BITCOIN

The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Bitcoin

RICHARD OZER

Bitcoin:

The Insider Guide to Blockchain Technology, Cryptocurrency, and Mining Bitcoin

RICHARD OZER

ISBN: 1973754800

ISBN-13: 978-1973754800

Other Computer Science Books Written by Richard Ozer

Cryptocurrency Series

Ethereum: The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Ethereum

Bitcoin: The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Bitcoin

Want to keep up-to-date with new releases, special subscriber only promotions and other news/cool stuff?

Table of Contents

Introduction

There is no denying that the blockchain is one of the most ingenious inventions of all time, invented in 2008 by Satoshi Nakamoto. The invention was the backbone of the first ever cryptocurrency, the Bitcoin, a digital, decentralized currency that made money transfers much easier. Bitcoin is now accepted as a form of payment for goods and services in many places but the blockchain has moved on to greater things.

Because the blockchain allows us to distribute digital information but not to copy that information, it has begun a new era; instead of an Internet of Information, we are fast heading towards an Internet of Value, a system that will be far more secure and less open to malicious hacking than ever before.

By the end of my book, you will understand what the blockchain technology is all about, what Bitcoin is and how the blockchain supports it. You will learn how to mine Bitcoin, how to spend it and how to invest in it for the future. We will talk about the pros and the cons of the blockchain and Bitcoin and end with a discussion on how Bitcoin differs from other cryptocurrencies that have been developed as competition.

I do hope you enjoy my book and I would like to formally welcome you to the world of Bitcoin and the blockchain.

Chapter 1: Bitcoin and the Blockchain Technology

There is a good reason why we call Bitcoin "digital gold". From inception to date, 9 years the currency has gained a total value of more than $40 billion and the blockchain that underlies the currency is more than capable of making other digital value types. Like the internet, you don't really need to know how the blockchain works to gain value from it but it does help to have a basic knowledge so you understand the true value of it

What is Blockchain Technology?

According to the authors of the Blockchain Revolution, Don, and Alex Tapscott, the blockchain "is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

What the blockchain is, is a distributed database. To help you envision that, try to imagine a spreadsheet that has been copied thousands upon thousands of times to different computers on a network. Now try to imagine that the network has been designed in such a way that it updates the spreadsheet on a regular basis so that every computer on the network gets the updated copy and that is blockchain technology.

It does go quite a bit deeper than that, obviously. Any information that has been stored on the blockchain will exist as a database that is shared and is continually updated. Of course, this has some obvious benefits – for a start, the database doesn't get stored in one location and this means that all the records on it are public and can very easily be verified. There is no central version, which makes it less likely, in fact nigh on impossible, that a hacker can gain access. Instead, the database is hosted by many computers, millions in fact, and the data can be accessed by anyone who has access to the internet.

How Durable is the Blockchain?

Like the internet, the blockchain has serious robustness built in. Because the blockchain stores identical blocks of information across the entire network, it cannot:

- Come under the control of a single entity
- Have any single failure point

Bitcoin came about in 2008 and since then the blockchain has worked

without any serious disruption. In fact, any problems that have occurred have come from mismanagement or hacking, i.e. human error or intent rather than an issue with the concept of the blockchain. The internet has endured properly for more than 30 years and that is a good omen for a technology that continues to grow and be developed.

The blockchain works because of the following:

It cannot be corrupted and is transparent

The blockchain network exists under what is known as "a state of consensus" and, every 10 minutes, it will check on itself. This is a kind of auditing system; each transaction that happens in each ten-minute interval is reconciled and each of these 10-minute groups of transactions is called "a block". Two very important things come out of this:

- **Transparency –** the blockchain data is stored on the network and is defined as public meaning all transactions are verified by many people and everyone can see them
- **Incorruptible –** because it is so transparent, there is no way to edit or change any transaction without using vast amounts of computing power to get around the network.

Of course, it is possible, in theory for this to happen but in practice, it is highly unlikely. Not only does it require vast amounts of power, if a hacker were able to gain Bitcoins in this way, the value of the coins would be destroyed and there would be no point in owning them.

A network made up of nodes

A node is a computer that is connected to the network via a Bitcoin client. This client carries out the jobs of validating each transaction and relaying them. The nodes each receive a copy of the blockchain automatically when they join the network. Put together, these make up an incredibly powerful sub-level network thus providing us with a revolutionary new vision of how the internet could work.

Each node is a network administrator and voluntarily joins the network. It is this that makes the network decentralized – there is no central authority and everyone is there by choice. However, each of these has a decent incentive for joining – the chance to win a few Bitcoins. This is done through 'mining' and later I will be talking more about Bitcoin mining and how to do it. Really though, the nodes are competing against one another to solve 'puzzles' – not in the

conventional sense though, these are very difficult mathematical and computational puzzles that take a significant amount of power to solve.

Right now, it is estimated that there are more than 700 cryptocurrencies like Bitcoin but the blockchain is moving on from that and there are several other potential applications in development or active already.

The Idea Behind Decentralization

The blockchain is, by its very design, decentralized. Anything that happens on the blockchain is a function of the entire network not just one bit of it and there are some very important applications that come from this. Because we have a new way of verifying transactions, there are a few aspects of commerce as it is today that may become obsolete. For example, stock market trades happen almost simultaneously on the blockchain or some record-keeping could become public, such as land registry. And, like it or not, decentralization has already become a reality.

A network of computers spread across the globe manage the database using blockchain technology. In the case of Bitcoin, all transactions are recorded and that means that Bitcoin is managed by the network as a whole and not by a single central authority. Decentralization ensures that the network works on a P2P (peer to peer or user to user) basis and no one transaction can be recorded and verified by just one user.

Who Will Make Use of the Blockchain?

Right now, the strongest blockchain use cases come from the finance industry. For example, international remittances – according to the World Bank more than $430 billion was transferred in 2015 and the blockchain has the potential to take the middleman out of the equation. When the GUI (graphical user interface) was invented, personal computing entered the domain of the general public in the form of desktop computers. In a similar way, wallet applications are the most common version of the GUI for blockchain and these are required for Bitcoin to be purchased, sold, traded and stored.

Enhanced Security

Because the blockchain data is stored across the whole network, the risks that are inherent with centrally held data are eliminated. The blockchain network does not have any vulnerable points that can

easily be exploited. We all know of the issues that face internet users, especially in terms of security. The traditional 'username and password' system of identity is the easiest one to hack into and that is why blockchain doesn't use it. Instead, enhanced encryption techniques are used for security.

The basis of this encryption is the public and private key pair. The public key is made up of randomly generated numbers in a string and is the address for the user on the blockchain. Any transaction made with Bitcoin over the network are recorded to that address. The private key is similar to the password, providing access to the stored Bitcoin for the owner. This means that, unless you deliberately divulge your private key your data cannot be corrupted.

Why is Bitcoin so different from the currency we are used to?

In one sense, Bitcoin is very much like the fiat currency we use today, the Euro the dollar, the yen, for example, simply because it can be used to purchase goods and services electronically. However, it has one very important characteristic, one that separates it from traditional currency and you already know what that is - the fact that it is decentralized. And because it isn't controlled by any single entity, more people are at ease because it means their money is only controlled by one person – themselves.

Bitcoin was created after Satoshi Nakamoto decided he wanted to produce a currency that didn't depend on centralized authorities, a currency that could be transferred instantly, electronically and with incredibly low fees for each transaction.

Bitcoin is not printed, like our traditional currency is, by a central bank and completely unaccountable to those who spend it, let alone making up the rules as they go along. These banks are able to produce money whenever they want, whenever the national debt needs to be covered and this results in a devaluation of that currency. Bitcoin is digital, created by a community rather than one entity and this community will also process transactions that are made by the currency and this is what makes the Bitcoin its own network for payments.

