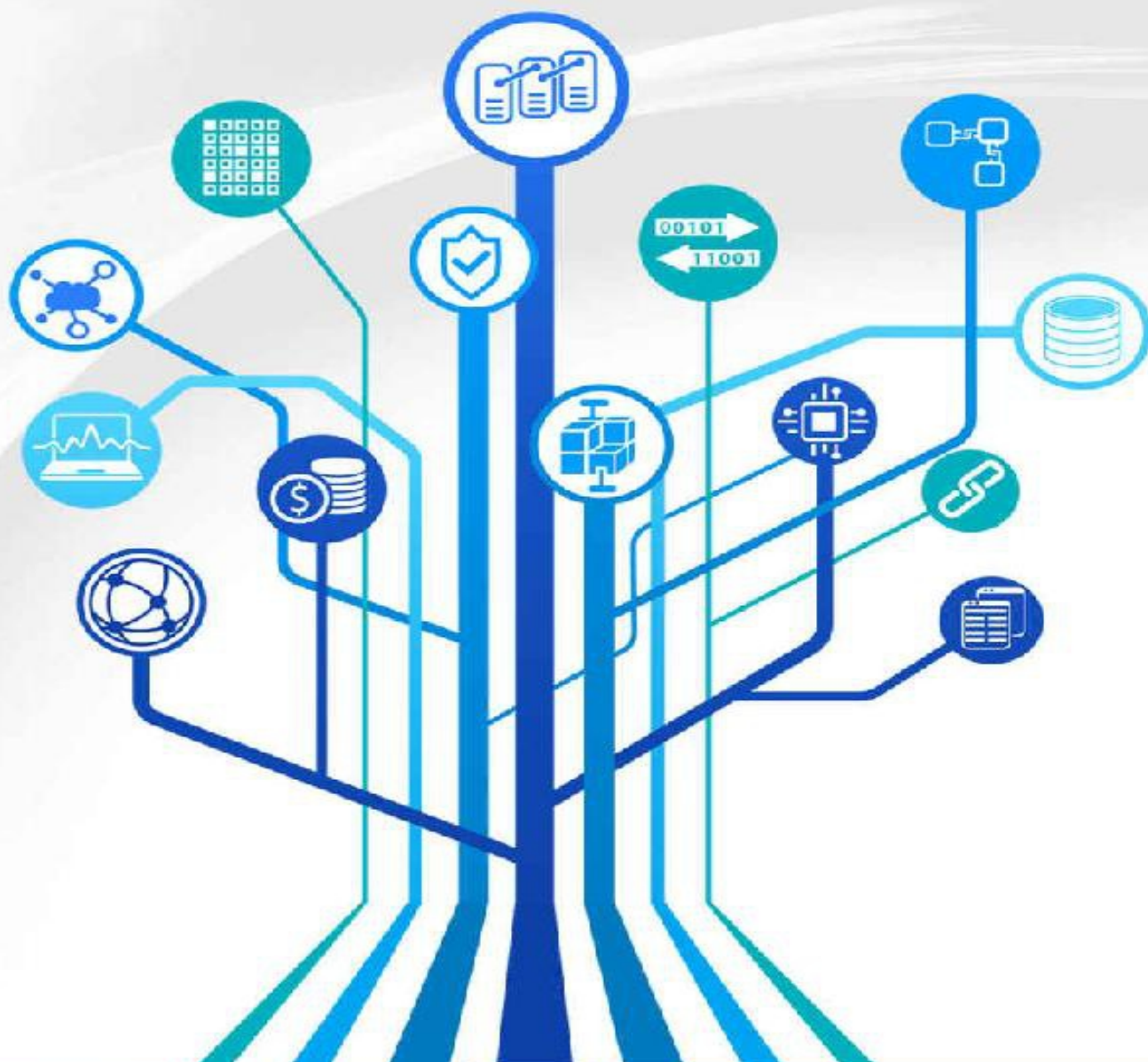


BITCOIN

THE ULTIMATE STEP-BY-STEP GUIDE TO BITCOIN



JAY ISAACS

BITCOIN

Ultimate Guide to Bitcoin

Author Name

Table of Contents

[BOOK TITLE HERE](#)

[Table of Contents](#)

[Introduction](#)

[Chapter One: What is Bitcoin](#)

[Chapter Two: What Can I Use Bitcoin For?](#)

[Chapter Three: What Are the Characteristics Of Bitcoin](#)

[Chapter Four: History Of The Bitcoin](#)

[Chapter Five: Buying Bitcoin](#)

[Chapter Six: Blockchain](#)

[Chapter Seven: Who Controls The Bitcoin Network?](#)

[Chapter Eight: Bitcoin Mining](#)

[Chapter Nine: The Pros And Cons Of Bitcoin](#)

[Chapter Ten: The Best Ways To Use Bitcoin](#)

[Final Words](#)

© Copyright 2017 by - All rights reserved.

It is not legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited.

Introduction

Thank you for downloading this book about bitcoin, the father of digital currencies.

Much myth and misinformation exists around bitcoin, and indeed all cryptocurrencies. From the misplaced and ill-informed assumptions that everybody using them is either a terrorist or master criminal, existing in some dark underworld of lawlessness and moral weakness, to a belief that they are just the flash in the pan plaything of techy geeks.

This book seeks to dispel these myths and share the truth about bitcoin.

It will discuss with you the advantages of bitcoin: safety, privacy, security. But will also not pull back from highlighting the uncertainty of the new which surrounds digital currency.

From reading the book, you will discover how to buy, store and trade with bitcoin. The best ways to use the currency as an investment, the risks and potential rewards of doing so. You will learn about mining, including ways to take part.

And most of all, you will gain a perspective about the financial innovation which will help you to see it in the context of physical currencies such as the dollar, Euro and pound. To gain an insight into ways in which digital currencies are changing the way we trade, and how major institutions are getting in on the act.

After reading this book you will have a strong understanding of bitcoin, and know where to go to further your knowledge.

It might only have been around since 2008, but bitcoin has already changed many people's lives. Further, it seems inevitable that we will all become more exposed to it over the coming few years. Those in the know

will be able to make use of bitcoin for their own purposes, taking advantage of its speed of transaction and opportunities for trade without a middle man.

