A Gentle Introduction To Bitcoin

BRAVE NEWCOIN.
Digital Currency Insights

Table of Contents

A Gentle Introduction To Bitcoin

Authored By

Antony Lewis

Antony Lewis has a passion for virtual currencies such as bitcoin, and the underlying technologies behind them, including blockchain data structures and distributed consensus systems. Antony believes that these new ways of putting the technologies together will change the world of business, reminiscent of how the internet changed the distribution of information. Antony consults businesses, helping them understand the implications of blockchain technology.

antony@bitsonblocks.net

@antony_btc

Published By

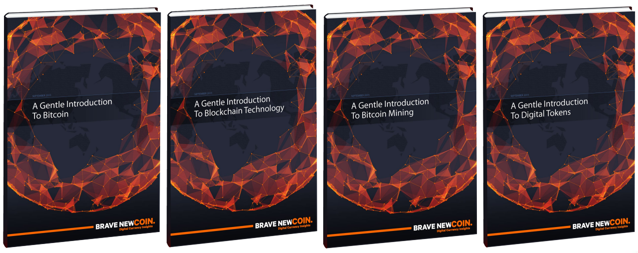
BraveNewCoin

Digital Currency Insights

Adapted from

Bits On Blocks

The '**Gentle Introduction Reference Papers™** are the first in a series of accessible documents published by Brave New Coin for industry decision makers. Designed to demystify the inner workings of Bitcoin, Digital Currencies and the emerging Blockchain technology.


A Gentle Introduction To Bitcoin
A Gentle Introduction To Blockchain Technology
A Gentle Introduction To Bitcoin Mining
A Gentle Introduction To Digital Tokens
BRAVE NEWCOIN

Series ONE covers:

"A Gentle Introduction To"

> Bitcoin

> Blockchain Technology

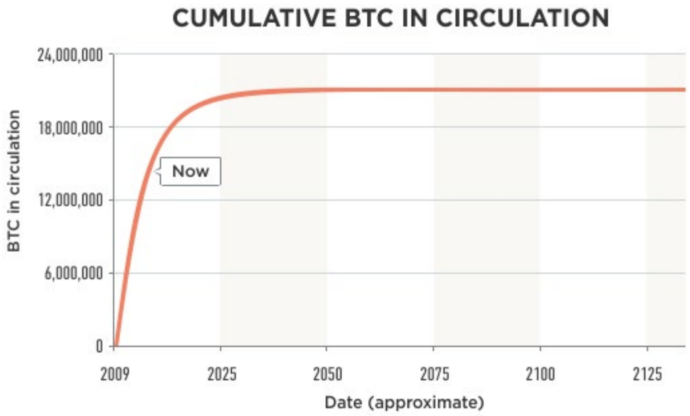
> Bitcoin Mining

> Digital Tokens

Free to Download and Share

Bitcoin

Why use Bitcoin?



Although bitcoin is often referred to as a decentralised digital currency, think of it as an electronic asset. This sidesteps questions around which government backs it and who sets the interest rate, which are often a mental block in understanding bitcoin.

As an electronic asset, you can buy bitcoins, own them, and send them to someone else. Currently there are around 14 million bitcoins that have been created, increasing by 25 bitcoins every 10 minutes or so. There is an agreed upon limit, of 21 million, the last of which should be created a little before the year 2140.

Bitcoin transactions from account to account are recognised globally in a matter of seconds, and are usually considered settled within an hour. Bitcoins have a price, which can be in any currency, but is usually in USD. This price is set by normal supply and demand market forces in marketplaces with traders, just like with oil or gold.

Bitcoin is just like any other international currency whose 'home ground' is the internet, as opposed to any geographical location. Put another way: if the internet were a country, bitcoin would be its currency. For the first time we have an entirely digital asset which can be controlled by the end user, without requiring an account with an institution.

Bitcoin payments. Payments of bitcoins can be made from one person to another, irrespective of geographical location or jurisdiction. Payments are relatively fast – the initial notification is within seconds, and it 'settles' in about an hour. In situations where the normal financial system is inadequate, it can be a useful way of transferring value to anyone who has access to the internet.