Another difference is that, where the central banks can churn out money hand over fist, that can't happen with Bitcoin. The rules of Bitcoin, the Bitcoin Protocol, state that the currency has a hard limit of 21 million 'coins' and once the final one has been mined that will be it. However, the Bitcoin is divisible and can be broken down into smaller

parts, right down to a Satoshi, one-hundred-millionth of a Bitcoin.

What is the Bitcoin Based on?

Fiat currency has always been based on and backed up by silver or gold. In theory, you would know that you could get gold from the bank by handing over dollars, or Euros or whatever currency you use (although this doesn't work in practice). Bitcoin does not have this basis. Instead, it is based on mathematics.

Across the globe, millions of computers are using software that follows a distinct mathematical formula to mine the Bitcoin. This formula is open to all to see so anyone can check on it if they wish to. The software itself is also open to all and that too means anyone can look and see what it is meant to do

Bitcoin has several distinct features that set it apart from the fiat currencies:

1. Decentralization – I know I have said it before and you will see it again but this is the whole point of the blockchain and Bitcoin. Remember back in 2013, when the Central European Bank got involved in Cyprus and took people's money away from them, causing an almost total meltdown? That can't happen with Bitcoin because there is no bank or agency that can do that
2. Easy setup - when you go to open a bank account, there are any number of hoops that the banks make you jump through before you can. Merchant accounts are so difficult to set up because of all the red tape and bureaucracy. Bitcoin can be set up in seconds, you don't need to answer reams of questions and prove who your great granny's best friend was and you don't have to fork over any hard -earned cash in fees either.
3. Anonymity. Bitcoin is pretty anonymous; you can have as many Bitcoin addresses as you want and none of them are linked to your name, your address or any other information that can identify you personally. However…
4. Transparency. All details of every Bitcoin transaction that ever happens is stored in the blockchain, which is open for all to see. Anyone can look at your public Bitcoin address and see how many Bitcoins are stored on it. What they won't know is who owns that address and those Bitcoins. There are some things that you can do to muddy your activities on the network, such as using different Bitcoin addresses for each transaction and not making transfers of

large amounts of Bitcoin to one address.

5. Small fees. While your bank may charge you several pounds or dollars for an international transfer, Bitcoin doesn't
6. It is fast. Money can be sent anywhere in minutes, within 10 minutes at the most once the network has processed and verified the transaction.
7. It is non-repudiable. Once a transaction has been done and the Bitcoins sent, you can't get them back unless they are returned by the recipient.

In theory, Bitcoin has tons going for it and practice is also shoring that up. With the price on the rise and set to go even further there has never been a better time to get involved with the Bitcoin gravy train. And so, for the next chapter, we are going to look at Bitcoin mining.

Chapter 2: How to Mine Bitcoin

Bitcoin might well be the next big thing for the finance sector but most people are not really aware of how it all works. And for those of us not into Math or numbers, it can be even more difficult. The thing is, these numbers and the Math are the most critical part of Bitcoin because, without them, it can't work.

As you know Bitcoin is a kind of currency, albeit a digital one. All currencies need four things:

- Checks
- Balances
- Validation
- Verification

Usually, the central authority, normally a bank or a government, will do these things and this is supposed to make any currency difficult to forge while making it easy to keep track of.

The major difference where Bitcoin is concerned is because it is decentralized and because there is no regulation, how do we know that the transactions Bitcoin is used for are accurate?

How do we know that John has sent 1 Bitcoin to Sally? And how do we know that John isn't going to send that same Bitcoin to Harry? The answer lies in the process called mining.

One of the best-known Bitcoin analogies is that it is akin to gold-mining. Just as there is with gold, Bitcoin has a limit to how many there will be and the more that gets taken out of the equation, the harder it is and the more resources are required for finding it. Aside from that Bitcoin is very different from the way it works and, once you understand it, it really is quite ingenious. One of the most important things to get into your head is that mining may not automatically create a Bitcoin. The Bitcoin is provided as an incentive a reward for the miners who successfully validate a set of transactions. But how do they do this?

In order to mine Bitcoin, you must have a specialized computer setup and special software. This software is used, along with a good deal of resources, which we will talk about later in this chapter, to compete with the other miners to solve a complex mathematical problem. Every

10 minutes, each miner will attempt to solve blocks that contain the latest in transaction data and they do this using cryptographic hash functions.

What's that, then?

It is, in its most basic form, one-way encryption that doesn't use a key. The encryption has an input and it will return a hash value, essential a randomly generated value of fixed length. Each word of a message is translated into a code if you like. Take this Movable Type SHA-256 algorithm, as demonstrated by Huffington Post:

The input is a message that says, "How does mining work?"

The output is a hash value of:

46550fef 26f87ddd 5e15407f 45a0b8d2 9513291c 4e0f0acc 24a974de 907a1569

If you were to change just one letter in the message, you would get a different hash value and that is where this works – the very random nature of it is why it is impossible to predict the outcome.

How do hash functions work for Bitcoin?

Because we can't predict an outcome, hash functions are used for something known as proof of work and for validations. Each miner will compete against others to find the input that results in a specified hash value, one that starts with multiple zeroes. It is not possible to measure how difficult these puzzles are but there is also no way to cheat on them simply because blind guesses don't work.

The aim of Bitcoin mining is to use a specialized mining rig to keep guessing until it finds a hash value that is lower than what the target might be. If you can do this first, before all the other miners, you have mined a block successfully but, be aware, this is not a five-minute job; it can take millions, if not billions of guesses, generated by computers all around the world. Whoever 'wins' will be rewarded with 12.5 Bitcoins. You won't technically be making the Bitcoin but the algorithm rewards the miner and helps in verifying the blockchain.

Each of the blocks is created in a sequence and each one contains the hash value of the previous block hence the name blockchain. Because the previous value is held in each block, it is very easy to prove that the order of the blocks. Sometimes, two miners may form competing blocks, each with different transactions and the one that gets picked

for the blockchain is the one that has the biggest amount of embedded proof of work.

The reason this works for transaction validation is that it is very hard to come up with an alternative block or blockchain. Anyone who tried to do this would need to convince every single person on the network, potentially millions of people, that their blockchain is the right one, the one that has enough proof of work in it. Bear in mind that all those millions of other people are working on the right blockchain, the amount of computing power it would take to convince all those people at the same time and beat them would be immense. The only way it can be done is through something called a 51% attack and we will talk briefly about this later.

Who are the miners?

To start with the miners were enthusiasts in cryptography, people who had some spare compute power and could help validate the transactions on the blockchain to get a reward of Bitcoin. Since the value has risen, more people have joined, seeing it as a potential goldmine as it were, with some even investing in entire warehouses full of mining rigs in order to get as many Bitcoin as they possibly can.

To keep the costs down, these warehouses are usually located in places where power prices are low and it is all of this that has made it very difficult for a hobbyist to make anything from Bitcoin mining.

How do you mine Bitcoin?

You need a specialized mining rig which is built from computer components and the hardware comes in three different categories, each one significantly more expensive than the last, not to mention more powerful. By now you understand what Bitcoin is and how it works and you have an understanding of the blockchain. Now it's time to move on to the practicalities of mining the Bitcoin so you can start generating some cold hard digital cash. First, you must determine what hardware you want and to do that, you need to consider two things:

1. Hash rate

The hash rate is the number of calculations that can be performed by your hardware every second as it attempts to crack the puzzle. Hash rates are measured per second as:

- MH/sec – megahashes
- GH/sec – gigahashes

- TH/sec – terahashes

The higher the hash rate of your hardware, compared to the average at the time, the more likely it is that you will be able to solve the puzzle

2. Energy consumption

All this power is going to gulp down the electricity and that won't be cheap. Do look at the energy consumption of your hardware in watts when you make your choice. You don't want to spend all your cash on electricity only to find your rewards don't cover the cost.