The use of bitcoin by major banks is almost upon us; bitcoin ATMs are already to be found in many cities; traders such as Amazon and Microsoft have embraced it. It IS going to become a part of our lives, and we owe it to ourselves to be ready for this.

Take the opportunity now to learn about bitcoin in this easy to read guide. At the end, you will not only know about the currency, but hopefully you will be inspired to get in on the act yourself.

The time to invest in your own bitcoin supply might just be around the corner.

Chapter One: What is Bitcoin

As much as discovering what Bitcoin actually is, it is definitely helpful to learn what it is not.

The definition of Bitcoin is fairly straightforward. It is a global currency, accepted in most parts of the world, that exists only online.

Consider the moneys of the world - dollars, pounds sterling, the euro, the rouble and so on,. Collectively known as fiat currencies, these are monies that have no intrinsic value in their own right, but have built up and maintained a worth based on the economic success of the nation they represent.

To illustrate this point, imagine that the US Dollar suddenly ceased to be the money of the nation. Many of us, around the world as well as in the United States, would have small, rectangular copies of printed paper. Suddenly, these pieces of paper would be worthless. They have no value as a piece of paper.

In this respect, Bitcoin is like fiat currency in that, taken out of the online world in which it flourishes, it becomes just a series of numbers, a code, but within the internet, Bitcoin has considerable value.

But let us focus now on how this currency differs from your standard currency.

How Does Bitcoin Differ From Fiat Currency?

A Complex Way To Buy Your Daily Cappuccino

Firstly, although it may be worthless in its own right, a fiat currency has a physical form. This is the dollar bill or pound coin that can sit in your pocket. That you can exchange for goods, such as a cup of coffee or a bar of chocolate.

Bitcoin is different. The closest it gets to a physical form is the complex code in which it is stored, traded and bought. Therefore, although it

could be used to buy a coffee from a store that accepted it, you are probably better off to use your normal cash. As things currently stand, it is just easier.

Bitcoin takes the form of a code.

There is No Middle Man

If you think about it, whenever you use your normal bank account, a third party is involved. That is, your bank. This financial institution has access to the amount of money you have, knows your spending pattern, can track your interests. The bank knows all but your cash transactions (and even then, knows when you take the cash out to spend). It acts as a facilitator, and most likely charges you for the pleasure of doing so.

The same applies if you use a credit card, or take advantage of the rapidly developing escrow type services such as Paypal.

Bitcoin is different. Transactions using the online coin are peer to peer, that means that the money goes straight from one 'wallet' (more on these later) to another. Straight from buyer to seller.

No third party has access.

This offers beneficial opportunities for cost (there is no fee involved), security and privacy.

A Different Kind Of Privacy

Unless your normal bank account is hacked, the details within it are moderately private. Whilst there is no public scrutiny, clearly your bank, and its employees, can view your account. Similarly, following proper procedures, authorities such as tax agencies can also gain access. Your account could be frozen, or delays put on your access.

None of this applies with Bitcoin. The code (called your private key) which holds the amount of bitcoin you own is accessible only to you. There are no means by which it can be shared, other than to have it hacked from out of your own storage system.

This has obvious advantages of privacy, but does present a potential problem. After all, if nobody other than you know the amount of currency

you hold, it should be possible to ‘cheat’ on the amount possessed.

But bitcoin has the solution. Using blockchain technology (another area we will investigate in much more detail later) a record is made of every transaction that takes place. These details are available to every user in all respects except one – the identity of the users.

This means that every use of bitcoin is recorded. The records are held on parts of blockchain technology called public ledgers and they ensure that there can be no crookedness surrounding the exchange of the currency.

A Global Currency

Most of us will have experienced the thrill of going on holiday to another country. Learning of the culture, the geography and the climate of the foreign place. Therefore, we will also have learned of the issue of getting our hands on our spending money.

Firstly, you have to convert your own currency into that of the country you are visiting. You have to decide in the form you will take it – probably a small amount of cash (in case of theft), perhaps a pre-loaded card or credit card.

What you also know is that it will cost you to get the new currency in the first place, perhaps in the form of a direct fee, or additional charges on your card, or in a not too generous exchange rate. You also know that, short of major economic change while you were away, you will get a worse rate when you try to change it back.

Bitcoin avoids these problems. There is an exchange rate against other altcoins (types of digital currency that are NOT Bitcoin, such as Litecoin or Ethereum) and also against the fiat currency you may use to buy them in the first place, but that rate is driven very much by the users, not the financial institutions, seeking profit, and the national Governments, seeking to manage economic performance.

Once you have your Bitcoins they can be used increasingly widely. There are a few countries, Ecuador and Iceland being two, that ban their use. Some others, such as Russia and China, permit them, but do not make them easy to use, but mostly Bitcoin is welcome across the world.

Since transactions exist on the internet, there are none of the tax, exchange, political tariff and other issues to worry about that occur trading with fiat currency.

Isn't Bitcoin Just the Same As Using On-line Banking?

Certainly, there has been a substantial move from banks globally to remove cash from the currency flow. After all, it costs money to print, gets lost, is hard to keep a track of and is far too easy to forge.

Nowadays, under ten per cent of the world's money exists in cash form. If we consider it, there are substantial parts of our own money that we never actually see. Monthly payments, taxes and such like are taken directly from our accounts before we would have a chance to take our money in physical form, even if we wanted to.

But despite this, there remain substantial differences between digital use of fiat currency and use of bitcoin (and, for that matter, other cryptocurrencies). The main one of these is that bitcoin has an inbuilt deflationary tool. The supply of the coins is capped at 21 million. This means that as prices rise, the value of bitcoin increases to meet them (there are many other reasons for the increase in value of bitcoin, and we will consider these later). However, fiat currency has no cap on supply which means that, over time, more of the money is printed, and its value therefore goes down.

We see this in simple terms of the price of a loaf of bread. It costs more to buy this today, than it did at the turn of the century.

Chapter Two: What Can I Use Bitcoin For?

It is certainly the case that, in its early days, there were serious market induced limitations to how Bitcoin could be used. Put simply, there were very few merchants prepared to accept them.

Times have changed. Now, tens of millions of transactions have taken place, involving a not dissimilar number of users. But bitcoin does not just have to be used as a tool with which to trade.

An Investment Opportunity

As we will discover later in this book, many investors in Bitcoin have gained amazing returns. The value of this digital currency does vary, and is as volatile as a storm at sea, but there is an overall trend in the value of investments, and that is upwards. We will look later at ways to invest, the associated risks and the potential gains.

