsible for keeping the block chain. The scary answer is: no one. There is no single organisation or person that holds a definitive copy of the block chain. Bitcoin is built to be distributed, so there's no point of failure that could maliciously or accidentally corrupt the block chain. Instead, the block chain is held separately by every single computer mining Bitcoins.

Where there's silicon, there's brass

These miners, then, are both the custodians of the old transactions, and the ones responsible for making sure new transactions are added. Their job is to create (or 'mine') new blocks. These new blocks contain any new transactions that have taken place. In compensation for mining these new blocks, they're rewarded with some Bitcoins. This acts as an incentive to make sure enough people keep mining to keep the network working.

That brings us to wallets. This is the part of Bitcoin that regular users see. The term wallet is a bit of a misnomer, since they don't actually store Bitcoins at all -- Bitcoins are stored only as a record of transactions in the block chain. The wallets store a private key that authorises the user to add transactions to the block chain for a given address (which is the public key that corresponds to the private key).

> **"The term 'wallet' is a bit of a misnomer, since they don't actually store Bitcoins at all."**

HASHTAG

Hashing – sometimes known as one-way encryption – is a method for changing something in one way that can't be reversed, but can be verified. Take for example a very simple hashing operator: modulo 10. In this, you divide something by ten and the remainder is the hash – for example, 45 hashes to 5.

There are two crucial functions about the hash. The first is that it's easy to verify. Every time you do it, it's quick and you get the same result. The second is that you can't reverse it. If someone tells you that the hash is 5, it's impossible to work out that they started with 45.

However, modulo 10 is a bad hashing algorithm because it's easy to find something else that hashes to the same value. A good hash has both of the first two properties, but make it impossible to predict how the output will changed from a change in the input. A slight change in the input should result in a drastic change in the output.

Hashes are used frequently in computer security. For example, it's how passwords are stored on Linux systems. The passwords themselves are never store; instead, their hashes are. You can see them if you type:

```
sudo cat /etc/shadow
```

Every time you log in, your computer hashes the password you type and compares the result to these stored hashes. If the two hashes match, then it logs you in. The fact that you can see every hash on the system (if you have superuser privileges) doesn't make this any less secure because it's so hard to reverse these hashes. In fact, it's only really possible if you can guess what the hashes might be (by checking with a list of dictionary words, for example).

In Bitcoin, hashes are used both to verify the integrity of the block chain, and in the proof-of-work (see the boxout below). They work in the block chain by proving that none of the blocks have been edited since they were first mined.

HASHCASH

Hashcash is the proof-of-work system that miners use to verify that they have actually mined a block before it can be included in the block chain. The basic function of this is to make it computationally unfeasible to alter the block chain, because anyone seeking to alter a transaction would have to recalculate all the proof of works until they had a block chain longer than the previous one.

It relies on hashing (see other boxout), specifically the SHA256 hash function. This takes an input and outputs a 256-bit number. The inputs to the hash function are the block header (which contains a counter) and a hash of all the transactions. The task of the miner is to find a value for the counter where the output of the hash function is below a certain threshold. This threshold corresponds to the current difficulty setting, which changes every 2016 blocks.

The only way to calculate this is with pure computing power. You have to generate as many hashes as possible with different values for the counter and hope that one of them comes up with a hash below the set value. The faster you can generate hashes, the more likely you are to find one that satisfies this requirement. If you do come across a hash like this, then you have mined that block and you can transmit it to all the other miners in the network.

The rate at which miners are trying different hashes is used to show the current speed of the network or the power of a particular Bitcoin-mining computer (usually measured in billions of hashes per second GHs)

Miners don't have to worry about their proof-of-work being copied because, it includes a hash of all the transactions (in something called a Merkle Tree), and one of these transactions is the miner paying themselves for mining the block. Anyone copying the proof-of-work can't alter this without changing the resulting hash.

Note that the hashcash algorithm used in Bitcoin is slightly different from the hashcash algorithm used to prevent email spam, though they both work in the same general way.

MAKING A TRANSACTION

When you make a Bitcoin transaction, you transmit it to the network of miners. However, there has to be some security to ensure that someone else can't make transactions from your wallet without you knowing.