By using these factors, you can work out how many hashes you will get per watt of electricity – divide the hash count by the watts. For example, if you a device that hashes at 500 GH/sec, and it uses 400 watts of electric then your hash rate is 1.25 GH/sec. Your power provider can tell you how much your electricity is per watt and you can work out what that is costing you in cash.

Bitcoin Mining Hardware

Now we come to the main categories of hardware for mining:

- **CPU/GPU**

This uses your own computer and is the least powerful. In theory, you could use the CPU on your computer to do your mining but, practically, this would be incredibly slow, so much so that there just wouldn't be any point. You could give things a boost by putting in some extra graphics hardware; these cards have GPUs in them that are designed for heavy lifting in terms of mathematics because they need to be able to calculate complex polygons in the bigger and better video games. Because of this, they are good at the SHA hashing that is needed to solve the blocks.

Choose your GPU from ATI or Nvidia and be prepared to spend some serious money on it. Although they are more expensive, GPU hashing has a distinct advantage over CPU and that is in speed and the number of hashes per second. One of the best things about GPU hashing is that your options are more open in that they can be used with other cryptocurrencies, such as Litecoin. These days, GPU mining is almost obsolete but it can be done. The reason is that the difficulty of mining has increased significantly with the advent of the ASIC mining power that the poor graphics cards simply can't compete. If this is a route you want to take you will need a motherboard that is capable of taking several graphic cards.

- **FPGA**

FPGA stands for Field Programmable Gate Array and it is an integrated circuit that has been designed for configuration after building. This lets hardware manufacturers purchase the chips in large volumes and then they customize them for mining before inserting them into their own hardware. Because of this customization, the performance is much better than the CPU or PU mining and, like the GPU cards, you can have more than one chip.

- **ASIC**

ASIC is where it all happens. An acronym for Application Specific Integrated Circuit, the ASIC has been designed to specifically mine Bitcoin, nothing else and the speeds that it performs are at mind-blowing with, even better, a relatively low cost of power. However, the chips are not cheap because they are designed and fabricated for this one task

Calculate Your Potential Mining Profitability

Before you go ahead and splash out your cash you should calculate the potential profitability. You can find a profitability calculator online and use parameters such as your hash rate, the cost of the equipment, electric consumption and the current price of Bitcoin to see how long it could be before you start to make a profit.

Another important parameter to take into account is network difficulty. This will work out the difficulty of solving the blocks and that will vary as per the hash rate of the network. As ASIC becomes more prevalent, that difficulty is likely to significantly increase so when you do your calculations, increase the metric to see what effect more miners joining in will have on your return.

The next step, once your hardware is in place, is to download your software. If you choose the FPGA or GPU hardware, your host computer must be running 2 things:

- The standard Bitcoin client – this will connect your hardware to the network and will allow it to interact with clients, forward the transactions and helps to track the blockchain. It isn't quick to download because the blockchain is rather large now but the software is designed to take information from your miner to the Bitcoin network.
- Bitcoin mining software – this software is what tells the hardware

to get on and do the work, passing the transaction blocks to be solved through to it. There are several of these so choose the best one for your requirements and your operating system. If you are using an ASIC miner, you may need this software too although some of the newer hardware comes pre-configured, right down to a Bitcoin address.

You are now set up and ready to start mining. But what if you don't want to spend out all that cash and power on the small chance that you will earn yourself a Bitcoin or two?

Join a Mining Pool

A mining pool is basically a group of people who club together and share the rewards. When you are making a decision on which pool, be sure to check out how the rewards are shared between members and if there are any fees. Here are several different schemes for sharing the rewards and most concentration on how many "shares" each miner has submitted as the proof of work. These shares are not the easiest of concepts to get the hang of and you do need to bear 2 things in mind: first mining is all about solving puzzles that are cryptographic and second, mining does have a level of difficulty. When a block is solved by a miner, that block has a level of difficulty that corresponds to it. If the rating of the solution is higher than the level of the whole currency, it will be added to the block chain and the Bitcoin rewarded.

In addition, mining pools set their own difficulty levels – if a block is returned with a difficulty level somewhere between that of the pool and that of the currency, it will be recorded as a share. These share blocks have no use at all but they are marked down as proof of work, a way of showing that the miners are working at solving the blocks.

In this way, the basic payout is on a per share model. Some pools will put a limit at the rate that is paid out per share and some pools may not even have a priority level for miners. Obviously, you also need to consider the deductions made by the pools and these typically range from 1% up to 10%. There are some pools that charge nothing.

Getting Started with a Mining Pool

Now you have decided which pool you are going to use, you can get started by creating your account on the website for that pool – no different to the way you create any other account on the internet. Next, you must create what is known as a "worker" and you can have as many of these for each hardware that you are going to use as you want.

By default, most workers are set up as a number and a password of ‘X’ but you may change this to what you want.

All I can do now is wish you luck with your Bitcoin mining. Next, we are going to look at what we can spend the Bitcoin on.

Chapter 3: Bitcoin as a Currency

Although we are all used to bank accounts, being able to take physical money from an ATM and paying for goods and services with it, many of us are still confused about how it is 'centralized' while the digital currencies are 'decentralized'. Unless you understand what both terms mean you won't be able to see what the benefits of either are.

Centralized Currency – the Downfall

The most commonly heard comment is that fiat currency may be printed on demand whenever it is needed. There are those who believe this to be an over-rated comment but it cannot be denied that governments the world over can "print" more currency when they need or want to. Obviously, as with anything, the more currency there is in circulation, the less value it holds, especially where the currency being printed is backed by its previous value.

This is nothing more than the creation of the illusion of value but it is fair to say that US dollar hasn't had a tangible asset tied to it for a long time. In fact, the only backing that every US dollar in circulation has is "the full faith and credit of the United States" – there is absolutely no intrinsic or inherent value to this whatsoever.

On top of that, when 'new' money has been generated out of nothing, money that has no value at all, the US Treasury will then distribute these extra funds to one of 12 Federal Reserve Banks. One important thing to note here is that two of these banks are privately owned and that leads to an ecosystem that is not transparent, an ecosystem in which a few people are responsible for determining the wealth of the whole nation.

Of course, the term "privately owned" is not necessarily the right description here. Every one of the Federal Reserve Banks can do exactly as it pleases simply because they have no direct government agency overseer. To some, this could be seen as almost decentralized but in this case, this is by no means positive. You only have to look at the numerous financial crises over the last few decades to realize that.

Last but not least, this new money can be injected into the economy by the Federal Reserve, this money that was created out of nothing and has no value – through the purchase of Treasury Bonds. There is,

however, another option, because that worthless money can also be used for purchasing loans that have one single purpose – to finance the massive debt of the whole of the United States of America, or any country that prints this money.

How Does Decentralized Currency Differ?

We know that Bitcoin is the most popular of all the decentralized currencies at the moment and we know that it has a hard limit of 21 million. Beyond that number, there will be no more coins issued and that will mean that every single Bitcoin in circulation at that time will have a value of some kind and will also have the potential for that value to increase as time goes by. However, that isn't set to happen until around the year 2140.

In terms of generating Bitcoins, unlike fiat currencies, there isn't any central institution that prints extra ones. The only way to get Bitcoin into circulation is through the process of mining and, as you know from the last chapter, the Bitcoin is rewarded to the miners who solve the complex equations, giving those miners the opportunity to spend the new coins before anyone else.