An Increasingly Legitimised Currency

Like all new ideas, Bitcoin was met with a mixture of fear, cynicism and distrust by many on its launch. It has taken time to gradually challenge these feelings, but today Bitcoin is regarded widely as a legitimate company.

One of the main reasons for this has been a steady increase in the range of major businesses and financial institutions to have bought into the concept.

Many major banks now employ staff looking at how they can utilise Bitcoin. Even more significantly, the currency has been overtly recognised as a legitimate means of trade by the European Union and some other countries. Most others accept its existence although do not become actively involved in it – yet. Major companies are also getting in on the act. Dell, Microsoft, Amazon, Apple – the list grows almost daily.

The major financial analysts, Forbes, have also investigated and legitimised the currency.

This means that more businesses have sought to be open to trade with

Bitcoin.

Who Will Take Your Money?

The number of merchants prepared to accept bitcoin is growing by the day. Between the process of writing this guide and your reading of it, undoubtedly the number of traders prepared to come on board will have substantially increased.

In addition to those listed above, here are some of the biggest traders prepared to accept the coin online.

Memory Dealers, also connected to the field of computing technology, was one of the first companies to come on board with the new currency.

The retailers Tigerdirect and Newegg are retailers specialising in the fields of electronics and computers. Showroomprive.com is a European general retailer prepared to take the coin.

You can pay for your university place in some countries.

And, if travel inspires you, book a flight with AirBaltic or Air Lituania (both East European) and you don't need to visit your bank to pay. Fancy a cheaper flight? Then head towards CheapAir.com.

You will need somewhere to stay when you arrive, and BTCTrip will help to organise this in return for a bitcoin or two. Plus, if it is the United Kingdom to which you are headed, you can experience a touch of British culture by buying theatre tickets through Theatre Tickets Direct.

And, an after-show drink can be supplied by Honest Brew, another UK based user.

Even supermarkets are getting on board. Monoprix, a French giant, now accepts Bitcoin. Sticking with the European theme, there is now a Bitcoin Boulevard based in The Hague, Netherlands.

An increasing number of agents are offering gift cards which can be bought via bitcoin. Included amongst these are Amazon, Walmart and Nike.

Finding a Discount

The market is an active place, and some dealers are seeking to get in on the action by offering discounts for bitcoin users. Purse.io seeks to link

consumers wanting to buy from Amazon with others wishing to buy bitcoin.

It claims to be able to secure discounts of up to twenty percent for buyers using the digital currency.

In-Store Purchasing

A new development has seen some stores being prepared to accept bitcoin 'over the counter'. CeX, based in Scotland, opened recently and provides a bitcoin ATM. Reeds Jewellery, one of the biggest US companies in the field, will take bitcoin instore. Some sports franchises are also joining the party. For example, San Jose Earthquakes, a soccer club based in California allows tickets and some merchandise to be purchased using the currency, as does the NBA franchise, Sacramento Kings.

And, the Medcover Group is beginning to roll out bitcoin payment for medical services.

Payment for these instore purchases is usually made via an app or cloud based storage facility.

How To Find Out More

There are many online forums which offer ready, and usually reliable, advice about where you can spend your bitcoins. On top of this, specialist websites such as coindesk.com will offer sound information.

Chapter Three: What Are the Characteristics Of Bitcoin

Let us drift briefly into the murky world of hypothesis. There are some, including the Central European Bank, who have, at times, attempted to make the case that bitcoin is not, in fact, money.

Economists define nine characteristics of money. Whilst something might still be used for trade (as could, for example, food or gold), if it does not possess these characteristics, it is not money.

The Characteristics of Money

Money should feature the following characteristics: it needs to be scarce, durable, recognisable, easily storable, used widely, difficult to forge, portable, divisible and fungible (ie – replaceable with another identical item).

So, does it meet these criteria?

Scarcity - Yes

Bitcoin is limited to 21 million coins, or units. So, clearly, it is scarce. In fact, compared to fiat currency, it fits this criteria more fully since it is possible to predict, with a degree of accuracy, the supply of bitcoin over the next few decades in a way that money cannot be predicted.

Durability – Yes

Again, it fits the bill more closely than currency. Your dollar bill or five pound note will undergo severe strain over its life, thrust into wallets, clipped into cash tills, pushed into vending machines. On the other hand, bitcoin is purely digital, and cannot therefore physically degrade.

Portable – Yes

Certainly. It is just a question of popping the bitcoin onto a removable drive, or app, using its code.

Divisible – Yes

Whilst you can't go lower than the lowest denomination for a fiat coin, bitcoin can be divided down to eight decimal places. In other words, it can theoretically be used in denominations as small as 100 millionth of a coin.

Recognisable – Maybe

A tougher criteria to meet for a digital currency this. After all, the money exists only in a digital code, and that code is unique to each owner. However, it does exist on the blockchain which means that it can be seen and identified there.

Storage – Yes

Bitcoin is stored in wallets and recorded on the blockchain, and although this may present more challenges over time since every transaction ever made is stored on this software, it is expected that technology will improve as the need to develop greater storage capacity evolves.

Difficult to Counterfeit – Yes

Again, this is an area in which bitcoin outscores fiat currency. Physical money is relatively easy to copy, and even digital fiat currency can be hacked and corrupted. By contrast, through the private key and blockchain, it is, as we currently understand it, completely impossible to forge.

Widespread Use - Yes

This affirmation may not have been applicable until fairly recently, but as we saw earlier, the currency is now widely used, and is operated by a growing number of established organisations.

Fungability – Yes

A bitcoin is a bitcoin is a bitcoin. Whereas a dollar is not a pound is not a yen. All bitcoins are equal, and, to paraphrase the awesome George Orwell, no bitcoin is more equal than any other.

Hoping that our journey into philosophical exploration has not been too foggy, we can see that bitcoin has the characteristics of money. And, therefore, is money.

Thus, it represents everything (and more) that can be authorised by your

bank account or ten buck note.

So having identified the characteristics of bitcoin as being those of a form of money, we can next look at three of the greatest characteristics of bitcoins, factors that it shares with most other forms of digital currencies but, because bitcoin is the big daddy of them all, hold greater significance for this currency.