Bitcoin transactions take place between two (or more) wallets. These, as we said before, are simply a public/private key pair and are used to encrypt data. They work in such a way that any data encrypted with the public key can be read with the private key, and vice versa.

In Bitcoin, you don't have a pool of money that goes up and down like a bank account. Instead, you have a specific set of Bitcoins that can each be chained all the way back to their original miner. When you make a transaction, you have to reference the transaction in which you got them (you can reference more than one). You then have to digitally sign each referenced transaction. This means that you hash the details of the transaction and encrypt them with your private key. Since your public key is tied to your address (and therefore tied to the referenced transaction), this confirms that you are authorised to make the transaction. The transaction also includes the output address to which they are being sent.

(This is a bit of a simplification. See **https://en.bitcoin.it/wiki/Transactions** for a more complete explanation.)

Notice that nothing physically leaves your wallet other than this message to the block chain. The amount of Bitcoins in a wallet is calculated by seeing all the transactions in the block chain. This means that anyone can know how much is in any wallet at any one time. It doesn't necessarily mean they know who has how much money since it's not always possible to tie a specific wallet to a specific person, or know how many wallets a person has.

Once this transaction goes to the miners, it's added to the next block. However, as we've seen, the block chain can split (and a malicious miner with a lot of computing power could split it deliberately). There is no one point when it's guaranteed to always be in the block chain, but the assurance is calculated by the number of blocks built on top of it. If it's just one, then a lucky attacker may be able to outrace the rest of the mining network. However, with each subsequent block that's added to the block chain, the amount of work an attacker would have to do to reverse the transaction increases.

A depth of six blocks is usually considered enough to be sure that a transaction is properly added to the block chain. At a block rate of one every ten minutes, this is an hour. For high-value transactions, you may wish to wait for more blocks before considering the money truly transferred.

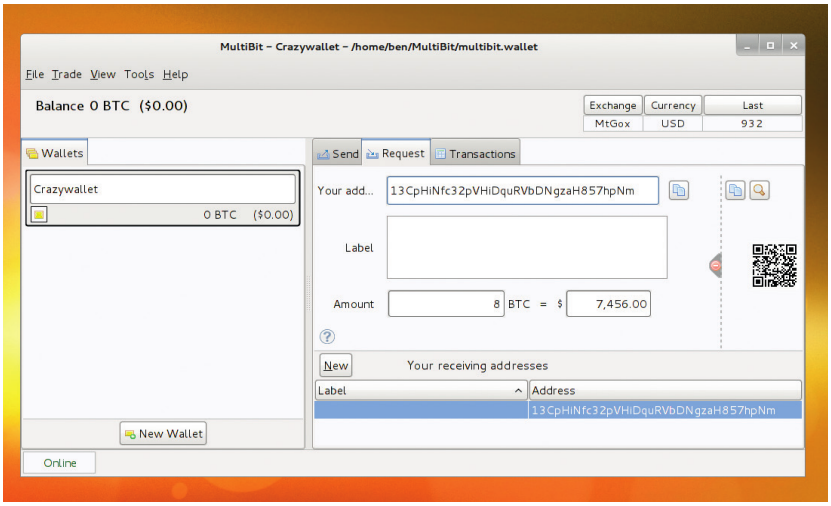
The previous four paragraphs have given a basic overview of how Bitcoins work, and you could quite easily go about using or mining Bitcoins using only this knowledge. However, the chances are that you wouldn't trust the currency, since it sounds suspiciously like it would be easy somehow to corrupt the system and defraud users. The beauty of the currency is in the cryptographic techniques that protect users. Let's go back and look at in more detail to see how this works.

> **"The beauty of Bitcoin is in the cryptographic techniques that protect the users."**

A huge part of the security of Bitcoin comes from hashing, and it's these hashes that are used to link blocks together in the block chain. Each block contains a hash of the previous block, and this can't be changed without altering the current block's hash (which will be included in the next block). Anyone can go and check that none of the transactions have been changed at any point. If they had, the hashes would no longer match up.