Until Bitcoin number 21 million is mined, anyone can take part in mining. You don't need to be approved because Bitcoin is an open ecosystem, allowing people from across the globe to participate. All the funds are under the control of every active miner in his ecosystem and not one single entity – this is what makes it a decentralized system.

On top of that, unlike centralized agencies, Bitcoin doesn't have that single failure point and this is what makes the network more secure and incorruptible. Unlike the fiat currency, where one single agency takes responsibility for controlling the supply, Bitcoin is controlled by everyone, it is consumer-driven, with points of distribution spread all over the world.

Lastly, any Bitcoin that are spent are put straight into the fast-expanding Bitcoin economy, thus circulating constantly whereas fiat currency, once spent, stays out of the ecosystem until it goes back to the bank – that could be a matter of hours or it could be years before that happens. The Bitcoin economy is self-sustainable and is wide open to anyone who wants to use it.

Where Can Bitcoin be Spent?

More and more places are now starting to accept Bitcoin as a form of

payment, with two of the biggest US e-commerce companies recently stepping onboard. TigerDirect.com and Overstock.com have both gone a long way to getting themselves a decent amount of press and not a small amount of goodwill for their decision.

These are online stores but users of Bitcoin can now spend their hard-earned coins in proper brick-and-mortar shops with CVS, Home Depot, Kmart and Sears accepting the digital currency. One of the largest online marketplaces in the world, Amazon.com is also accepting the Bitcoin although, at the moment, you can only use it to buy Amazon vouchers, which you can then spend.

eGifter.com offers more than 150 digital gift cards which can be paid for in Bitcoin and this can be done at the checkout of many national retail chains through an Android or iOS mobile app and, because eGifter uses CoinBase wallet for transaction processing, it is incredibly secure. According to the CEO of eGifter, Tyler Rowe, the beauty of a digital gift card is that you can spend exactly what you want to spend, right down to the cent.

Eventually, it is likely that chain stores like JC Penney GameStop and Gap will start to accept the Bitcoin through their Point of Sale systems but, until then, eGifter is the perfect workaround. And given the number of early adopters that buy and trade in Bitcoin, Rowe says that accepting it as an alternative payment form is a no-brainer.

Sadly, Bitcoin users are lacking in the amount of places they can spend their new currency and, given the huge jump in value in the last year, many users have made a lot of money and want to be able to spend it. Eventually, the bigger retailers will have a choice to make – accept Bitcoin as a payment form or lose out to the stores that will. Obviously, this is not going to happen overnight but companies like eGifter have seen the opportunity and embraced it with open arms.

For now, it is a case of watch this space and check the internet for an ever-growing list of places that your Bitcoin will be accepted as payment.

Chapter 4: Bitcoin as an Investment

When you make the decision to invest your hard-earned cash in something it shouldn't be a decision that you take lightly. You need to carefully evaluate the investment and that evaluation should be based on an analysis of the investment and a technical analysis of the pricing trends.

The same applies to Bitcoin and, before you invest in it, you need to know exactly what it is, how it works and how it is used. Bitcoin isn't a stock because there isn't any company structure or company information to back it up. And, unlike a company Bitcoin doesn't have a physical product that company managers can give us an estimate or forecast of future sales on. Unlike a bond, Bitcoin has no underlying interest rate or any assured payment of principal either.

Fundamental Analysis of Bitcoin

When you do a fundamental analysis of Bitcoin, with a view to investing in it, you will need to use different metrics to what you would use for a bond or stock. It is, however, a necessary step to take before you jump in and throw your money at it. First, you need an understanding of Bitcoin and once you have that, you can continue with your analysis of it as a sound investment.

Learn about the role that Bitcoin plays as a currency form and evaluate things like the total supply of it. You can also track all Bitcoin transactions, and you can get a look at the creation stats. Make yourself aware of how many wallets there are, both existing and newly created. This will give you a good idea of the data and the trends that you need to consider.

Technical Analysis of Bitcoin

One of the major factors that highlight investment maturation and gives you a basis for trading is when the investment in question can be technically evaluated. Bitcoin has been in existence for 9 years now and there has been sufficient trading on Bitcoin exchanges that make a technical analysis appropriate. When it was first introduced and was very thinly spread out, it was vulnerable to wide swings in price and when an investment is like that it is very difficult to apply the technical analysis rules to.

Right now, investors and traders in Bitcoin depend on a technical analysis evaluation of the price trends as their driver behind their investment. The theory is, investment prices always move in trends and by mapping these price changes over a period of time, it should be easy to spot the trends. These will often give an indication of whether an investment is increasing in price (an uptrend) or decreasing in price (a downtrend). Over time, we can start to draw lines between the high and low prices, allowing us to better see fluctuations in the trends. These are called channels and these will sometimes create a natural range, indicating when an investment hits a resistance level, which is when it is attempting to increase within the range, or when it hits a support level, which is the floor of the investment. On top of that, you can use candlestick charts or head and shoulders to give you further analysis. Provided you apply the technical analysis effectively, you should be able to see when that investment is going to break out of its range and this is an indication of an increase or decrease in the price.

Right now, Bitcoin is enjoying heady heights in terms of value, trading at just over $2000 per coin although it did go as high as almost $3000. This is fantastic news for the very early investors who were purchasing Bitcoin for fractions of a cent or the early miners who were accruing 25 Bitcoin rewards for mining the blocks. This isn't a sudden increase; the value has been climbing steadily for the last 9 years but, perhaps because it has been known to crash, and other factors, there are still many people who are reluctant to put their cash into Bitcoin.

One thing that definitely won't have helped that is Mt. Gox. The once popular Bitcoin exchange suffered a hack, resulting in the theft of hundreds of thousands of Bitcoins – this is where decentralization falls down; because there is no regulation, once the Bitcoin are gone, they are lost forever. Or maybe the fact that Bitcoin is so volatile, 26 times more so than the S & P 500, and the lack of oversight by the government is causing speculators to forecast imminent disaster. This is, in some ways, understandable; Bitcoin doesn't have the backing of gold or silver, it doesn't have the backing of a country or even a bank. Its only backing is sentiment and, although there are advantages to this kind of system, there are also some dangers and obstacles that must not be ignored. If you are willing to take that risk though, Bitcoin could well be the one risk that pays off handsomely.

So, Should I Invest in Bitcoin?

There are a number of reasons why you should seriously consider

Bitcoin as an investment tool:

1. **Incredible growth**

Although Mt. Gox caused a serious setback, Bitcoin has recovered immensely and is now on a path to rapid growth. Just a couple of months ago, the value of Bitcoin shot past one troy ounce of gold value and is now experiencing even bigger margins over the price of gold. If you had invested years ago, say $100 in 2011, your investment would now be worth around $600,000.

2. **Fixed supply**

We know that only 21 million Bitcoins will be released and by 2140 we expect all 21 million to be in circulation. Every year, the number of Bitcoin due for release is cut in half, slowing down this process immensely. Some say that a fixed supply currency is counterintuitive; after all, with fiat currency, if we need more we can get it printed, thus pushing more money into circulation.

The official Bitcoin website says, "Bitcoin is intended to inflate in its early years and become stable in its later years... With a stable monetary base and a stable economy, the value of the currency should remain the same." Although there is the chance that a lower supply of currency will result in people hoarding it and thus causing deflation, this is not likely to happen to Bitcoin because we know that the supply is fixed.