These three are:

Safety

Privacy

Freedom from Legislation

Safety

We will consider this in far more detail in the chapter of blockchain, but basically bitcoin is protected from theft (almost) and forgery.

Because every transaction is recorded on every computer simultaneously, there is no way for hackers to get into the system. In order to do so, they would need to hack every computer of every user simultaneously, which is beyond the realms of possibility. In the region of twenty-five million users would need to be attacked – and defeated – at exactly the same moment.

Then, there is a further level of protection. An owner's bitcoins are recorded on an encrypted code. Called the private key, it is unique to the owner. Were it to be intercepted, then the owner would know because this would be immediately recorded on blockchain.

But in order to use the bitcoin, another encrypted code is needed. This is called the public key, and it carries the bitcoin to be used in a transaction from peer to peer. One key will not work without the other.

On top of this, the public key will only transfer the amount agreed by the owner of the private key. The public key ensures that once the transaction is initiated, there is an immediate transfer from the private key of the buyer to the private key of the seller.

Unlike a normal transaction, there is no delay and there is no passage of

the money through a middle man.

Everybody knows that the transaction has taken place, because it is immediately reported on blockchain.

There are two risks, but neither involve the technology used by bitcoin directly.

Firstly, if a user loses their private key, there is no way to get it back. Most are stored in wallets, which are online storage devices which can run from as simple as a piece of paper on which the code is written, to cloud based storage facilities. We will look at wallets in a little more detail next.

Secondly, your own computer or device might be hacked when you access your wallet. For example, if your computer has been infected with key stroke malware, a hacker will be able to identify your code.

Cloud based wallets have an advantage that they often come with additional password codes, although some of the privacy advantage is given up because a third party is employed. Online storage is good in that it allows for ease of use, but it does mean that your bitcoin is only as secure as your computer.

A portable hard drive is also a good system to use, because it is only connected to a network (and therefore vulnerable to attack) when it is plugged in. Some paper wallets offer more than just the noted number, but are actually software programmes that generate random codes which must be combined to access your wallet.

The best advice is to store any bitcoin you get in a variety of wallets.

Privacy

Bitcoin has a wide number of agencies prepared to accept it now, and it is increasingly used for transactions. It is not possible, because of the nature of the blockchain technology on which it is based, for anybody to identify the name of the users in any exchange or trade.

Freedom From Legislation

Because bitcoin is global, and operates via the internet, individual nations have no way to legislate on its use. This could change in the future,

but at present its whole world status is one of its strengths.

Chapter Four: History Of The Bitcoin

Have you ever experienced the overwhelming urge for a pizza?

Possibly, or maybe not. Whichever, buying one (or two) using an entirely new form of payment would probably not feature that highly on your to do list.

At The Birth Of Time – Internet Time

The concept of a digital form of money has been around as long as the internet itself. It is just that, prior to bitcoin, nobody could make it work. The first form was called Ecash but, just as with subsequent efforts, the linkage of the new currency to some centralised body proved too problematical.

Decentralisation – A Radical Concept

The actual inventor of bitcoin is not really known. Satoshi Nakamoto created the currency, it is just that nobody is really sure who that is. A pseudonym, it might represent a single person or a group of inventors working together.

However, whoever he, she or it might be, they came up with a radical new idea. Take away the middle man, and just allow peer to peer transactions. Then, rather than having some huge institution overseeing the entire process, let it be run and monitored by the users themselves. A proper meritocracy.

Transactions would be recorded on a public ledger, which every user could see and every user could monitor.

The ledger would follow the destination and use of every single bitcoin, just protecting the actual users through the use of encrypted ‘keys’ or codes. In order to provide security, every transaction would simultaneously be available for scrutiny on every single computer of every single user. A completely ground-breaking concept.

Nakamoto decided that the currency would emerge out of digital mines. Briefly, because we will look at this in more detail later, those interested in technology would solve complex mathematical problems with the aid of their computers, and be rewarded with coins. Nakamoto decided that the supply of bitcoins would always be managed, with a maximum of twenty-one million eventually being in circulation.

Within a year, a miner earned enough bitcoins to buy two pizzas. He paid 10000 for them, although these days he could probably buy around 3 million of the cheesy topped treats for that amount.

Indeed, it was the financial context of the times that perhaps helped bitcoin to take off. In 2008, when the idea first hit public attention, the collapse in the subprime market had led to global recession. People needed something different, but trustworthy, in which to invest their money.

But this was still a way off. Initially, the market grew amongst computer programmers, with the odd forward-thinking investor and others who had heard and were intrigued about the concept. They were a self-regulating community, trading amongst themselves, and mining to increase the supply of bitcoin in the market place.

Early on, Nakamoto offered tips to miners, but as the rewards grew, so ever more complicated problems needed to be solved, requiring increasingly specialised equipment. Today, the chances of achieving any success as a miner with a standard computer are highly minimal.

Nakamoto disappeared from the scene in early 2010, about the time of the pizza purchase. Rather like a caring mother whale, he or she (or they) left their cub to survive the economic tempests on its own, hoping it would grow into of the giants of the financial seas.

By the beginning of 2011, nearly a quarter of the total availability of bitcoins had been mined.

More and more merchants were prepared to accept, and often embrace, the currency, and the big boys of the trading world started to take note.

Investors began to put their hard cash into the digital currency. The market is volatile, but the over-riding trend is upwards. At the time of writing, a bitcoin was worth in the region of \$3000, with trading taking place

down to millionths of a coin, worth approximately three cents.

Early investors have realised fortunes, and the papers abound with stories of forgotten transactions which have changed people's lives.

The growth of bitcoin also spawned many other contenders. Collectively known as altcoins, that is all digital currency that is not bitcoin, they are largely tiddlers to the bitcoin's whale. Many have been lost to the currents and predators of economics, who consumed them whole. But some have done well, and are starting to grow in value; nothing yet as big as bitcoin, but evolving. Litecoin, Ethereum. Dogecoin – they may one day secure a role close to their big daddy.

Chapter Five: Buying Bitcoin

Now we have shared some information about bitcoin, a little of its history, what it looks like, how it can be used and what it actually is, you may be ready to go out and get your own bitcoins. In this chapter, we will look at how to do this.

Step One – Find An Address

This is a bit like your bank account. It is the actual place where your bitcoin will live. An address is a complex line of code and users can possess as many addresses as they wish.

