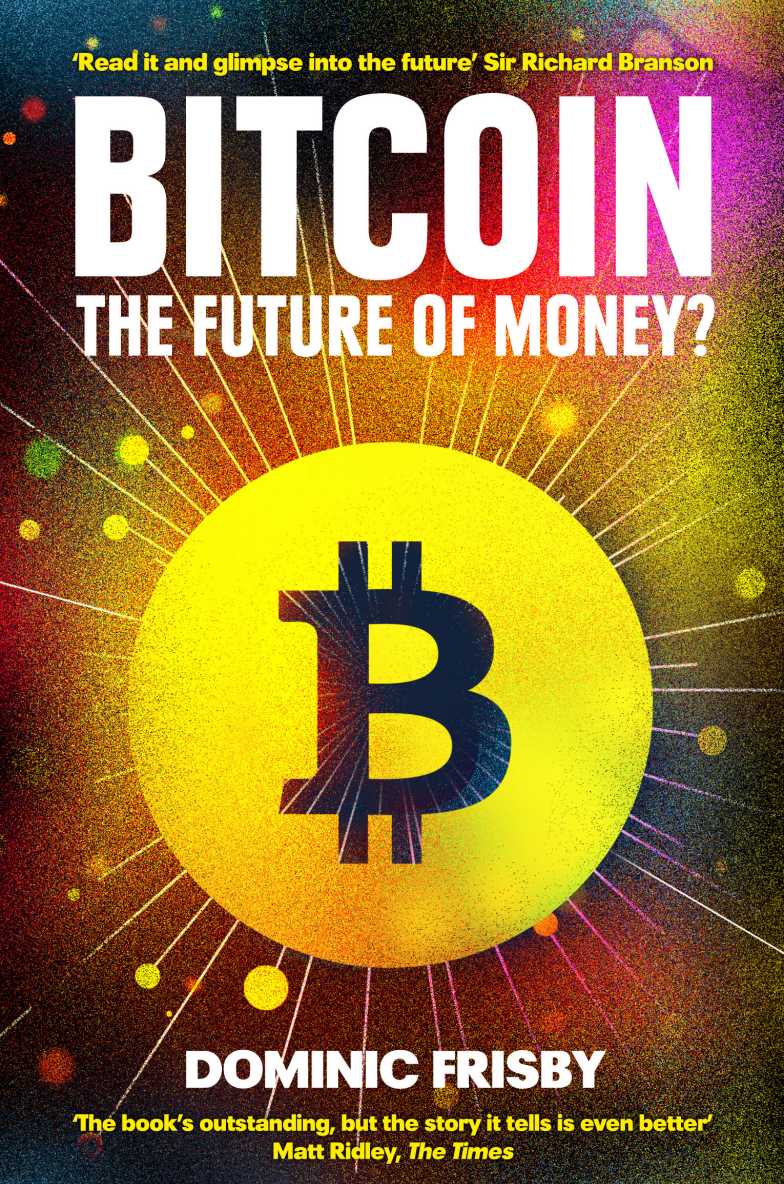
'Read it and glimpse into the future' Sir Richard Branson

BITCOIN

THE FUTURE OF MONEY?



DOMINIC FRISBY

'The book's outstanding, but the story it tells is even better'
Matt Ridley, *The Times*

Contents

AUTHOR'S NOTE

I have called this book *Bitcoin: The Future of Money?* Really, I should have called it *Cryptocurrency: The Future of Money?*

Bitcoin is just one of many cryptocurrencies (don't worry, I'll explain what that means). It is, arguably, not even the first. But it is the first that works. And it is the one that has caught everyone's attention. Rather as people say 'Scotch tape' or 'Sellotape' instead of 'sticky-back plastic', Bitcoin is the name everybody knows – hence my choice of title.

I have quoted extensively from online forums and chat boards. These often contain spelling mistakes and grammatical errors. For the sake of accuracy, I have made the decision to leave these errors uncorrected. Nor have I acknowledged errors with a 'sic', as I felt this would be both patronizing to those I quote and burdensome on the reader. So, when you come across errors in quoted passages, now you know why.