Potential users. Some communities are underserved by banks, due to the cost/benefit of the brick & mortar banking model, and regulatory cost; some international transfers are unreliable, or can take many days, with manual processes and faxes being used as part of the plumbing; some people may want to accept digital money for selling digital goods; there may be use cases where small payments, less than a penny, may be useful; these are all currently difficult with existing fee structures and payment options.

Price volatility. Just like other currencies, bitcoin's price fluctuates. Bitcoin's price is more volatile than a lot of currencies, although the volatility is decreasing). If you account for your wealth in your local currency, then owning bitcoin could be seen as a bet on bitcoin's future exchange rate price, otherwise know as speculation. You can see historical price volatility on the BNC website.

Conversion. Just like other currencies, if you have one currency (say, Pound Sterling), and you want to convert it to bitcoin, you need to find someone to exchange it with. This necessarily has some friction and fees, either dressed up as commissions or built into the conversion price, know as the spread. With time, conversion is getting easier and cheaper as more exchanges are springing up in more countries.

Maintain cynicism. You may hear of bitcoin being 'fast' and 'free' or 'low cost'. While that is true when you are strictly in bitcoin, it's worth thinking about the costs involved in the 'on' and 'off' ramps, getting from sovereign currencies into bitcoin and back.

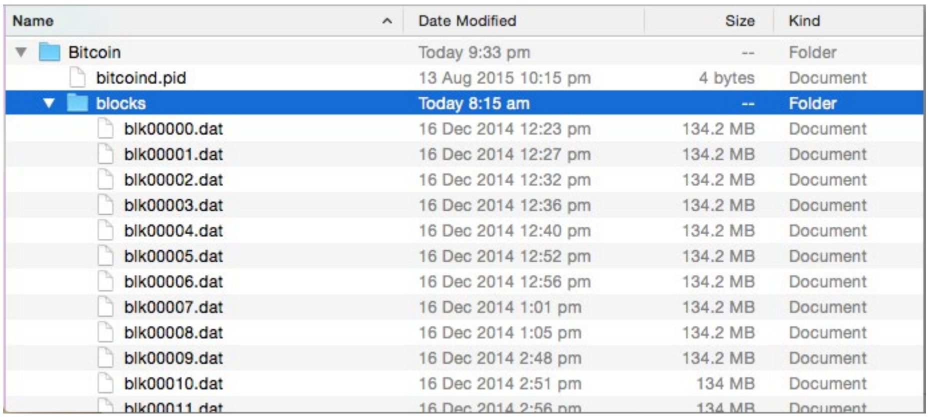
It's worth noting that while bitcoin has spawned many other similar cryptocurrencies, such as litecoin and dogecoin, bitcoin is still the most widely used and traded.

How Does It Work?

Keeping track of payments: The Bitcoin Blockchain

A network of computers keeps track of bitcoin payments, and adds them to an ever-growing list of all the bitcoin payments that have been made.

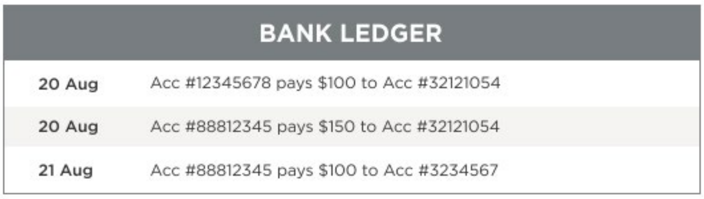
This list is a file called "The Bitcoin Blockchain", and sits on thousands of computers across the world. When you read the word "blockchain", think "database" or even "list" and you have the right kind of idea.