The block chain is a publicly verifiable record of every transaction that's ever taken place. Each time you perform a transaction, details of that transaction are propagated to all the miners on the bitcoin network with a request to include it in the next block.

For a miner to get paid for mining a block two things have to happen: they have to solve the



Multibit has all the usual wallet functions and can create QR codes to help someone send you money. These include the receiving wallet address and the number of Bitcoins.

SATOSHI NAKAMOTO

Bitcoin has become a household name, and the currency is worth billions of pounds, but for all that fame, one thing still remains secret: the identity of the creator. They're known only by the pseudonym Satoshi Nakamoto. It's not known for sure if Satoshi is male or female, or even if they're a single person or a group.

Satoshi mined many of the early Bitcoins (possibly up to a million), so at today's exchange rate, he (or she, or they) is a very wealthy person. It's possible that they have hundreds of millions of pounds worth of Bitcoins, but they have never spent any of them. Herein lies a problem. Since there's a strong suspicion surrounding which addresses are Satoshi's, if they ever spend any of their Bitcoins, they'll reveal their identity. So far, they've preferred to keep their anonymity rather than cash in; but will this last?

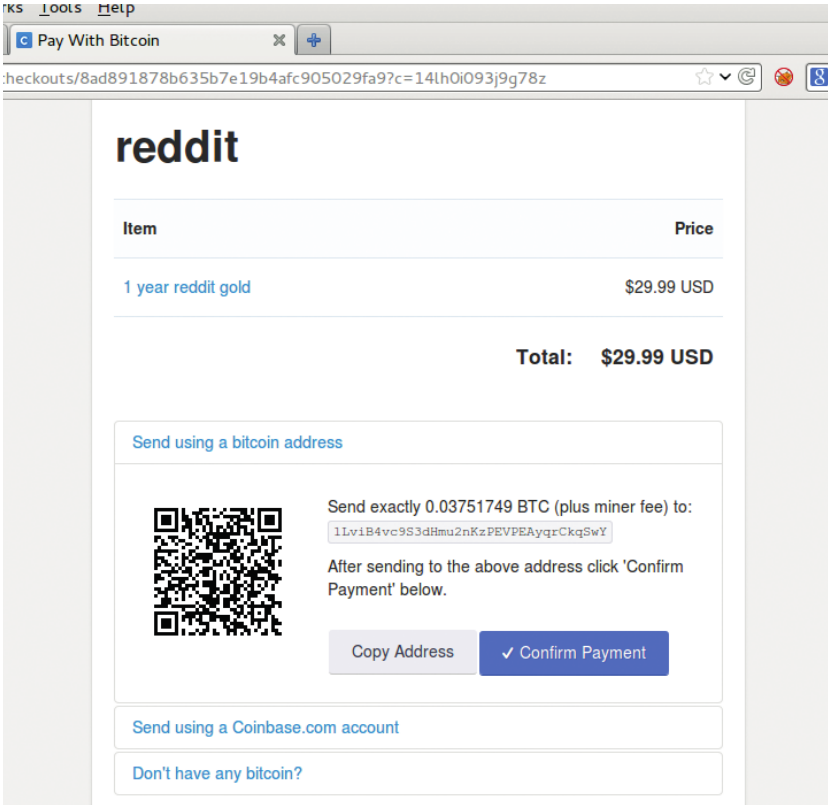
Of course, there's been wild speculation about who could have created the currency, and several researchers and journalists have pointed the finger at various people, but all have denied it. Perhaps at some point in the future, the lure of money will be too strong and the mysterious creator will reveal themselves. We can only wait and see…

ANONYMITY

Bitcoin has become the currency of choice for anonymous transactions online, most famously for illegal shops like Silk Road. However, it isn't designed as an anonymous currency, and in fact doesn't really fulfil the role particularly well because of the block chain. This records every single Bitcoin transaction and allows anyone to view the exact path that any Bitcoin has ever taken.