Step Two – Get A Wallet

We talked briefly about wallets in an earlier chapter. In order to get an address it is necessary to get a wallet.

Remember, there are various kinds of wallet and the best advice for beginners is to start small. Purchase only a small fraction of a bitcoin so you can see how it works, and what it can do you. Rather like the entry level of a complex computer game, by playing around you will pick up the basics and be able to ascend to more complex levels.

There are a number of sites from where you can get your wallet. A bit of personal research is advised, but among the best and simplest services offered are:

Mobile Wallets (very flexible, best for small amounts) eg Airbitz, CoPay and Mycelium

Software Wallets (kept on your computer, so make sure that your anti-virus is a good one, and is up to date.) eg Armory and Bitcoin Core

Wallets (usually stored on cloud, so can be easily accessed but run by a third party – possibly the most vulnerable form) eg GreenAddress

Hybrid Wallets (offers flexibility of a web wallet, but private key kept by owner) eg Copay

Hardware Wallets (secure, but don't lose the hardware!) eg Ledger and Opendime

Step Three – Buy Your Bitcoin

There are a number of ways you can do this. Some of the ideas are listed below.

Perhaps the most popular way, especially for the beginner, is to visit an exchange. This is, as the name suggests, an online place where you can buy bitcoins (and sometimes other cryptocurrencies) using credit cards, debit cards and bank transfers. The exchange will set the rate for purchase. There are many that are local to a particular country or region, but here are three international exchanges with good reputations.

Kraken, Local Bitcoins and Bitstamp. Simply go to their websites for details.

A second option is to purchase through Paypal, and in some urban centres it is possible to get your bitcoin through an ATM.

Since we are dealing with a new currency here, it is not always essential to use traditional ways of paying for your currency, although the next suggestions are as traditional as they come. You could contact somebody with access to bitcoins and offer to sell them something, or do some work for them and get paid in bitcoins.

Or, you could seek out an individual and offer to buy bitcoins directly from them. This can cut out the cost of the middle man, although as you will be paying with a fiat currency, the same level of security is not present compared to using an exchange.

Our best advice is, once again, start small and get an understanding of the concept of using bitcoin. Do your own research, and join a forum where you can share practical advice and have specific questions answered.

But it is really as simple as that – set up an address, acquire a wallet and buy your bitcoin.

Then, you are ready to trade, or keep your investment and watch it, hopefully, grow.

Chapter Six: Blockchain

Imagine a giant spreadsheet. One that holds millions of cells of information. Now, imagine that every ten minutes it is automatically updated with numerous new cells.

Next, consider that this spreadsheet is on the computers of everybody in a giant network. The spreadsheet is identical on each, because it is the same spreadsheet.

And, when it updates, it changes at exactly the same time with exactly the same information on all those computers.

This, in a very simple form, is how blockchain operates.

What Is Blockchain?

In fact, blockchain is far more complex than this. As the name suggests, the blocks of information it holds are connected, or chained together. It is the technology on which cryptocurrencies operate, including bitcoin.

But as a facility, it has many more uses, and its functionality is very much in the early days of discovery.

So, it could be used to hold central registers of pretty much anything – votes cast in an election? Planning permission applications? Any kind of transactions? The list is endless.

It works by offering a network of computers to the chance to hold, simultaneously, a ledger, or book of information, that is spread throughout the entire network. Hence, this is called a distributed ledger. The ledger is also public, creating the term ‘public ledger’.

Decentralisation

Blockchain is a decentralised technology. This means that there is no

one 'holding' base. If we use the example of a spreadsheet given above, and imagine it as a ledger of sales records, normally such a system will operate in the following way.

The head office will hold a central record. On it might be a list of the names of the sales staff at the company, then rows, perhaps showing weekly amounts sold, spreads out so that it is possible to track the sales of an individual sales person, or perhaps a group.

This spreadsheet might then be sent to the area offices, and managers there might use that data to share with others and use as, for example, the basis of a 'sales person of the month' award. At the end of the week, the sales staff will contact their area office to update their figures, these will be shared with the head office, who will update the spreadsheet and start the process again.

Although it can be difficult to get our heads around, the decentralised system of blockchain cuts out the different steps.

Here, every person associated with the company has a live version of the spreadsheet. After every individual sale, the sheet is updated instantly (or pretty much so) on each person's computer.

Some Advantages Of Decentralisation

Such a system offers a range of advantages. It is incredibly fast. We can examine this by linking it to money and take an example still in use today, a main form of exchange until very recently. If somebody wished to buy something, they would often choose to pay by check.

The buyer would need some form of guarantee on the check, and the seller might have to wait three or four days to actually receive the money. A third party, the bank, would process the exchange of money. With bitcoin, because it uses blockchain technology, the currency leaves the buyer's wallet and appears simultaneously in the wallet of the seller.

The system is also secure. For somebody to hack they need to hack every person on the network's computer simultaneously. This is, as we see it at present, effectively impossible. The fact that it is not run by a single being or body adds to the security, since a solo operator is much more vulnerable to

attack than a large group.

A decentralised approach offers privacy as well. There is no third party to oversee or spy on the use of the currency. Certainly, the blockchain records (on the distributed ledger) that a transaction has occurred, and it has involved the transfer of X amount of bitcoin. But it does not record from and to whom the transaction operated. It does not know, because each person's bitcoin is in fact a unique and encrypted code.

Taxation and suchlike is difficult to enforce. Because there is no third party, nobody is witnessing the exchange of money. Therefore, it is impossible to know, for example, how much tax (of whatever kind) might be owed on an exchange. To illustrate, somebody offering services in return for fiat currency payment will be required to pay income tax on the money they make.

Unless they are paid in cash, and keep that cash under their mattress, then the tax authorities can, and do, check with their bank to ensure that the correct amount is paid.

If the service provider is paid in bitcoin, then nobody knows how much they have received. Or, indeed, that they have performed the service (other than the recipient).

Thus, it is impossible to track the due tax. Some countries and unions have recognised and accepted this, and do not (at the time of writing) require payment of tax for transactions using bitcoin.

Others, such as the US, put the onus on the trader to honestly declare their income.

It Is Low Cost

Whilst the benefits to individuals of this are fairly limited, global financial institutions are excited about the opportunities blockchain technology offers to settle global transactions at far lower cost, because of the speed involved and the absence of a middle man.