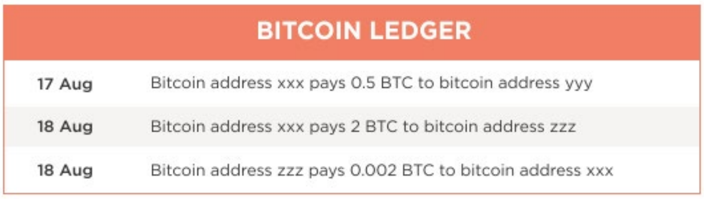
Name	Date Modified	Size	Kind
Bitcoin	Today 9:33 pm	--	Folder
bitcoind.pid	13 Aug 2015 10:15 pm	4 bytes	Document
blocks	Today 8:15 am	--	Folder
blk00000.dat	16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat	16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat	16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat	16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat	16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat	16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat	16 Dec 2014 12:56 pm	134.2 MB	Document
blk00007.dat	16 Dec 2014 1:01 pm	134.2 MB	Document
blk00008.dat	16 Dec 2014 1:05 pm	134.2 MB	Document
blk00009.dat	16 Dec 2014 2:48 pm	134.2 MB	Document
blk00010.dat	16 Dec 2014 2:51 pm	134 MB	Document
blk00011.dat	16 Dec 2014 2:56 pm	134 MB	Document

A screenshot of The Bitcoin Blockchain files on a computer. Here you can see The Bitcoin Blockchain split into files, each 134MB big, and the total currently (september 2015) is about 50GB.

This file contains data about all the bitcoin transactions, payments of bitcoins from one account to another, that have ever happened. This is often called a ledger, a term found in accounting. A bank's ledger keeps a record of payments between bank accounts.



BANK LEDGER	
20 Aug	Acc #12345678 pays $100 to Acc #32121054
20 Aug	Acc #88812345 pays $150 to Acc #32121054
21 Aug	Acc #88812345 pays $100 to Acc #3234567



BITCOIN LEDGER	
17 Aug	Bitcoin address xxx pays 0.5 BTC to bitcoin address yyy
18 Aug	Bitcoin address xxx pays 2 BTC to bitcoin address zzz
18 Aug	Bitcoin address zzz pays 0.002 BTC to bitcoin address xxx

How Does It Work?

Keeping track of payments: The Bitcoin Blockchain

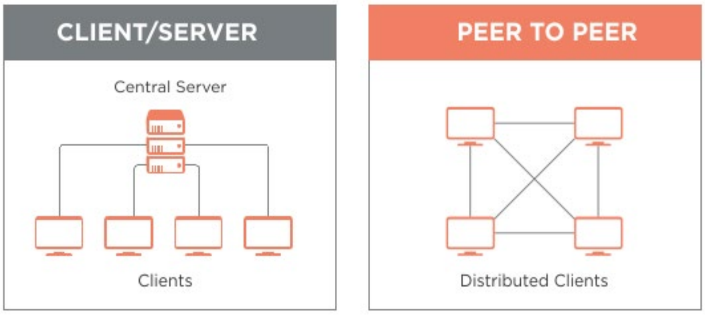
The bitcoin network. The computers which store the list of transactions also run software that connects them, over the internet, to the other computers running the same software. This forms a network of computers that can talk to each other, relaying information.

1. New payments, currently (September 2015) there is about one new bitcoin payment per second, but this comes in fits and starts.

2. Updates to The Bitcoin Blockchain occur every 10 mins, on average. A new page, or block, of valid transactions is confirmed and added to the ledger on all of the computers. This lengthens the chain of blocks, and gives the ledger its name.

When you make a bitcoin payment an instruction is sent to the network. The computers on the network validate the instruction and relay it to the other computers. After some time has passed, the payment gets included in one of the new blocks, and is added to The Bitcoin Blockchain file on all the computers across the network.

Peer-to-peer. The distribution of data works on a peer-to-peer basis, rather than client-server. Peer-to-peer is like a gossip network where everyone tells a few other people the news, and eventually the message gets to everyone in the network. The client-server model is more like a conventional organisation, where a boss tells subordinates the news, and the boss is a central point of reference, and potential failure.



Client-server vs Peer-to-peer data distribution models

One benefit of peer-to-peer (p2p) over client-server is that with p2p, the network doesn't rely on one central point of control which can fail.

How Are Bitcoins Stored?