In researching this book, I have come across entire political and technological movements I'd never even heard of, filled with characters I knew even less about. They might be infamous to a small band of computer coders, but not to most people. What's more, those who discuss Bitcoin and its associated technology quickly slip into technical jargon, particularly regarding computer code. It can make it all rather baffling and, worse still, alienating. If you think finance and

economics are hard to write about in a clear way, try computer code with an all-star cast whose names mean absolutely nothing to most people.

I've tried to make it all as clear and concise as possible – to tell this amazing story in such a way that you don't have to be a 25-year-old computer hacker to understand it – but nor will you be bored if you are one. To get the balance right, I have had it read, at one end of the scale, by numerous computer programmers and, at the other, by my 82-year-old, technologically illiterate dad.

I hope you enjoy it.

PROLOGUE

We have not only saved the world, er, saved the banks...

— Gordon Brown, former UK Prime Minister

In September 2008, crisis gripped the world.

Many believed the entire financial system was about to collapse. It was a 'global financial tsunami'; we were 'on the brink' and 'staring into the abyss'.[1] Capitulating stock markets, bankruptcies, bank runs – events came thick and fast and, at first, nobody seemed to know quite what to do.

Then, under immense pressure from the world of finance, governments and central banks reacted dramatically. They created money and credit on a scale unprecedented in human history. Banks were bailed out, interest rates were slashed to levels never seen before and the process of creating money electronically known as quantitative easing was begun.

The result?

The financial system was saved. Central bankers were hailed as heroes. The idea spread that governments and central banks really can operate an economy. Even those who would normally oppose such interventions seemed to think the right thing had been done.

A few dissenters argued that the few were being bailed

out at the expense of the many, that enormous problems in the financial system were simply being deferred when they needed to be faced, and that these problems would only come back on a far greater scale. At the heart of the problem is *money itself*, they said. The way money is created means that banks and governments have inordinate control over our financial system. They profit hugely by it, while everybody else loses. The system actually creates inequality.

But such dissent was ignored – if, indeed, it was even heard.

'Only a crisis, real or perceived, produces real change', said economist Milton Friedman. Here was that opportunity for real change – an opportunity to reform our systems of money, banking and finance – our entire economies even. Politicians chose not to take it, preferring instead to save a broken system.

But that badly needed change was taking place – secretly, in a remote corner of the internet, far away from the sound and fury of this great financial crisis.

On August 18th 2008, a domain name is registered – bitcoin.org.

Even today, nobody knows who registered it.

Two weeks later, one Satoshi Nakamoto publishes a nine-page white paper outlining a design for 'Bitcoin: A Peer-To-Peer Electronic Cash System'.[2] Nobody takes any notice.

Two months pass. On November 1st 2008, with the stock market now in full-on crash mode, Satoshi mentions his paper on a mailing list for people with an interest in cryptography.

'I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party',[3] he says.

Readers throw him various technical questions, which he answers. Nobody seems persuaded. It does not 'scale to the required size', says one. The code 'can't work on today's internet', says another. Governments will close it down if it takes off, says a third.

'I believe I've worked through all those little details over the last year and a half while coding it, and there were a lot of them', says Satoshi. 'I appreciate your questions. I actually did this kind of backwards. I had to write all the code before I could convince myself that I could solve every problem'.[4]

A week later the Bitcoin project is registered at Sourceforge, a website 'dedicated to making open source projects successful'.[5]

On Saturday January 3rd 2009, the day UK Chancellor Alistair Darling announces his second bailout of the banks, the first 50 bitcoins are created – or, to use the correct terminology, 'mined'. A few days later, Satoshi returns to the mailing list and says, 'Announcing the first release of Bitcoin, a new electronic cash system.'

What had been born was a new form of money – money that could change the world.

1

WHAT IS BITCOIN? HOW IS IT MADE?

Cash is king.

— Stock market saying

It was probably the greatest trade in all of recorded history.