The only mitigating factor in the public display of information is the fact that you can create a Bitcoin wallet without telling anybody who you are. In this sense, the wallets are private, but the currency is completely public. This means that if you get Bitcoins anonymously (for example, if you mine them, or buy them with cash in an untraceable way), spend them in an untraceable way (for example, paying for something that's not delivered or tied to you personally in any way), and you don't link the wallet to your physical location (for example, only connect it to the internet through Tor), then the transaction will probably be anonymous. However, that's an awful lot that has to go right. If you slip up in any one of these ares, then the transaction is probably traceable back to you.

It is possible to make an anonymous transaction with Bitcoin, but, in most cases it'd be far easier to stay anonymous with cash. The block chain is a big-data analyst's gold mine and will almost certainly be used by law enforcement more and more in the future.



A typical screen to pay by Bitcoin. It contains all the information you need to make the transfer.

hashcash proof of work, and that block has to be included in the block chain. The first is purely a technical challenge, but the second is what forces them to check everything. If the block contains invalid transactions (for example, if someone is spending coins they don't have), and they do the proof-of-work, when they send the completed block to other miners, the other miners will reject it. This means that the original miner doesn't get paid, and has wasted his time. Therefore they will check every transaction to make sure it's valid before including it in a block.

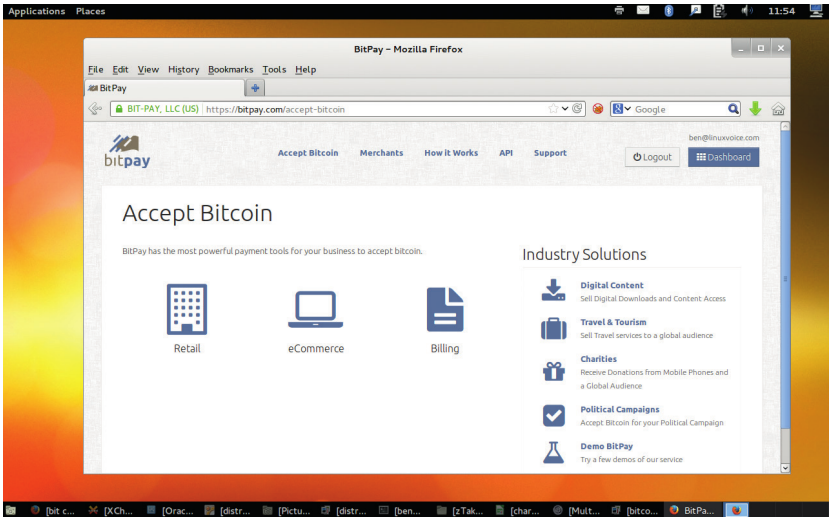
Honest self-interest

When a miner receives a block from another miner, they have an incentive to try and find fault with it for two reasons. Firstly, if they can reject the block, it means that they are still in with a chance of mining it themselves. Secondly if they accept a block that other miners reject as invalid (if they don't properly check it, for example), then any mining they do that builds upon that block will be wasted because it will never main it into the main block chain.