Bitcoin accounts: Addresses & wallets

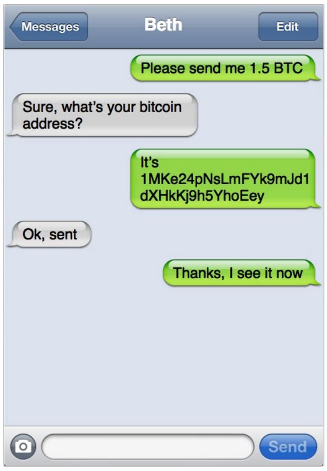
Bitcoin ownership is tracked on The Bitcoin Blockchain, and bitcoins are associated with "bitcoin addresses". Bitcoins themselves are not stored; but rather the keys or passwords needed to make payments are stored, in "wallets," which are apps that manage the addresses, keys, balances, and payments.

In banking you have accounts which keep pots of money separate; in bitcoin you have addresses. A bitcoin address is similar to a bank account number, with a few differences.

Here's an example of a bitcoin address:

1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey

Just like with bank accounts, if you want to receive a bitcoin payment, you need to tell someone your bitcoin address, so they know where to send bitcoins to. A typical conversation, which could be in person, or online, or on chat (Whatsapp/Skype etc) looks like:



Please send me 1.5 BTC

Sure, what's your bitcoin address?

It's 1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey

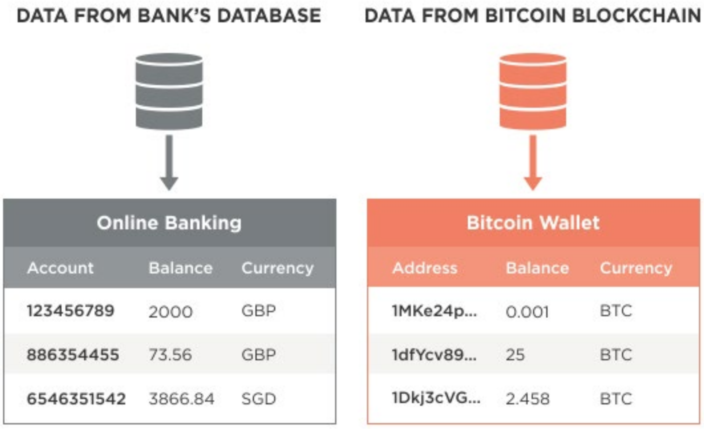
Ok, sent

Thanks, I see it now

(BTC and XBT mean the same thing and are industry standard abbreviations for bitcoins, like GBP for Pound Sterling)

Using a bank, under one single username/password, you can control a number of accounts (eg incoming salary, monthly savings, tax, etc), each of which has a balance or amount of currency. Similarly, Bitcoin wallets are apps that display all your bitcoin addresses, display balances and make it easy to send and receive payments.

For a wallet to provide accurate information, it needs to be online or connected to a Bitcoin Blockchain file, which it uses as its source of information. The wallet will read the Bitcoin Blockchain file and calculate the balances in each address.



Online Banking

Account	Balance	Currency
123456789	2000	GBP
886354455	73.56	GBP
6546351542	3866.84	SGD

Bitcoin Wallet

Address	Balance	Currency
1MKe24p...	0.001	BTC
1dfYcv89...	25	BTC
1Dkj3cVG...	2.458	BTC

Bitcoin wallets let you create bitcoin addresses to receive incoming transactions and make outgoing payments, plus have other features that make them user friendly.

How Are Bitcoins Sent?

Payments, or bitcoin transactions

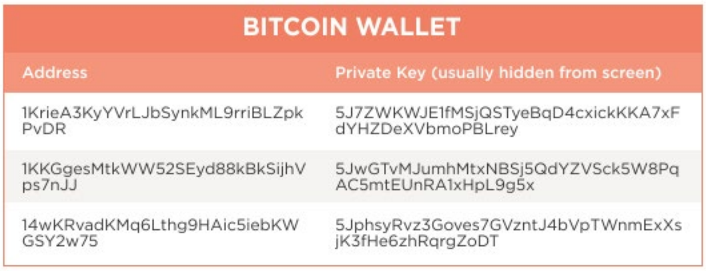
Each bitcoin address has its own private key, which is needed to send payments from that address. Think of a key as a kind of password, but it's mathematically linked to its respective address, so it can't be changed, unlike a conventional password or PIN number.