For example, whilst waiting the \$2 payment to clear your bank following your online sale of a set of pencils will not cost much in lost interest, a \$200 million global transaction costs much more if the monies take

a day to clear.

Plus, the commission of the middle man will be substantial.

Data Leakage Is Prevented

At present, when we need to find information about a person, for example their age if they wish to drink in a bar, or their qualifications for a certain job, we tend to use a sledgehammer to crack a nut.

For example, imagine somebody uses a driver's licence to confirm their age, that licence also contains lots of other, in this case unnecessary, information which has been shared with the supermarket as you try to buy your beer.

Blockchain technology would stop this, as it would only prove the information asked for.

And the immediate nature of the information could also speed up, for example, getting car insurance. All the details needed would be immediately available, and there is no need to go back to the company to confirm a no claims discount.

Further, since the information is something to which you already have access as a part of the blockchain network, there is no middle man to pay for facilitating the sharing of information.

Whilst blockchain works really well for bitcoin and other cryptocurrencies, the opportunities for further use are manifold.

Chapter Seven: Who Controls The Bitcoin Network?

The most straightforward answer to the question of the title is that the bitcoin network is owned by the users.

As is inevitable and probably desirable, the software that is bitcoin is regularly upgraded and developed, so the technology wizards behind these changes do wield more influence than a single user (called a node), but there is no compulsion on users to take up these changes.

However, the principle behind bitcoin is that it is a decentralised currency. In order to work properly, it must be capable of peer to peer operation. Therefore, there is a pressure on the users and developers to reach consensus on how it operates.

Perhaps this does identify a vulnerability in its operation. We can use the analogy of the George Orwell's novel, *Animal Farm* (itself an allegory of the rise of communism).

Animal Farm is ruled by the animals. It is a complete democracy, every animal has a say in what takes place, and all changes must be agreed the inhabitants.

In the novel, the Pigs are the cleverest animals, and they quickly see that they can utilise the Farm's production for their own ends. They use a combination of firstly persuasion, then fear, to force the other animals to adopt the rules that they want.

Ultimately, all the rights are taken away from the other animals, and the Farm becomes a kind of dictatorship, run by the dominant animal group – the Pigs – who in turn are led by the dominant Pig – Napoleon.

The risk to bitcoin comes if a significant group from within or (more probably) outside the user network seek to wield more power than the set up allows.

In this case, it would be possible for updates to begin which change the fundamental operating system of bitcoin. Most users will have little interest

in the operations of the system, and as the pioneers who hold the concept in their hearts become diluted through ever wider use of the system, then the possibility of infiltration is possible.

Whilst at this stage, the currency seems safe from such intrusion, there are potential scenarios which could emerge.

For example, we know from the Edward Snowden leaks that the NSA, and GCHQ in Britain, like to snoop on their citizens. This is all blanketed by concerns around terrorism and organised crime, but Snowden's revelations indicate that Government organisations were (and probably still are) doing more than just seeking to prevent terrorism.

If, and as, Bitcoin becomes ever more widely used, it is possible that such an organisation might wish to see more details of the people carrying out transactions. Whilst the global nature of bitcoin should act against this, as agencies only have authority within their own nations, we know from Snowden that, for example, the US based NSA was actively hacking into the private communications of other world leaders, such as German Chancellor, Angela Merkel.

More likely, as bitcoin transactions become ever more popular, it is possible that Governments will see these transactions as potential cash cows, accessed through levies and taxes. Legislation would be very hard to bring about, again because of the global nature of bitcoin, so a slice by slice 'salami' approach, encouraging certain types of upgrades and gradual changes in the protocols might be the way to bring about the changes they, but possible not most of the users, would want.

A third way that a group might emerge as underground controllers of the network would be if a fork in the technology developed through unreconcilable differences in beliefs around the system's development.

It is possible that a 'second' bitcoin could develop, with the currency operating in two ways. Over time, if the new version became dominant, it could take over the traditional form.

There is some evidence that this will not happen. In certain ways, the development of altcoins has challenged bitcoins status. Many of these altcoins have sought to improve on the original, and some are venture capital

backed. These coins are there to make money, and to do so could work in different ways to bitcoin. For example, a coin such as Korecoin, could have backers who feel greater legitimacy, and therefore greater value, comes from removing the private nature of transactions using the coin.

Should currencies such as these overtake and supplant bitcoin, then control of the cryptocurrency world, if not bitcoin itself, could move out of the hands of users. (Whilst bitcoin might still exist in the above scenario, if its value slumped, it might die because the market chose not to use it).

The thing is, however, that none of these emergent altcoins are coming close to presenting a challenge to bitcoin as the leader of the pack.

However, the ideas above are just 'conspiracy theories'. At this stage, the users of bitcoin run the network. That is one of the founding concepts behind the currency.

But...increased legitimisation of the currency is a two-edged sword. On the one hand, by making the currency more legitimate, demand will increase and the product will become both more usable and hence more valuable. That supply is finite could further add to an increase in its value. On the other hand, the involvement of major financial groups might put pressure on changes in its structure, which would represent a body (probably Governmental) seeking to exhibit control.

After all, nobody wants to see a huge institution getting away without paying its taxes do they? Not that such an organisation would ever seek to do so...perish the thought.

Chapter Eight: Bitcoin Mining

As we saw earlier, the original and, at the outset, only way to get your hands on the first bitcoins was through mining. Whilst now there are numerous ways to become involved with the currency, mining is still a way to get your hands on not only bitcoin, but other cryptocurrencies.

To recall, the miner would use their technological skills and computer processing power to solve complex mathematical problems. Success was rewarded through the payment of bitcoins.

A ‘Pickaxe’ Used To Be Enough

In the early stages, the value of these coins was minimal. But, with (at the time of writing) each coin carrying a value of over \$3000, and supply slowly closing in on the maximum permitted, so the complexity of the mathematical problems has increased enormously.

Whilst other cryptocurrencies are still highly mineable by individuals, the same is probably not true anymore with regards to bitcoin. From the middle of the decade, the processing power needed to solve a mining problem began to exceed the capability of the standard, everyday desk or laptop.

These days, your computer needs to run a host of graphics cards to increase its capability, and increasingly, specialised equipment costing thousands of dollars is required to be successful.

Pool Your Resources

However, alongside the increase in difficulty of mining solutions began to develop. Mining pools were formed, to which users can join and add their computing power to that of others to make mining possible.