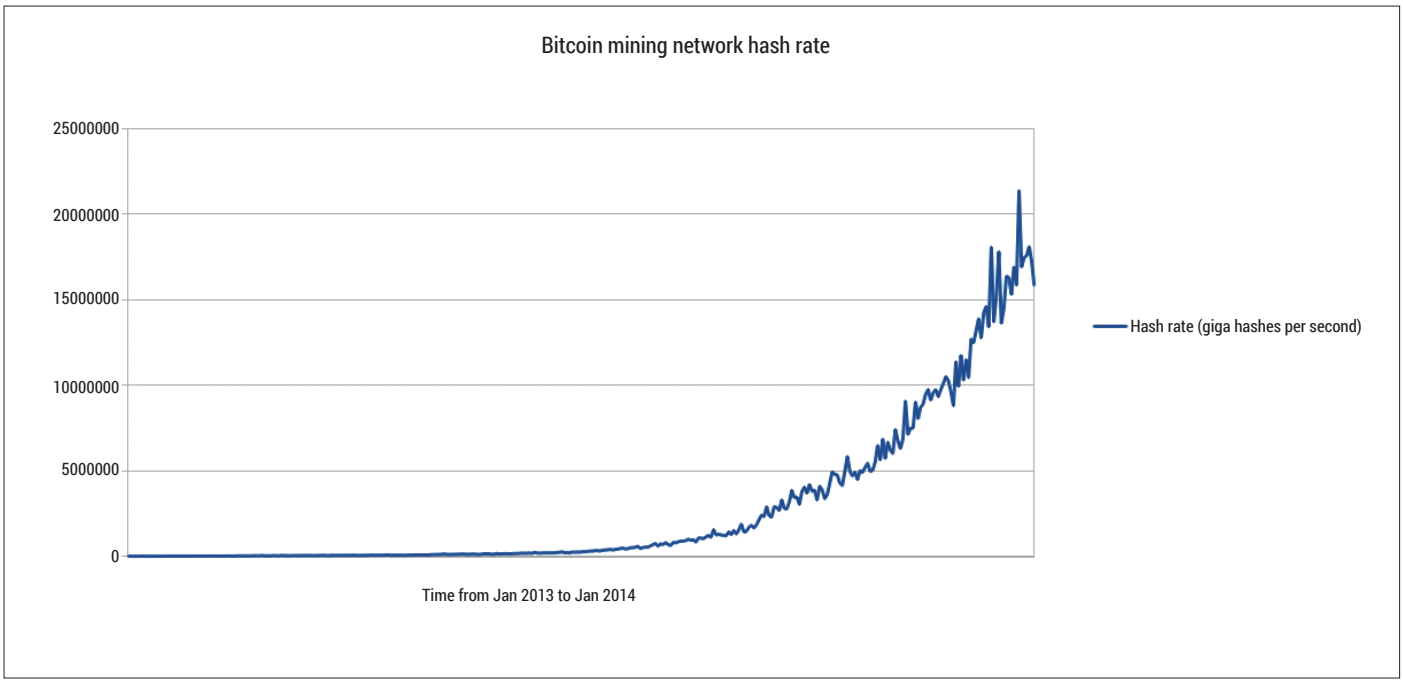
At the same time they have an incentive to accept valid blocks, because if they reject a block that everyone else accepts, then any subsequent blocks they mine will be rejected by the rest of the miners.

There is a slight issue that two miners could generate the same block at roughly the same time and send it out to all the other miners. At this point, there would effectively be a split in the block chain. Some miners would work on one, and some on the other. The rules of Bitcoin say that the longest valid block chain is the right one. One of the two splits would be first to get the next block, so then the bitcoin miners would move over to that because anyone mining in the shorter chain isn't going to get paid for mining unless it somehow overtakes the longer one, which will be increasingly unlikely as the longer one gains more and more miners.

These rules ensure that a network of miners who are each out to maximise their own profit will keep the integrity of the currency. A group of malicious miners seeking to somehow undermine the system need to have more computing power than all the legitimate miners combined (so they can mine blocks at a faster rate and maintain the longest block chain). The



You can buy Bitcoins from exchanges like this one (www.mtgox.com). They don't all have the same price or reliability, so it may pay to shop around.



The strength of a cryptocurrency is in its mining power. As you can see, this has increased dramatically in recent months.

hashcash proof-of-work, then, protects the Bitcoin network through raw computing power.

This is the reason Bitcoin mining has to remain profitable. As it currently stands, the Bitcoin network is performing at about 15 peta hashes per second and rising fast (see above). To buy computing power to beat this (if you bought the latest mining machines, although this would be impossible since there isn't enough of them to do this many hashes), it would cost around £150M (based on good Bitcoin-specific hardware). That's just for the hardware to equal the mining pool at the time of writing. The power of the mining pool doubled in the last month, and it's still increasing quickly. This also doesn't take into account electricity (they use alot), storage, cooling, people to run them, etc. Realistically, any attack on the block chain would have to perform so much fraud to cover its costs, that Bitcoin would crash in value, and the attack wouldn't be worth it.

Fraud prevention

However, the above only stays true while it's sufficiently profitable to mine bitcoins. Should this change in the future, then miners will take their computing power elsewhere (or stop upgrading it). This will then lead to a situation where the network could be exploited.

The profitability of mining Bitcoins is controlled by two factors: the difficulty in mining each block, and the number of Bitcoins the miner gets for each block.