For this address (**1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey**), the private key is **5KkKR3VAjjPbHPzi3pWEHVQWrVa3C4fwD4PjR9wWgSV2D3kdmeM**. Whoever knows this private key, can now make payments from the address.

To get your own address/private key combination, it is not given to you by some authority like a bank, but rather you use a random number and apply some maths to it – wallet software will do this for you.

Private keys. The private key is something you want to keep securely and never expose. Because you can not change that private key to something more memorable, it can be a pain to remember. Most wallet apps will encrypt that key with a password that you choose. Later, when you want to make a payment, you just need to remember your password.

Because bitcoins don't exist, as such, bitcoin wallets don't store bitcoins but store the keys that let you transfer or 'spend' them. Copying a wallet doesn't double the number of bitcoins you own, you simply have a copy of the same keys. If someone manages to copy and read your wallet, they can empty the accounts, just as two people with duplicate keys to a bank's safe deposit locker can race to unlock the locker, but the contents of the locker do not double.



BITCOIN WALLET

Address	Private Key (usually hidden from screen)
1KrieA3KyYVrLJbSynkML9rriBLZpkPvDR	5J7ZWKWJE1fMSjQSTyeBqD4cxickKKA7xFdYHZDeXVbmoPBLrey
1KKGgesMtkWW52SEyd88kBkSijhVps7nJJ	5JwGTvMJumhMtxNBSj5QdYZVSck5W8PqAC5mtEUnRA1xHpL9g5x
14wKRvadKMq6Lthg9HAic5iebKWGSY2w75	5JphsyRvz3Goves7GVzntJ4bVpTWnmExXsjK3fHe6zhRqrgZoDT

Bitcoin wallets contain private keys, not bitcoins!

What happens when I make a bitcoin payment?

A payment is an instruction to unlink some bitcoins from an address you control, and move them to the control of another address (your recipient).

Your payment instruction includes everything you'd expect, including:

1. Which bitcoins you're sending.

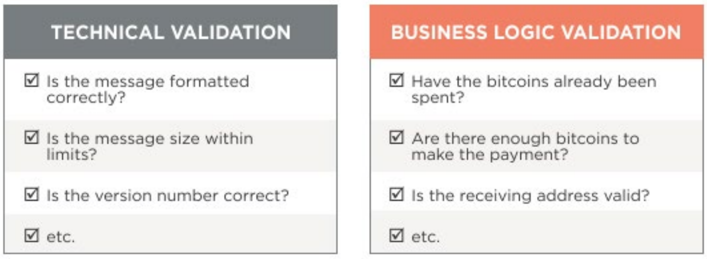
2. Which address you're sending them from.

3. Which address you're sending them to.

Digital cryptographic signatures. The instruction is digitally signed with the private key of the address which currently holds the bitcoins. This digital signing demonstrates that you are owner of the address in question (because only you know the private key).

Payment instructions are sent from the wallet software to any of the computers on the network ,called "nodes" or "payment validators."

Validators. When the first computer receives the instruction, it checks some technical details, and some business logic details (eg, does the payment attempt to create bitcoins out of nothing? Have the coins being sent already been sent elsewhere? etc).



TECHNICAL VALIDATION	BUSINESS LOGIC VALIDATION
☑ Is the message formatted correctly?	☑ Have the bitcoins already been spent?
☑ Is the message size within limits?	☑ Are there enough bitcoins to make the payment?
☑ Is the version number correct?	☑ Is the receiving address valid?
☑ etc.	☑ etc.

Validators validate at technical and business logic levels.