There are various forms of these pools, from a simple ‘buy-in’ where the facilitator does the actual work, to more hands-on approaches. To take one example, a mining pool such as Multipool works by taking a tiny cut of

the mining proceeds in return for organising a pooling of resources.

The thing to remember is that by going it alone any returns are held just by yourself, but the chances of success are remote. On the other hand, the rewards of mining are more likely to be achieved as a part of a pool, but the coins you get will need to be shared amongst the group.

One possible way in for those keen to enter into mining as a way to find coins is to start by playing around with some of the smaller currencies, for example, Dogecoin is both accessible and seeks to put the fun into cryptocurrency. Once some experience has been gained, then one can move to a more advanced scenario, for example by tackling bitcoin.

Is A Head-Torch Enough?

Software is needed in order to mine. Whilst the omnipresent Microsoft Windows is fine for the purpose of mining, it is eschewed by many serious and experienced exponents of the art.

The reason for this is that these experts feel that Windows is not a good fit for mining operations; security is not sufficiently tight because the operating software was not designed for this purpose.

For this reason, the operating system of choice for many miners is Linux. Not only does it provide a good fit with mining requirements, but Linux has developed specialist programmes to assist with mining. One such programme is LinuxCoin.

For those seeking to look into other cryptocurrencies, a google search to their website will access good advice.

Do remember as well that you will need somewhere to keep your digital gold once it comes your way, so make sure you have a wallet ready and waiting.

Watch Out – There's A Thief About

Although you will be mining on the ultra-secure blockchain platform, your tools are less protected. Since your PC will be behind the actual digging process, it is a device that is vulnerable to attack.

If you make a big find, or even act as part of a pool who strike a rich

line of ore, then you might be making a fair bit of money.

Hackers and other cyber-crooks will love to get their hands on this. Therefore, make sure that your anti-virus and anti-malware protections are up to date.

As more and more technological amateurs seek to buy their way into bitcoin, and other cryptocurrencies, the online thieves, like herring gulls by a coastal sandwich store, flock for easy gains.

And, personal security systems need to be constantly updated to even stay in touch with the malware merchants.

Take care.

There we have mining. As a final point in this chapter, it should be remembered that there was a fun element to the very first bitcoin development of the late 2000s. Mining is fun, and is perhaps best viewed as such, rather than as a money-making enterprise.

Those days are largely gone, at least as far as bitcoin and the individual miner are concerned. The potential rewards are considerable. A block mined today will release twelve and a half bitcoins, with a value, at the time of writing, of \$40000, or thereabouts.

A new block becomes available every ten minutes.

Such rewards have attracted the big boys, who have access to the sort of technology about which the independent user can only dream.

Then again, dreams do sometimes come true.

For those who would like to learn to more than could be provided by this brief examination of bitcoin, bitcoinmining.com offers plenty of free and easy to understand information.

Chapter Nine: The Pros And Cons Of Bitcoin

Let's start here with the negatives, because bitcoin is not a perfect solution offering wealth, privacy and security in return for a bit of a play on the internet.

For all that it can offer, and we will go there at the end of the chapter, there are disadvantages to consider.

Myth and Understanding

There are still people out there who regard bitcoin as the currency of crime and terrorism. Whilst we know that this is not the case, and that the currency is used by authoritative companies. Nevertheless, there is the risk of being seen by some (the uninformed) as somehow 'underground'. Not that this should be a problem.

The currency is also extremely new. Although it has around since 2008, by contrast pound sterling has been legal tender for close to 900 years.

Because the currency has only recently been available, there is a lack of understanding of how it works. Whilst those with a special interest may understand it, the everyday trader, merchant and customer are in the semi-dark.

And this very newness adds the further concern that there is no long-term history against which future trends can be judged.

Volatility

Whilst the general trend regarding the value of bitcoin has shown a steep upwards curve, within that overall rise there have been vast fluctuations in value. The coin has also grown up in a time of global financial uncertainty.

A period of worldwide economic growth could see a major trend back to fiat currency at the cost of bitcoin, and this could result in a sharp drop in its value.

Lack Of Protection For The Buyer

When you use a credit card to buy, for example, a new laptop the card company itself offers some protection to the consumer. For example, if the goods are faulty and the seller won't sort this, the credit card company may return your funds to your card.

There is no facility to do this with bitcoin. Once you have paid, you have paid. Also, since the transaction details remain private as to the people involved, any consumer rights would be extremely hard to prove.

Uncertainty

There is more to bitcoin than just its financial value. Its very difference from fiat currency means that we cannot predict how it will be affected and influenced by future political interest and, maybe, interference.

The Rise Of Other Cryptocurrencies

Bitcoin is currently leader of the pack, but we know that the alpha male lion will eventually lose its place at the head of the pride, and even Usain Bolt eventually failed to win an athletics final.

Currency is of course different, but the principle remains. Whilst it is today the major cryptocurrency, we cannot be sure that it will not be superseded in the future by one of the new kids from the block.

Has It Peaked?

Surely, the rise in value of the currency cannot be sustained? Logically, there has to become a point at which its value can go no higher.

The financial world is a competitive market place, and if bitcoin continues to be so successful, surely other, larger, players will seek to take on its attributes?

Again, this is all supposition, but as we saw earlier, because it is such a new currency, we cannot predict with any confidence where it might go.

Advantages of Bitcoin

We have already touched on some of the multitude of advantages bitcoin provides, but these certainly deserve a brief recall.

Transparency

Because all transactions are always available to view on blockchain, the 'brown envelope' deals using fiat currency are not possible, or at least are extremely difficult, to achieve.

And, because it is a decentralised currency, its value is totally determined by the market place. It is worth what somebody is prepared to pay for it. Therefore, it is much harder to manipulate or corrupt.

Privacy

Remember, it is only the transaction that appears on the blockchain. The users involved in that transaction remain private.

This has all kinds of positive ramifications. Sometimes, somebody may simply enjoy privacy, because it is something to which we are all entitled.

It allows for users who would rather people do not know what they have bought, sold or the level of their investment to maintain their privacy.

Low Cost

The absence of middle men keeps costs low, potentially to zero levels. This has great positive implications for all sizes of transactions, whilst also adding to the privacy levels since no third party can watch an account.