USING BITCOIN

The crux of a currency, for most people, is how you use it. For most real-world currencies, this involves handing over metal discs or pieces of paper, but there are no such things for Bitcoin.

The first thing you need is a Bitcoin wallet. This is really just a public/secret key pair that's used to sign transactions. However, you need somewhere safe to store this because if you lose it, you can never get the coins back. How safe depends on how much money you want to store. There are wallets for almost all computing platforms, including smartphones. Remember that there's no cost to setting up a wallet, so there's nothing to stop you from having several. For example, you could store some of it on your main computer and some on your phone, meaning that you can spend it on the go. It's also possible to get wallets that are hosted online, for example, at **blockchain.info**. However remember that with online wallets, the host potentially has access to your Bitcoins.

All Bitcoin wallets work in roughly the same way, and have all the information you need to send and receive Bitcoins, and to see previous transactions.

After creating a wallet, you need to get some coins. For most people, this means buying them from an exchange such as **www.mtgox.com**. Unfortunately, this isn't as straightforward as buying most goods, since it's not usually possible to buy them with a credit card or PayPal. This is because fraudsters have previously made money by buying via these methods, then complaining to the card company that they never got the coins, and reversing the charge leaving the seller out of pocket. The credit card companies could easily check the block chain, but in the past they've chosen to side with the purchaser and now none of the major exchanges accept card. The result is that generally you have to pay by bank transfer. As it stands, this is probably the biggest thing putting most people off buying Bitcoins [*It put Ben off buying some for this feature, and in the last few days the price of Bitcoins has increased by 50%. Oh well, never mind*].

When you buy Bitcoins, you'll be asked to provide a wallet address. Once the bank transfer has taken place, the exchange will transfer the coins to the specified wallet. You then own the coins and can transfer them to whoever you wish.

Spending coins is far easier than buying them. More and more companies are accepting Bitcoins every day. When you go to a checkout, you'll be given a wallet address to transfer the funds to (this is usually a wallet created just for this transaction so don't try to reuse the same address in the future). This is often expressed as a QR code. If you have a phone wallet, you can usually transfer the funds just by taking a picture of this code. Remember that you don't send the transaction to the receiver, but rather to the mining network. The person receiving the money then gets the block chain from the mining network and looks for a transfer into the appropriate wallet.

The company receiving the funds will usually wait until the transaction has reached a depth of six or more blocks, which could take around an hour. Once this is done, you should receive the product. Remember that bitcoins are like cash, and there's no way of getting them back should the person you pay not supply you with the product.

These two things also have to be balanced to account for rising computing power and the rising market value of Bitcoins.

The number of Bitcoins awarded per block changes at a fixed rate: it started at 50 and halves every 210,000 blocks (approximately four years) until 21 million Bitcoins have been mined, then no more are awarded for mining subsequent blocks.

The difficulty is varied every 2,016 blocks. The network is designed to generate a new block every 10 minutes on average. This time was picked to be a happy medium between two opposite forces: shorter times would make transactions happen more quickly, but are more likely to lead to more than one miner generating a block at the same time, which leads to wasted resources as the two block chains compete to become longer. To keep this time period despite the hash rate of the network varying wildly, the algorithm looks at the time it took to generate the previous 2,016 blocks and tries to compensate for this.

You may have noticed a slight flaw in the plan. First we said that the security of the system was dependent on the amount of computing power it had available which was in turn dependent on the profitability of mining. Yet then we said that at some point in the future, when 21 million bitcoins have been mined, there will be no more rewards for mining.

This isn't quite true. There will be no more new bitcoin rewards for mining, but when you carry out a transaction you can include a transaction fee, which goes to the miner. At the moment this is rarely done, since mining is profitable enough that people do it without this additional incentive, and the transaction volumes are low enough. However, each block is limited in size to 1MB (there is currently a debate about whether to change this). This means there's a fundamental limit on the number of transactions in each block. If a miner reaches a situation where there are more transactions than there is space in the block, they have to decide which ones to put in. Obviously the miner will go with the ones that have the highest transaction fees. The other transactions won't be lost, they'll just be rolled forward into future blocks. Higher transaction fees will result in faster transactions.