3. **Effective diversification**

Bitcoin is fast starting to be taken note of more seriously by investors. 5 years ago, it was barely heard of, now it's everywhere. There are Bitcoin-specific kiosks now for trading and the currency is in use virtually every day for transactions, trade and for investment. Adoption rates are up and trust has strengthened significantly.

Cryptocurrency is on the rise as more and more alternatives to Bitcoin are released, known as altcoins, flooding the market and you even have the likes of JP Morgan Chase, Microsoft, and Intel backing Ethereum, another blockchain currency. Investors are looking for better, more unique opportunities and Bitcoin is the leader in a race of viable alternatives for both retail and institutional investors.

Bubbles

In order to fully understand the risks involved in trading, be it with

Bitcoin or something else, you should understand about bubbles. The price of digital currency has shot up significantly since the start of 2017 and that has led to no small amount of speculation as to whether the market value is exceeding the underlying value.

This happens when speculators push the price of the asset up to a height that is simply not sustainable and this causes what is known as a bubble. Like all bubbles, they must pop at some point and with a financial bubble, that can cause ruin to some, especially those who bought when the price was near its ceiling. Not only that, a strong speculative bubble can cause investors to steer clear as they don't want to get caught in the fallout.

The extreme growth in digital currency price is causing no small amount of concern in some areas. In contrast to NEM and BitShares, Bitcoin's price has risen by a modest amount, just 290% since the start of the year. NEM has seen an increase of just over 8000% while BitShares has risen by more than 11000%. This kind of growth is surely not sustainable and, as has been seen many times over the years, such increases inevitably lead to the bubble that pops with a loud bang.

Although some investors are warning that Bitcoin and other cryptocurrencies should be avoided until that bubble bursts, there are those who argue that bubbles are impossible with a digital currency. This is down to bipolarity in the market and, as George Soros tells us, "market conditions are "reflexive" due to the synchronization cognitive and manipulative functions".

Cognitive function is the part where economic participants will look at the fact and assess them for what they are while the manipulative function is where facts are turned to gain an advantage. As soon as the cognitive is affected by the manipulative, neutrality is put in a different light because it turns into the fact that has been manipulated. Because of this, markets tend to reflect the perspective and views of their participants, rather than the big picture and scope of the economics.

Historic Bubbles

One of the most historic bubbles was the Dutch Tulip Mania. Dutch traders began selling tulip futures, resulting in prices wildly diverging from the value that underpinned the asset. Traders bought these futures for one reason only and it wasn't because they really wanted tulip bulbs. It was because they planned on selling the contract for a

much higher price at a later date. This continues until the value of a single bulb went higher than the price of a luxurious house in Amsterdam. As could have been predicted, as soon as the market saw no new investors, the price collapsed and the tulips went back to a normal price.

Another example is the South Sea Bubble. 1711 saw the creation of the South Seas Company, intent on enjoying the same kind of success that the British East India Company had. By making a significant payment to the British Treasure the company was given exclusive rights to trade with South America and, investors, expecting to see huge returns and believing in the massive amount of hype, poured money in, and the stock price so up beyond belief. Sadly, for the investors, it wasn't long before it became clear the company could not succeed and the price plummeted to zero.

How to Be a Successful Investor

If you want to have success at investing in Bitcoin you need to do the following 3 things:

1. **Have a good plan**

You must have a strategy, especially when you are investing in something like Bitcoin. It doesn't matter if you intend to be a day trader, if you want to make enough money to pay your debts off or retire with a decent amount of money, it must be something for you to work for. Each scenario will provide you with a framework to make the decision on the risk reward payoff.

Let's say that you are a student and you have student loans that you need to get paid off. You might consider investing $100 now with the hope that, in 4 years' time, you can pay off those loans. Or, you could be a software developer and you invest $10,000 with the intent of retiring in 10 years' time on your profits.

If their Bitcoin holdings were to grow to $100,000, the student would know that his goal is reached and he can cash out, safe in the knowledge that he has the money he needs. The software developer, on the other hand, knows that $100,000 is just not enough and will need to keep holding. If you don't have a framework to work to, you won't know when the time is right to get out of the market.

2. **Expect the price to drop**

The price of Bitcoin will drop and it will probably freefall at a much

higher and faster rate than any other investment that you have ever made. Because Bitcoin is pretty much exclusively held by speculators, this kind of volatility is normal and, right now, its price is far more stable than it has ever been in the past.

There is no way of knowing if the blockchain technology will cause disruption to finance in the same way that the internet caused disruption to communications and there is no way of knowing if it will be displaced and shoved in the bin like other inventions. Bitcoin is as volatile as any tech startup and that is what is fostering the belief that there are potentially huge financial gains to be made.

3. **Secure your Bitcoins**

Every Bitcoin owner has 100% control over their own funds and with that immense power comes no small amount of responsibility. Aside from doing yourself down if you opt to sell low, you are also at risk of losing your Bitcoins to theft or malicious activity if you don't secure them properly.

It is reasonable to say that around 90% of Bitcoin theft comes from those who put their funds under the trust of another person and this is hugely ironic because the whole idea of Bitcoin was to remove that trust and put in yourself. The idea was to have a cryptographic system of electronic payments where two parties could trade between themselves without the need for that third party.

Whenever your Bitcoin funds are held in a wallet online, in an online exchange or even within a wallet, they are at a much higher risk. Businesses can be hacked, they may use poor management or an insider could steal the funds. The more people there are that use the service, the bigger the prize in a successful theft.

When you are considering where to put your Bitcoin, you need to think of a number of different factors:

- Who is the owner of the company?
- What is the location of the company?
- What, if any security features do they have in place?
- How is this business making money?

There are unscrupulous businesses that set up as a Bitcoin business with one goal in mind – to take your money.

Unfortunately, you can't even eliminate this threat by storing your Bitcoin on your computer or your mobile devices. It will cut down the size of the target but there is little to stop your device or computer from being hacked, of you being the victim of a convincing phishing scam or of infection through a virus.

You can keep your Bitcoin on a computer that is fully up to date, is properly password protected, preferably with 2-step authentication where it can be used, and one that is less likely to become infected.

If your investment grows significantly, one of the best things you can do is consider an offline paper wallet that is fully encrypted and keep it stored in a safe place, such as a safety deposit box. That will eliminate all the risks we talked about but it does reduce access to the funds on the wallet.

If Bitcoin is successful in getting to even a small fraction of the price predicted for it, provided you follow these steps, you will see benefits in an investment in Bitcoin and the blockchain technology.

Chapter 5: The Opportunities and Risks of Investing in Bitcoin

When the value of Bitcoin shot up above $1000, it wasn't just the media that was alerted. All the media was flooded out with reports, large numbers of investors also showed renewed interest as they looked for alternative ways to generate better returns in the climate of low-interest rates.

When you look at Bitcoin from the perspective of an investment, it tends to be compared to gold than to any fiat currency. The reason behind that is that gold and Bitcoin are both assets with a lot in common. Both have limited supply, both have a functional use and both are thought, despite the fact that they are so volatile, to be excellent stores of value. When the two assets were compared in investment terms over 5 years, Bitcoin far outperformed gold with an annualized return of 155%; gold showed an annualized loss of 6% for the same period. These returns are a good indication that Bitcoin is generating a good deal of excitement from investors looking for a new class of asset.

The soaring value and a proven performance record for investors, against the gold standard, are also indicators that now is a good time to weigh up the opportunities and the risks of investing in Bitcoin.

The Opportunities

There are those that argue that Bitcoin and other cryptocurrencies have only got a value because we perceive it to have one. For this reason, Bitcoin critics see the price growth as just a bubble but there are, in fact, a few drivers behind the returns that have absolutely nothing to do with speculation or hype:

- **A cashless society**

We all know that we are headed for a cashless society; we all use electronic payments services, like credit or debit cards, making payments by mobile phone, etc. Bitcoin has a definite place in this society as it can easily be used to make transfers and payments from any mobile device anywhere in the world.