Speed And Security For Sellers

Merchants gain many benefits. The money is in their digital wallet immediately a transaction is made.

There is no risk of default, since the payment has already been made.

There is no buyback of the goods. Once somebody has paid, they cannot reclaim their money. This makes managing cash flow much easier, and also offers additional certainty to traders. The indirect effect of this is that the traders have more confidence in the market, and that mean goods and services have downward pressure on their prices.

There is also less risk of fraud. Since bitcoin only exists as an encrypted code, and that is verified on the public ledger of blockchain, it is impossible to counterfeit the currency.

Security

Since each person is in charge of their own bitcoins, with no possible interference from a third party (the only exceptions being with some kinds of web and cloud based wallets), users are in complete control of their finances.

It cannot be used as a source of identity theft, since the identity of users is not known.

Further, when used as a payment means, only the currency is used, there is no sharing of personal information.

The transparency provided by blockchain means that merchants cannot apply 'hidden' extras.

High Returns on Investment

We will look at this aspect in a little more detail in the final chapter, but the fact is that anybody who has kept bitcoin for even a moderate amount of time has seen their investment yield substantial growth.

Chapter Ten: The Best Ways To Use Bitcoin

In this chapter, we will consider two specific uses of bitcoin in some detail. We will look at using bitcoin as an investment, and using it as a purchasing tool.

Investing In Bitcoin

The first question here is, is buying bitcoin and keeping it with a view to seeing its value increase an investment or a gamble?

A Wise Punt?

The evidence so far is thus – over time bitcoin has increased substantially in value, growing at a much faster rate than other currencies.

The gamble is then, has the bubble burst, or about to go pop? But then, this is the judgement for all investments. The dot.com bubble seemed certain to last, and attracted many millions of dollars in investment...until it went bang.

Bonds are investments, and will almost certainly offer a return, but they are low risk and the returns reflect this.

The question to ask is what level of risk is acceptable to you as an investor?

A Volatile World

In 2013, the value of bitcoin fell to around \$20 at one point, within a very short while it spiked to \$1200.

Seemingly, it would be wise to jump on the bandwagon, but anybody who did would see a slump of over \$1000 per coin in a flash. Sell, and cut losses, or stick with it?

Those who kept their investment in place, now see a figure two and half times the 2013 high when they change bitcoin back to dollars. Those who

sold...well. Bad decision.

Invest As A Part Of Your Portfolio

With major institutions from Goldman Sachs to American Express dipping into the market from 2015, and the establishment of a Bitcoin Index and investment trusts, it would seem as though the big boys who handle investments such as IRAs could be exposing their clients to the coin, albeit not directly but as a part of the packages they offer.

Middlemen make charges, and these can be avoided by simply buying or acquiring the coins yourself in a peer to peer transaction. A middle ground of investment would be to include some bitcoin as a part of your plans, without exposing more than you could afford to lose.

Safer Than Fiat Currency?

Yes, the risk of bitcoin crashing or losing value heavily does exist, both in the short and long terms. But, the same is true of fiat currency. For example, taking a long time spread of 100 years, a dollar is worth today only around 5% of what it was a century ago.

That bitcoin will stop production of new coins from around 2140, when it reaches the 21 million mark, would suggest that its value will continue to increase.

After all, although it exists in an inflation free zone, because it is decentralised, its worth is (at least today) measured against the dollar and other currencies, so should keep on rising over time.

Can We Trust Any Forward Predictions?

The future is uncertain, but some research suggests that investment in bitcoin is a no-brainer. Analyst Gil Luria estimated the amount of use of bitcoin in the future, taking out those coins lost (when owners lose their private key), those held in investment and those used in active currency, and predicted that investments made in 2015, when his research took place, could see returns 40 times greater than that initial investment within ten years.

The risks of investing in bitcoin cannot be ignored. But when

considered in the context of other information, it would seem that they are a good, if risky, bet for an investor.

Advice could be to spread your investment portfolio, but include bitcoin in your higher risk/higher return element.

Transacting Using Bitcoin

We have already looked at the advantages of using bitcoin, such as privacy and security, so here are some other tips that could see you getting the most from your cryptocurrency

Trade For Other Cryptocurrency

By spending time watch the market in altcoins, you will be able to detect when coins are increasing in value. At any stage where another cryptocurrency appears to be growing faster than bitcoin, it can worth a punt to buy.

For investors looking at short term gains, it is worth investigating peer to peer exchanges, or forums to find people wishing to trade, as this will remove the fee most exchanges charge.

Picking up on the idea of spreading your portfolio, it could be worth taking a small part of your investment reserve and using it to speculate on long term altcoin growth.

There is obviously risk in this, but the opportunity for big gains is there.

Develop Your Political Knowledge

When using bitcoin to purchase, or receive them when selling, it is worth looking at the legislation in that country.

A nation where trade is difficult might see peers more willing to pay more for your goods or services. Equally, a country which supports the use of the currency might be one where people are prepared to accept a little less to get their hands on it. Research and discussion can help to ensure that the you gain the best rates.

Further, look to trade with people in countries where there is no tax, as people are more likely to be open and keen to link up in these locations.

But most of all, stay on top of developments. Bitcoin is such a fast-moving currency that those in the know of what is happening will make the biggest profits.

Final Words

It won't be long in coming. Of that, we can be pretty sure.

Imagine the scene. Sitting at the breakfast table with your morning coffee and laptop, scanning the day's news.

The article about the latest Presidential mishap is just another in a long line of similar stories, and you skip over it. Over the page is an article on the latest cryptocurrency to hit the market. Since reading an e-book a couple of years ago, digital currency has become an interest of yours.

You already have investments in bitcoin, and three other altcoins. You decide to read the article, and click on it.

Instantly, your wallet has reduced by two microbits, the cost of reading the article. The online paper itself was free.

You head off to work, scanning your mobile wallet on the station reader and instantly the cost of today's fare is removed from your web wallet. It's cheaper than it used to be, because your fare goes straight to the operator, no company stands in the middle to take their cut.

You check your blockchain data, and follow the link to bitcoin prices; they've gone up again, and so you book the table to take your partner to dinner. You can afford to. Your investments are paying off.

This is the world that bitcoin is leading us towards – decentralized, secure, private, safe. At least, we hope it is.

And, having read this book, you are in a better position to make your own judgements as to your own involvement with the currency.

We thank you for your foresight, and your interest.