At the moment, most Bitcoin transactions have no transaction charge, but this isn't a fundamental feature of the currency that will stay with it forever. It remains to be seen whether the transaction fees will be less or more than for other payment methods in the future. I really wish I'd bought some when I started writing this feature!

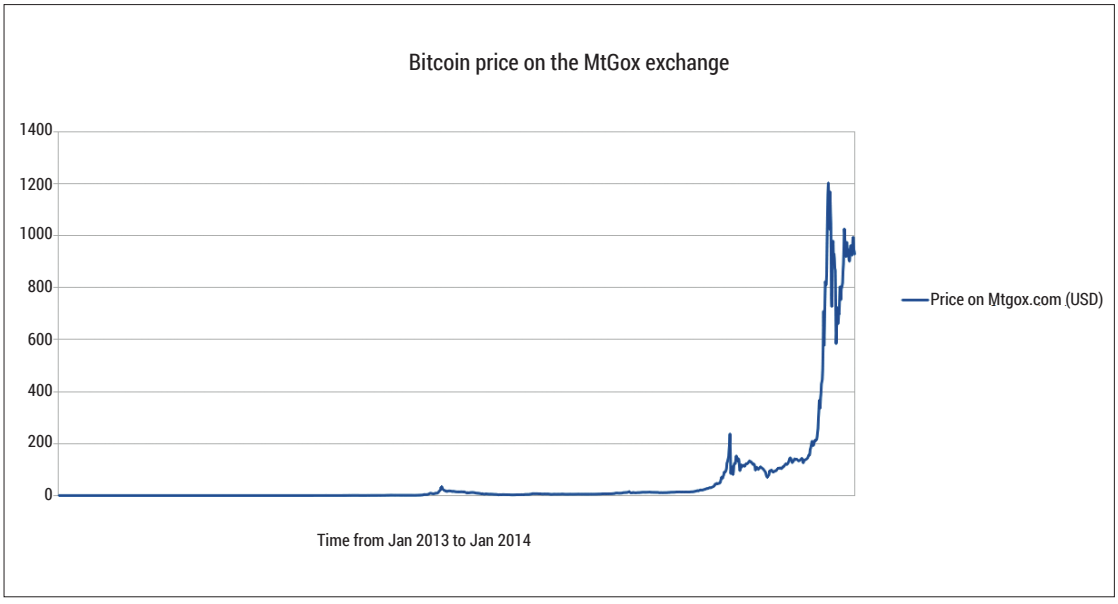
"When you carry out a transaction you can include a fee, which goes to the miner."

WHAT IS MONEY?

One of the most common concerns with Bitcoins is that they aren't real money, just numbers on a computer. This, in a sense, is true, but what actually is money? Once upon a time it was linked to physical goods, and some of the currency names reflect this (A British Pound was originally the value of a pound of silver). That link between currencies and physical goods, though, is long since gone. The last major currency to lose the link was the US Dollar, which was tied to gold until 1971. Nowadays, currencies don't have any value other than what people place in them, and the varying values people place in them is what makes exchange rates change over time.

The only real difference between Bitcoin and a national currency is that national currencies are backed by governments, whereas Bitcoins aren't really backed by anyone other than the miners. Whether or not this is a good thing depends entirely on your economic philosophy. On the positive side, no one can print excessive amounts of money leading to excessive inflation (like the German government did following World War One). On the negative side, there is no one to step in and help stabilise it should things start to go wrong (for example, the various governments that printed more money to help ease the cash flow crisis in the 'Credit Crunch').

In practical terms, the biggest difference between Bitcoin and most other currencies at the moment is the wildly fluctuating exchange rate. The value of the currency can double or halve in just a few days. Proponents say that this is likely to stabilise as the currency become more popular, and this is probably true, at least to some extent. In reality, though, no one knows what will happen in the long run since currencies without the backing or a state or organisation haven't been tried before.



The dollar value of Bitcoins has increased by almost a factor of 100 over the last year. Some people see this as a bubble set to burst, others as a sign of the currency coming of age.