In October 2009, a Bitcoin aficionado who went by the name of 'Liberty Standard' published the first bitcoin exchange rate. He arrived at the figure by dividing the cost of the electricity consumed by his computer over a 30-day period by the number of bitcoins it generated. 1,309 bitcoins to one dollar was the price.[6] Liberty Standard was actually criticized for valuing bitcoins too high.

Four years later, on November 29th 2013, one bitcoin was $1,242 – over 1.6 million times higher. A bitcoin was the same price as an ounce of gold.

If anybody managed to buy the low (which actually came in December 2009 at 1,630 bitcoins to the dollar) and sell the high, they made over two million times their money. In four years, one dollar became two million dollars.

Nice work if you can get it.

The story of Bitcoin is amazing – not just for the gains (and the losses) that have been made, not just because of the revolutionary technology, but also because of the human stories that have come about as a result.

There's the developer in Finland who, trying out the tech, bought a beer from his buddy for some bitcoins. Three years later, his buddy sold those coins and bought a des res apartment in the trendiest district in Helsinki. There's the computer nerd with an interest in economics who became the FBI's most wanted drug dealer. And, of course, there's the great whodunit.

Who invented Bitcoin? Who is Satoshi Nakamoto?

He has a Japanese name, a German email address and he uses British spelling. He has invented a new form of money that could change the world. He is worth almost a billion dollars. He has computer programmers the world over purring at the unhackable genius of his tech. Half the internet – as well as investigative journalists and forensic scientists, even – have been trying to figure out his identity for over three years. And yet still, nobody knows who he is.

I think I've cracked that, by the way.

The story of Bitcoin has everything from the hilarious to the mysterious to the audacious to the calamitous.

Genius computer hackers. Dogs with funny names. Cypherpunks. Cryptography. Financial systems. Governments. Organized crime. Attempted murder. Political insurrection. Inspiring bursts of generosity. Squatters. Poker players. City traders. And people just like you.

How Bitcoin could change everything

Everybody is constantly thinking about ways to make money.

The average American spends more hours of each day attempting to earn it than he does anything else[7] – be that eating, playing or even sleeping.

But hardly a soul – not even highbrow economists – stops to consider what money actually is and how it works.

It is hard to overstate how important money is. Like the air we breathe, it is part of almost everything we do. Just about every transaction we make involves money. To use another analogy, what blood is to a body, money is to an economy.

Governments, central banks and private banks create modern money – dollars, pounds, euros and so on. This ability to create money is – as I'm sure you appreciate – an immensely powerful privilege. While most have treated this privilege responsibly most of the time, there are plenty that haven't. And all sorts of abuses have crept in.

Politicians are forever spending more money than they have – aka running up deficits – in pursuit of some ideology or political agenda (normally popularity and re-election). They might spend the money on bailing out banks, on welfare, on some kind of subsidy; they might even spend it on wars (the US military is the world's biggest employer). Central banks manipulate interest rates and inflation numbers on behalf of politicians and special interest groups. Private banks, through such means as lending and leverage, perpetrate their own abuses in pursuit of profit. As a result of all this, money gets debased.

Government agencies even use money as a means to control people and spy on them.

Money is supposed to be a means of exchange and a store of wealth, but it is also a political tool. This has been the case throughout history, but the control of governments and banks has grown over the last hundred years and is now unprecedented. It has led to huge concentrations of wealth and power. Both the state and finance now occupy, in the eyes of many, disproportionate territory in our economies.

Meanwhile, over half the world's population still doesn't have access to basic financial services and is shut out.

Suddenly, along comes Bitcoin, an open-source currency with no central authority, offering an alternative that could undermine the existing monetary order. Nobody even knows who designed it. It's by no means the first attempt at digital cash, but it's the first that works this well. It's actually more efficient than dollars or pounds. It's immune to all the manipulation and abuses that go on, there are no barriers to entry, bar internet access, and it has captured a zeitgeist in a way that nobody could have foreseen.