- **Demand from emerging markets**

Developing countries are showing an increased demand for Bitcoin, largely those countries that are suffering economic distress and weak currencies. For example, a pie in the demand has been witnessed in Bolivia, Venezuela, Brazil, Turkey, and Columbia, mostly because their own currencies are significantly weaker and have far less value than they used to have. Right now, demand for a form of international currency, accessible by the internet is high and, like gold, when there is uncertainty or economic distress, the price rallies, driven not just by speculation but by genuine demand.

- **Not everyone wants a bank involved**

This is a significant reason for the increase in demand for Bitcoin – many individuals prefer control of their own money and not leave it to a bank. By storing your capital, be it all or part, in a Bitcoin wallet, and being able to use it to buy services and goods, you can be your own bank and you won't need the intermediaries that banks use for conducting transactions. This development has strengthened as the Bitcoin economy has grown, now including saving accounts, prepaid debit cards, and P2P lending, amongst other things.

Risks

Although Bitcoin has shown very impressive annualized returns in recent years, the stark reality is, the currency is still very young and we have no way of knowing whether it will become accepted across the world or whether it will disappear as fast as it arrived. All this uncertainty is firmly reflected in the volatility of the price.

When it comes to investing your money in Bitcoin, there are a few risks that you need to keep in mind:

- **Regulatory**

Regulatory risk is the single biggest risk that the future of Bitcoin faces, be it as a currency or as an investment class. Let's say that China implements a ban on any citizen holding Bitcoin; the price would come crashing down quite spectacularly simply because it is the largest trading market, with more than 90% of Bitcoin trading occurring there. Any negative changes in regulation would affect Bitcoin investment the world over.

- **Scalability**

Another risk is if participants of the network failed to agree on the handling of scalability issues. If Bitcoin is to be successful, the

blockchain must be in a position to handle much higher volumes of transactions than it does now and in a much shorter time. Right now, transactions usually take anywhere between 20 and 40 minutes, great for transfers aboard but not when all you want is a cup of coffee. If changes to scalability cannot be agreed it could lead to Bitcoin struggling to be classed as a transactional currency.

- **Large-scale hacks**

Large Bitcoin companies and exchanges have a potential to suffer losses from cyber-attacks and this has influenced price in the past. Mt. Gox is the perfect example, pushing the price of the currency down. Since 2009, almost a third of exchanges have been the victims of a hack and, although there have been significant efforts to shore up security, the risk of a large-scale hack is real and is likely to happen again. That said, these hacks only tend to have a very short-term effect on the value of Bitcoin and shouldn't have any effect on the price development over the long term.

- **Altcoin take-over bid**

Another of the risks that are often talked about is the potential for another digital currency to take over and become the strongest option for investment. Bitcoin does have a few issues, like scalability, which another digital currency could improve on or eliminate. However, the Bitcoin has the first-mover advantage and a fast-growing economy that has put it in a firm position as the leading currency that a takeover seems unlikely. Not only that, Bitcoin has outperformed a whole heap of other digital currencies so, from the point of view of an investor, holding on to Bitcoin will most likely be the better bet than putting your money on the altcoins taking over.

- **51% attack**

This is the one risk that most investors will not be aware of. A 51% attack is when a single centralized Bitcoin mining operation gains more than 50% of the total control of the blockchain. By doing this, they would then be able to reverse transactions and this would make the blockchain unusable because there would be no trust left in it. Right now, mining is spread out over a wide scale and the network is totally decentralized. To be fair, the computing power needed for a takeover of this kind is so immense and the value of the Bitcoin would plummet significantly if it happened, that it isn't likely to be a real factor. The risk should always be considered though.

Chapter 6: Bitcoin vs Other Cryptocurrencies

When you do some serious research on Bitcoin, you will notice a pattern in the way that people think of Bitcoin as they begin to discover the ecosystem that surrounds it. Normally, their thoughts are something along these lines:

1. Bitcoin is truly amazing! There are only so many ever going to be released and I can have great control over my own money! How do I get my hands on some?
2. Bitcoin mining sounds like it could be cool. That's where the real money will be made. How do I get started on mining and make some Bitcoin?
3. Mining looks hard, too difficult for me. I think it would be easier if I just bought some Bitcoin. Where do I get it from?
4. Great, I've got some Bitcoin! What are all the other coins I keep hearing about though? Are they going to take over and will I lose money on Bitcoin?
5. I think Bitcoin might well self-destruct at some point so I want to hedge against that. Should I consider buying some of the other altcoins?
6. I can't look into all these altcoins, I don't have time and there are way too many of them? How do I pick one?
7. I know what I will do! I will just buy the most popular, they are the ones most likely to do well against Bitcoin.
8. Mm, the popular altcoins have high prices, a bit out of range of my wallet. Maybe I will just buy one of the smaller ones

Most people will stick at one of these and never move on. For example, there are people who have never paid a single cent to buy a Bitcoin and have, instead, mined all the ones they own. They will happily spend a good chunk of money on the equipment needed but won't part with the money to buy a Bitcoin. Others happily stay with Bitcoin and never even bother to look at altcoins while others hedge with just about every altcoin in existence. The point is, the pattern of trying to find the right way to invest in a new innovation is predictable but it shows that we are all different and we are all convinced by different things.

Why do People Buy Altcoins?

For the most part, altcoins are used as a way of hedging against Bitcoin and these are the most common reasons why:

- There is a chance that Bitcoin could be the subject of a catastrophic failure that doesn't affect the altcoin
- The altcoin may a utility in the future that is far better than Bitcoin and this would allow the altcoin to overtake the Bitcoin
- Bitcoin may continue as an incredibly valuable cryptocurrency but there may also be room for the altcoins to join the market in another niche. This would make them reasonably good bets on their own.

Let's go through each of these.

The Bitcoin Catastrophe

There is more than one way that the Bitcoin could suffer a catastrophic failure. The first way would be as a result of a technical flaw, such as a bug that would allow Bitcoins to be stolen. The second way would be an economic flaw, such as a change in code that gave millions of coins to someone for some reason. And the third way would be a consensus flaw, such as Bitcoin splitting into two coins that are roughly even.

A technical flaw could be a cryptography vulnerability in Bitcoin or a security issue in the consensus code that was easy to exploit. Cryptographic vulnerabilities could also extend to altcoins as many of them use the same libraries and, in the same way, the security vulnerability could be shared among all the coins with the same code.

Whatever, it is well worth asking the question of what the potential consequences would be if something of this nature did happen. First, provided the vulnerability was caught in time, Bitcoin would most likely patch it and then quickly fork to cut down the exposure to that vulnerability. Something of this nature has already happened with Ethereum and a fork was the result.

Perhaps a better question would be to ask what would happen if the vulnerability weren't caught in time. Most likely, this would result in a massive price drop, not just affecting Bitcoin but just about every altcoin in existence, simply because confidence and trust in cryptocurrencies would be shaken to the core. After all, how could you be certain that one of these vulnerabilities wasn't lying undetected in

all the altcoins?

Economic flaws would encompass changes the economic rules that govern Bitcoin. To date, this has never happened and it has never even been discussed. What we know is that Bitcoin needs a very strong consensus if it is to change and any change of that nature would require the complete support of virtually all the community. Catastrophes like this tend to be prevented before they can happen.

That said, to prevent the potential for economic and technical flaws requires a development team that is dedicated, talented and trustworthy and that the risks are hedged against. The same risks do exist in the altcoins and it should be pointed out that Bitcoin is one of the few digital currencies that already has a natural hedge, in the form of the alternative clients, against a degradation in development.