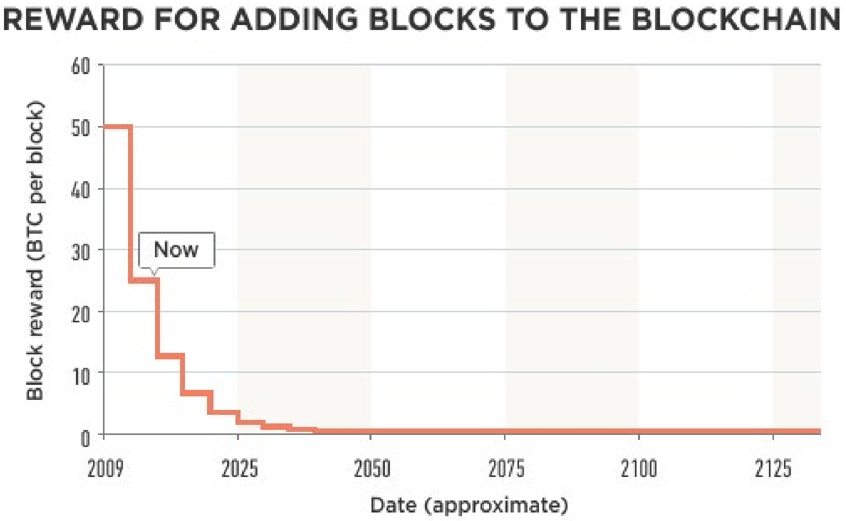
If these tests pass, then the computer relays it to others on the network. Eventually all computers on the network know about this payment, and it appears on screens everywhere in the world as an "unconfirmed transaction". It is unconfirmed because although the payment has been verified and passed around, it isn't entered into the ledger yet.

How are bitcoins tracked?

How do transactions get entered into everyone's blockchains?

As well as passing information about transactions between each other, nodes are also generally working to add these transactions, in blocks, to the blockchain. This is known as "mining" bitcoin. This is often described as "solving complex mathematical puzzles to win bitcoin." In fact there is nothing complex about this process, it just deliberately takes many computational steps, with no shortcuts.

Mining. A guessing game where your chance of winning is related to the processing power of your machine. Whoever guesses the right number first can publish this to the other computers on the network, who perform a quick validation, and if it checks out, then the guesser awards themselves with some amount of new bitcoins (currently 25 BTC, and halving roughly every 4 years). This happens roughly every 10 minutes on the network.



Due to this reward, bitcoin mining has become very competitive, with companies developing specialised hardware, called ASICs, which are very quick at the guessing game and associated number-crunching.

Bitcoin's protocol and code ensures that it takes around 10 minutes for the network as a whole to guess correctly. This is the speed that transactions take to be confirmed onto the blockchain.

Slow for security. By making it slow (10 minutes is slow compared to how fast it could be done if the guessing game was removed), and by making it computationally and therefore financially expensive to participate in this process, it also makes it financially expensive for malicious attackers to buy enough processing power to write their own abnormal blocks of transactions into the blockchain. Bear in mind that even if they were to do this, all the other computers would need to agree with the transactions, so they still cannot insert transactions that break the business logic rules, eg conjuring bitcoins out of thin air.

Bitcoin security

There are two parts to bitcoin payments:

1. Making payments

2. Block control

Making payments. The only thing needed to make a bitcoin payment is the private key of the address you want to spend from. There is a balance between making it hard for people to steal private keys, and having backups in case they are lost – there are stories of people throwing away old laptops containing – not bitcoins – bitcoin private keys controlling bitcoins worth millions of dollars.

Block control. Like an army of independent accountants and auditors, all auditing the same ledger, the romantic vision of bitcoin was for many thousands of independent block validators keeping the system true. This independence and mutual validation of transaction and blocks is supposed to prevent any one person or entity from adding rogue blocks and dominating the network with their influence.

In practice, miners join forces into 'mining pools' in order to win blocks more often. The spoils are shared, which has the effect of each participant winning less value but more often, much like a lottery syndicate. This works well for paying back capital needed to buy mining equipment. As a consequence, the mining pool owners have greater power over the bitcoin network in terms of creating blocks, voting on protocol changes, and potentially re-writing recent ledger entries.

If you have ability to re-write a recent block, then you could 'unwind' a payment in what is known as a 'double spend' attack. You would make a payment to a vendor, and have it confirmed in a block. If you can create a couple of blocks without the payment to the vendor, then the network will invoke the 'longest chain rule' and ignore / orphan the first block and use your longer chain instead. You also need to invalidate the original payment, by creating a slightly different transaction, spending the same bitcoins, but paying yourself or someone else, instead of the vendor. If you can slip this transaction into your new blocks, then the old transaction will be invalid to the network.