If Bitcoin changes the way we transact and the way we store wealth – and it has the potential to do this – the repercussions could be enormous. Think what email did to the postal service, or what the internet did to newspapers, publishing, music and television. With the huge costs involved in the printing and distribution of physical newspapers, news publishing was once the exclusive domain of a few large companies. Now any blogger, aspiring journalist or start-up can publish on the web, effectively for free. Huge opportunities have opened up to the masses, and the old dinosaurs have seen their monopolies eroded.

We're still a long way from that, but Bitcoin could do something similar to banking, finance and, even, the large state model under which we live. Without wishing to get too excited, it could bring about the huge changes to society so many are clamouring for, re-balancing the skewed distribution of wealth and opportunity. The implications are enormous.

That's why Bitcoin is important.

What is Bitcoin?

When you type a website address into a browser you might have noticed that the letters 'http' appear at the front. 'Http' stands for Hypertext Transfer Protocol. In typing an address you are actually sending an HTTP command to transmit that website to you. Hypertext Transfer Protocol is the means by which information is shared across the web.

Similarly, when setting up an email account, you might have noticed the letters 'smtp' – for example, 'smtp.gmail.com'. SMTP stands for Simple Mail Transfer Protocol. SMTP is the protocol by which we send emails to each other. What actually happens when you send an email through Gmail to, say, someone with a Yahoo address is that a Google server reaches out to a Yahoo server and transmits a text file; then the Yahoo server says to its user, 'you've got mail'.

So, a protocol is an agreed system by which information is shared across a network.

Bitcoin – with a capital 'B' – is another protocol. The function of the protocol is to send and receive payment information.

With Bitcoin, your computer reaches out to another user's computer, gives it some binary gibberish proving you control X number of coins at this address and want them to increase the balance at that address.

The unit of money on the Bitcoin protocol is the 'bitcoin' (with a small 'b'). As the dollar is the unit of money on the US banking network, so bitcoin is the unit of money on the Bitcoin system.

So, Bitcoin is two things – a protocol and a unit of money.

How do you get bitcoins?

Using dollars or pounds is easy.

You get paid in them. They're in your bank account (hopefully). And you can pay for things with them via electronic banking, by cheque, credit card, or in cash.

But where on earth do you get bitcoins?

There are three ways.

You can *get paid* in bitcoins. You can *buy* bitcoins. And last of all (the very unconventional bit), you can *make* bitcoins. Yes, you can, literally, create money.

You earn bitcoins by doing or selling something in exchange for bitcoins – just as you would earn normal money. If I do this job for you, you pay me in bitcoins.

You buy bitcoins just as you would buy and sell foreign currency – from the Bitcoin equivalent of a *bureau de change*, known as a Bitcoin exchange, or directly from an individual. You hand over your dollars, pounds or whatever currency you're using and you receive bitcoins.

To create bitcoins, you run the Bitcoin software on your computer. It's called 'mining' – more on that later. But I

should say that mining has now progressed to the point at which regular home computers are no longer much good.

Of course, you need somewhere to keep your money. You could keep your dollars in a bank account, your back pocket, your wallet or purse, even under your mattress. Bitcoins are kept in a 'digital wallet'.

There are hundreds of places to get a wallet, just as there are hundreds of places to get an email account. Often people will have more than one. You can keep a wallet on your computer or your phone, you could keep one on a hard drive offline, or you could keep one with an exchange. Some people with lots of bitcoins keep them in a wallet on a hard drive in a safe.

Each wallet has its own address – a sequence of different numbers and letters. To make a payment, you click on your wallet, type in the number of coins you wish to pay, copy and paste the payee's wallet address, hit send and the payment is made. To receive a payment in bitcoins, all the person paying needs is your wallet address. When you receive a payment, your computer might give you a little 'ching' sound to notify you. It is as simple as sending an email.

With barcodes you can open your wallet on your smartphone, photograph the barcode, hit send and the payment is made. The day is not far off when you will walk into a shop, select an item you wish to buy, photograph the code on the label, payment will be made automatically and off you go.

Once you get the hang of it, it is as simple as using a credit card. And, as long as you have internet access, there are no barriers to entry.