The last flaw is the real reason why you should use altcoins to hedge against Bitcoin. A long debate on scaling has shown that the community is open, even on a small part, to a split in Bitcoin. Suggestions have included a soft fork activated by users or for the activation of a consensus-busting feature. Both of these are symptomatic of Bitcoin not having any real leader and the fact that it is not an authoritarian system. Most of the altcoins do have a creator who is a de-facto dictator, albeit a benevolent one, for their own currency. The risk lies in the fact that Bitcoin does not have this but that is also seen as a benefit, due to the reduction in the risk of economic law.

Future Utility

Most of the existing altcoins are technically different to Bitcoin and this is most often the reason why some people choose to invest in them. This is down to the thought that the altcoins not only have the same utility that Bitcoin does, as a digital currency, they also have something extra. This makes the altcoin very useful, more so than Bitcoin and can result in a takeover.

In one sense, this is absolutely correct. If you have two products, the altcoin that exists in the vacuum would do as well, if not better, than Bitcoin existing in that vacuum. Even if the basis of the code were significantly different but they both had similar economics, they would pretty much have the same effect in that vacuum.

Of course, we are not living in a vacuum and the very fact that Bitcoin exists has an effect on the future utility. If a feature has been shown as useful, Bitcoin is likely to adopt it in one way or another so it goes

without saying that most of these features that altcoins have not been shown to be useful and fit for adoption by Bitcoin.

If an altcoin were to show some usefulness, Bitcoin could add the extra utility in one of a few ways. First, if Bitcoin decided that the feature was useful enough, it could add that feature into itself. Confidential transactions would be an example of this, a feature that is being proposed for a sidechain to Bitcoin. However, there are some features that would be in conflict with the current use cases of Bitcoin. For example, we all know that Bitcoin is one of the best stores of value and if a feature were introduced that would add a much large surface for an attack, unless it could be truly justified, it wouldn't be added in. However, entrepreneurs can always add in a similar function and still make themselves a tidy profit. Given that it isn't easy to change consensus, this is the path that would most likely be chosen to bring new innovation into Bitcoin.

In other words, the altcoins don't just need to compete with Bitcoin; they also have competition from every entrepreneur that is looking to use Bitcoin to build on. Hence, while it may make sense to use the altcoin to hedge against Bitcoin, most likely Bitcoin will, in one way or another, consume any other use case, thus cutting any advantage that an altcoin might have had.

Another Niche

While altcoins have already attempted to carve out their own niche, they haven't always been as successful as they would like. The main way that a niche coin would truly make sense is if to were capable of something that Bitcoin wasn't or wouldn't do. This kind of usage is much like the argument for future utilities but on a much smaller scale and, to be honest, the same argument does apply to both cases. Entrepreneurs have all the incentive they want to bring profitable innovation into Bitcoin, an innovation that is like the niche, given that they have a much bigger user base with which to work.

So, What Makes Bitcoin Different?

The two biggest advantages to Bitcoin over any altcoin are the network effect and the fact that security has been tried, tested and proven. Both of these are serious advantages that are almost insurmountable. Bitcoin has that proven case as a store of value and most altcoins are attempting to carve out something different but based on smaller use

cases, like anonymous purchasing, prediction markets, and decentralized domain name servers.

Bitcoin does have a long lead over the altcoins in that it has been in existence for longer without any real failure. Bitcoin security has already been proven to be strong and has proven itself more than once when pitted against the younger altcoins, with usage under just about every metric far exceeding the others.

Not only that, but Bitcoin is was more accessible than the altcoins, having many more exchanges, more software, more merchants and more hardware as a support for it. Bitcoin is more liquid, having way more volume than any other altcoin. It has the biggest ecosystem in terms of developers and has more software and more implementations than an altcoin does. It also has the biggest number of entrepreneurs busy creating Bitcoin companies, with a serious amount of dedication, intellect, and creativity being put into making Bitcoin eminently more useful.

When you go head to head in a competition against Bitcoin, you aren't just in competition with its significant user base, mining operations, and development team; you are also in competition with the huge ecosystem of Bitcoin startups, entrepreneurs and other open source projects built around it.

To try and make this a little clearer, let's imagine that a coin has been created to help with filtering out spam email. It's got a name, we'll call it a SpamCoin. The SpamCoin is an altcoin that gives you the ability to send a message to another person but only if you are prepared to pay them with some SpamCoin. Suppose this ends up being an incredibly useful service and loads of people adopted it. This would make the SpamCoin very valuable but what else would happen?

It is highly unlikely that Bitcoin would adopt the features of SpamCoin directly, although they could add it into a sidechain. There is, however, a very strong likelihood that an entrepreneur would take the idea of the SpamCoin and come up with their own service that was based on the Bitcoin. For starters, this would have a much bigger user base to begin with and there would be no need to use the actual SpamCoin. The entry barrier would be much lower and, in the end, this new service, built on Bitcoin, would have a much better network built in that could affect significant advantages over what the original SpamCoin could do.

That is not to say that SpamCoin would not win but it does have much

longer odds.

There is absolutely nothing to suggest that an investment in altcoin would be a bad thing. Every investor must evaluate their own needs and look at their own risk to reward ratio; they would need to determine whether that ratio fits in with their goals or not. What we do know, in all truthfulness, is that using altcoins to hedge against Bitcoin isn't a great idea. Much of the same risks that exist in Bitcoin also exist in the altcoins and most of the rewards that could potentially be gained would be instantly consumed by Bitcoin.

It is perfectly possible that an altcoin could take over from Bitcoin but it would need to show a much better utility, a present one, not a future one and it must be able to show growth that is competitive with the Bitcoin network before the Bitcoin ecosystem can get in and put the same feature in place.

As Bitcoin continues to evolve, we can expect to see some unexpected growth as new uses and utilities come to light. If you own Bitcoin, you can rest assured that its usefulness is only going to increase and, by contrast, those with altcoins will find themselves with significantly more risk of their coin of choice falling by the wayside. In other words, the Bitcoin has already gone around the field and lapped all the competition. It has the resources and it has the ecosystem needed and that comes with serious advantages. If there are two things that Bitcoin has going for it, it is entrepreneurship and stability, both of which exceed the altcoins by a long way and will make it very difficult to catch up, let alone overtake.

Chapter 7: Top Tips for Investing in Cryptocurrencies

If there is one fact regarding trading that should not be ignored, it is that you should come to terms with and accept the fact that you will never be able to time your buying and selling perfectly. Seriously, what is the chance of you being able to purchase when the price is at its real low and then sell when it is at its exact top? Add to that the need to put sufficient capital into the trade to make some kind of dent in your wealth and you can see how hard it is. Trading is by no means cut and dried because there is not one single path to take. Each trader has their own goals when they are trading and investing and cryptocurrency is no different.

If you have been involved in trading then you will already know what it is like to lose on a trade that didn't work as expected or one that worked fantastically but didn't give you the position size you desired. The best you can do is live in the now and forget about the past – you can't change it anyway and hindsight is such a wonderful thing. Yes, it would have been wonderful to have invested in Bitcoin when it was at a fraction of a cent and then cashed out when it reached more than $2500, but that, sadly, just isn't how things work. Think about it the other way – you buy into Bitcoin when the price stands at $600 and then it plummets to $100, you panic and sell out – that would be very painful. We can't do anything about the past and there is no way we are going to predict the future. So, all can do is learn from our mistakes and use that knowledge going forward.

The following are some top tips for those new to investing in cryptocurrencies.