Your ability to do this shuffle increases with 'mining power' and decreases with the age of the block you are trying to replace, as each block 'costs' a certain amount of mining power to create, and you are competing against the rest of the network to create blocks.

Scams. It's hard to research bitcoin security without hearing of Mt Gox, an early bitcoin exchange. Bitcoin exchanges are websites you go to to buy or sell bitcoins. If you want to buy bitcoins, you first make a bank wire to the exchange's bank account. When they see the funds in their bank, they let you place orders to buy bitcoins from sellers. Likewise, sellers need to send bitcoins to the exchange's bitcoin wallets before the exchange will let them sell the bitcoins. The exchange acts as escrow, holding onto cash and bitcoins and then releasing them once the trade has been made.

It is unknown what happened at Gox, but rumours include having private keys stolen, poor accounting practices, letting people trade first before sending collateral, etc. Just as you don't blame the US Dollar if a Citibank branch gets held up and funds stolen, it wasn't the security of the bitcoin network that was at fault; it was the security and poor practices of the exchange.

What is this decentralised bit?

Let's go back to "Bitcoin is a decentralised digital currency". We've seen that bitcoin is digital, and not really a currency (though it is easy to send, and it has a value that is determined by supply and demand on a number of exchanges). What about the decentralised bit?

Distributed validators. Centralised means one point or source of control, and decentralised is where the control is shared among participants. In bitcoin, participants are the validators of the transactions and creators of blocks. If enough of them decide to play by different rules, then the others will need to follow suit. The validators have "voting power" proportional to how much computation power they have. Anyone can be a validator, and get more votes, if they are prepared to pay for computing power, the costs of which are hardware, electricity, and support. So instead of one single authority who can change the rules, the rules can only be changed by consensus of those validators.

The validation logic (what does a valid transaction look like?) is baked into the code which is run by the validators.

Open source code. This code is open source, meaning that validators can see exactly what code or logic they are running. The version that is most often used (called the 'reference implementation') is stored here:

https://github.com/bitcoin/bitcoin

In theory, anyone can contribute to this reference implementation by uploading changes, though there are gatekeepers, people, who have the final say about what gets included.

In theory, anyone can write versions of this software, so long as they conform to the technical and business protocols of bitcoin. For example you could write you own version of the software, but with improved graphics, or a more user-friendly interface. If you want to change some of the protocol rules, however, you'd need to persuade the majority of the validators (miners) to run your software with the new rules. Here's an example version that has some changes to the technical protocols:

https://github.com/bitcoinxt/bitcoinxt

Changing the rules. So the rules can be changed, as long as you achieve majority consensus (another myth is that the limit of 21 million bitcoins cannot be changed. It can be changed, in one line of code, assuming you can get the majority of network participants to agree to run it). Getting the miners to agree to run new code is the real challenge, as they have invested huge amounts of capital and will not readily agree to change anything which may harm their mining rewards – "The turkeys won't vote for Christmas".

CONCLUSION

You will probably have guessed by now that there is a lot more to bitcoin than we have been able to set out here. In giving a gentle introduction we have had to present some concepts at a high level, which in practice are complex and highly nuanced. But as you read and learn more in our reports, we hope to be able to take you through a more detailed understanding of bitcoin, virtual currencies, and the underlying Blockchain technologies.

Puzzled by some of the terms used in these gentle introduction series? Please visit our glossary for a complete terminology breakdown.

www.bravenewcoin.com/bitcoin-basics/glossary/

About

Digital Currency Insights

Brave New Coin is a Data & Research company focused on the exponential Blockchain & Digital Equities industry. We collect, index and report on countless digital assets and their market & industry activities.

Subscribe to our weekly newsletters to keep in the loop with industry news.

Subscribe

www.bravenewcoin.com

contact@bravenewcoin.com

Bits on Blocks is a Singapore - based blog, run by Antony Lewis, who focuses on Blockchain Technology. Mr Lewis believes that Blockchain Technology can make the world a better place.

antony@bitsonblocks.net

www.bitsonblocks.net

Explore more resources

- Research & insights
- Market-Data
- Developer tools (API's)