- **Understand Just How Powerful Cryptocurrency Is**

We tend to look at this the same way as we do when we invest in stocks but cryptocurrencies are commodities, not stocks. Yes, both have a price but they are very different with the only real similarity being the exchange. We already know that the blockchain technology that backs Bitcoin is being studied for the potential to change retail and

institutional capital and the decentralized nature of cryptocurrency means that there is no way to shut it down and no way to easily manipulate it. When people ask why you want to invest in cryptocurrencies like Bitcoin, you can tell them that it is the safest investment anyone can make and that you believe in the future – for as long as Bitcoin capital continues to flow, its potential will continue to be realized.

- **Always Have a Strategy**

How often are you going to buy and sell? There are those that just want to be day traders but it has already been shown that your best bet could be to hold. The rule of thumb is that the longer you hold, the less risk there is and this rule works for cryptocurrency investments as well. However, sometimes it will be better to cut loose and get out and one of the indicators for that is when unforeseen structural issues cause declines in price. Always make sure you have a strategy in place that covers all eventualities.

- **Start Small**

One of the ways to cut risk in sudden changes with Bitcoin and other cryptocurrencies is to average the dollar cost of your purchase. This takes the sting out of sudden changes in pricing and cuts your reliance on a single entry point. Increasing your investment over time you cut out the need to buy and sell too often. Cryptocurrencies are here to stay so there is no need to go all out and fill the coffers straight away – unless of course, the prices drop to all-time lows!

- **Hedging Your Bets**

Some exchanges are happy to allow short orders – this lets you place a bet on either side of the price movements. For example, you could go 10% short and 90% long which would assume you have far more confidence in the long run. This kind of strategy can cater to all risk levels.

- **Altcoin Trading**

Never forget about the power of the altcoin. Bitcoin is not the only cryptocurrency in the world and the altcoins are not quite so prone to the public speculation. They have much smaller market caps which are

more prone to bigger pricing swings but each one has its own purpose and it has an intent. The risks of investing with altcoins are bigger but the rewards can also be much bigger too. Some, like Ethereum, are more stable while some are at a higher risk of fluctuation so allocate your percentages per your own risk tolerance. For example, you could put say 50% into Bitcoin, 30% into Ethereum, 15% into DASH and 5% in ZCash

There are plenty of rules and tips for investing but, on the whole, where cryptocurrency is concerned, you can get away with following the same guidelines as for other investments.

In our last chapter, we are going to take a short look at some of the terminology you may face when dealing with Ethereum, the blockchain, and other cryptocurrencies.

Chapter 8: Cryptocurrency Glossary

Trading:

- Exchange - a website where cryptocurrencies can be bought and sold
  Fiat – currency issued by a government, such as the USD, Euro, etc.
- Whale – a person that owns an eye-watering amount of any cryptocurrency
- Limit order – similar to a 'for sale' sign, this is an order to buy or sell when the price reaches a certain amount
- Margin Trading – risking all your coins to magnify your trading intensity – this is incredibly risky and should NOT be done by beginners
- Going Long – margin trades that will profit if the price increases
- Going Short – margin trades that will profit if the price decreases
- Bullish – expecting the price to go up
- Bearish – expecting the price to go down
- Altcoin – alternative cryptocurrency to Ethereum or Bitcoin
- ATH – all-time-high
- ETH – the token from Ethereum mining

Tokens:

The currency of the blockchain network projects that raise money through the issuance of tokens:

- ICO – Initial Coin Offering – the initial offering by a startup in exchange for 'currency". Pretty much Ethereum crowdfunding
- Shilling or Pumping – an advertisement for another cryptocurrency. For example, if a digital coin were promised to be the next cure for cancer, it would be called shilling
- Stable Coin – a coin that has a very low level of volatility and can be traded against the whole market
- Arbitrage – finding a difference in a commodity price on different exchanges and taking advantage of it
- FOMO – Fear of Missing Out – the overwhelming feeling that, when a price starts to go through the roof, you need to get on and join in
- FUD – Fear, Uncertainty, Doubt – a negativity without any base

that is spread by a person who wants to drop the price of something
- FUDster – the person spreading the FUD
- Pump and Dump – recurring cycle of one of the altcoins receiving high attention, pushing the price up which will then, inevitably, crash
- Bagholder – a person who is still holding on to an altcoin after the pump and dump crash.
- Market Cap – the whole value that a cryptocurrency holds, calculated by the multiplication of the total coin supply by the price of a single unit
- ROI - Return on Investment. The percentage of the total made compared to the initial investment. For example, 100% ROI would mean that the money has been doubled
- TA – Trend or Technical Analysis – the process of looking at current charts to predict the next movement in the market
- MACD – Moving Average Convergence Divergence – trend indicator that shows a relationship between the moving averages of two prices

Related to Cryptocurrency in General, Not Specific to Bitcoin:

- Blockchain – the technology behind Bitcoin, Ethereum, and other cryptocurrencies
- Node – a computer on the network that has a copy of the blockchain and maintains it
- Mining – the process of solving a block of transactions
- Mining Rig – the hardware required for the processing of the Proof of Work blockchains
- Fork – where the blockchain has been split into two
- PoW – Proof of Work, the current consensus algorithm that Ethereum uses
- PoS – Proof of Stake – the future algorithm that Ethereum will use
- Sharding – blockchain scaling solution. Right now, a copy of the blockchain is held on each node. Sharding allows each node to hold just a partial copy of the entire blockchain to increase consensus speed and network performance

- Software Wallet – where cryptocurrencies are stored. The wallet is a software file on the internet and can usually be generated free of charge
- Hardware Wallet – a hardware device that stores your cryptocurrency securely, one of the most secure methods of storage
- Cold Storage – moving your stored cryptocurrency offline for safe keeping. Methods to doing this include printing out a QR code for your wallet and storing it, using a hardware wallet or by moving the software wallet files onto an external storage source and then storing that somewhere secure

Conclusion

Now you know more about Bitcoin how it works and what it is used for, and hopefully you understand the blockchain a little more than you did before. It is clear that both Bitcoin and the blockchain are here to stay and that they will effect a huge change on the world in the future, not just in terms of the financial world but in our own day-to-day lives. It will become easier to send money, to make payments and to buy goods and services but, more importantly, it will become more secure. Government agencies, banks, and other previously centralized businesses will become accountable for their actions; so-called mistakes will be harder to hide and everything will be traceable back to its origins. Control will go back to the people.

Cryptocurrencies are just one small part of the revolution that is beginning to gather pace. The blockchain technology that underlies the digital currencies is taking shape as the technology of the future, a technology that has the potential to shake things up in a big way It is no surprise that some of the banks and governments are not interested in the technology because, although it will significantly decrease fraud and, as a result, the costs incurred through fraud, it will also decrease the chances of corrupting in high places. Eventually blockchain voting will be introduced and that alone will cause upset in the political world – everyone will be more likely to vote and that will have a significant impact on the results and election fraud will become a thing of the past.

Although there are those that say the time to invest in Bitcoin has passed, I hope you now realize that it hasn't and Bitcoin should not be dismissed out of hand. The time is ripe and, although the price may fall again, it is predicted to rise sharply in the next few years. The time to pick an investment and stick with it for the long-term is now and that investment, if not in Bitcoin should definitely be in blockchain technology.

ABOUT THE AUTHOR

Richard Ozer has nearly 30 years of professional experience as the CEO of Office Information Systems, and has provided hundreds of businesses in the California Bay Area with technology consulting, systems integration, database application development, and sales & service. He is a significant interest in the cryptocurrency market and advocates digital currency as an asset class for high net worth investors and regular individuals alike developing their financial portfolios.