THE PEOPLE'S MONEY BITCOIN

ADAM TEPPER

ISBN 9780646941981

CONTENTS

FOREWORD

By Adrian Przelozny

Adam Tepper tragically passed away in a traffic accident in February 2015, before he had the chance to complete this book. As Adam's close friend and business partner on countless projects, I was duty bound to finish what he had started by completing his manuscript and bringing this book to print.

I would like to stress that although I have made some changes and edits to his book, I firmly believe that they are in line with what Adam would have done himself, had he gotten the chance. This book then remains the work of Adam Tepper and has stayed true to his original concept.

A special thanks goes to all those who have donated funds to Adam's family and also via the donation page set up by the Bitcoin Association of Australia to assist with the publishing costs of this book. Thank you also to the Bitcoin Embassy - Australia and others who have volunteered their time to proof read and provide feedback on the book at various stages.

Adam was a warm-hearted, intelligent and passionate young man with a clear vision for a future where Bitcoin could change people's lives for the better. Adam's favourite author was Richard Feynman, for his ability to explain complex and seemingly inaccessible concepts in clear and simple terms. This is a talent which Adam also shared, and this book is a great example of this. I hope you enjoy the following pages whilst learning about Bitcoin through the words and thoughts of Adam Tepper.

- ***Adrian Przelozny***

Adam Tepper
13-Feb-1981 - 26-Feb-2015

INTRODUCTION

By Adam Tepper

As one of the founders of Independent Reserve, a currency exchange specialising in the exchange of Bitcoin into other currencies, I am frequently asked to explain what Bitcoin is, and why it matters. In the beginning, I probably wasn't very good at explaining it to people as it brings together so many different concepts, all of which are often unfamiliar. Albert Einstein once said, 'if you can't explain it simply, you probably don't understand it well enough', and I think to some extent that was probably why I was having difficulty explaining Bitcoin to others in the beginning.

Still today, I meet people who have never heard of Bitcoin and they ask me what it is. Generally I answer this in the shortest way that I can, explaining the practical benefits of Bitcoin and omitting the more interesting details of how it works. If the person is interested, I'll follow up by answering each of their questions until they've understood it to a level that they are satisfied with. This was the motivation for my book, and I have approached the chapters of the book in the same way. The intended audience for this book is the person that is completely unfamiliar with Bitcoin, and completely unfamiliar with Computer Science in general. It's for the reader that wants to understand how Bitcoin works on a fundamental level, and have the technology explained to them along the way. The book begins with an overview of what Bitcoin is and its practical value, then I explore the concepts behind Bitcoin and finally answer some of the more general questions that I get asked about Bitcoin today.

- ***Adam Tepper***

money *n.* a medium of exchange

currency *n.* a system of money

PART I

WHAT IS BITCOIN

CHAPTER ONE

INTRODUCING BITCOIN

Bitcoin is a currency, and thus it is money. Money has not always been as we understand it to be today, and in fact Bitcoin is the next evolution in the concept of money. One of the key distinguishing factors that Bitcoin has compared with other well-known currencies such as the United States Dollar ($), the Great British Pound (£) or the Euro (€), is that it is an electronic currency, meaning that generally Bitcoin is stored electronically[1] on computers and transacted electronically via the Internet. To many, the prospect of electronic money may be confusing or daunting, just as email may have been confusing to somebody in the 1980s when it was described as a letter that was stored and sent electronically via the Internet. Today, email is so pervasive that written letters, particularly personal letters, are considered old-fashioned, cumbersome and above all else, slow.

For those that were an early adopter of email in the late 1980s or early 1990s, you may recall that initially it was less useful, as most of your friends, family and colleagues didn't have an email address, nor perhaps an Internet connection. Friends posed such questions as, "What is email, and how do I use it?" This was at a time before Gmail existed, before Google existed, before even Hotmail existed. Email accounts were predominately provided by your Internet Service Provider. It didn't take long before the majority of people had email addresses and today it would be quite unusual for someone not to have an email address at all, much like not having a mobile phone.

I mention email because it is a great analogy to Bitcoin. Email took the process of sending a letter, which had been around for many thousands of years, and adapted that process to store and transmit letters electronically. Within a relatively short period of time, the process of posting hand-written letters became an archaic, if novel, method of communication. It would be difficult to imagine having to go back to posting letters in the mail for day-to-day communication, and waiting several days or a week for a response. It's worth mentioning also that over the past twenty to thirty years, the way we use email itself has slowly evolved. We can access email from all of our devices; we can send large attachments and rich content; and we can use email to book meetings which appear in our calendars. All of those ideas were not conceived at the introduction of email, but were

[1] It's possible to store Bitcoin non-electronically, such as on paper, but this is the exception rather than the rule. Transactions however, are always electronic.

evolutions of email, based on how we found ourselves using it. Of course, there are many other forms of electronic communication that have now been developed since email. These developments are continual refinements to electronic communication in general. And to think that in the beginning, few people saw the advantages of using email at all.

That brings me back to Bitcoin. As email was the facility that brought written communication to the electronic age, it is Bitcoin that is taking our monetary system to the electronic age. Before we look at how Bitcoin achieves that, it's worth taking a look at the history of money to put things into perspective.

CHAPTER TWO

A HISTORY OF MONEY

Money today is a very complex system. Most of the time it works, occasionally it fails catastrophically. Although it is a complex system, much of the complexity is hidden from us in our day-to-day usage. Throughout most of our lives the monetary system has changed very little – it's something we've grown up with and most of us have probably not spent a great deal of time thinking about how it works. Money has not always been the same. One of the biggest changes of the past hundred years was the floatation of most of the major currencies onto the open market, rather than having their value fixed by the government of the day based on gold or silver. This was quite a significant advancement in the monetary system, but let's go back a lot further and see how money has changed over thousands of years by different societies.

I remember as a child, I asked my father, 'what did they do before money'? My father explained that in the 'olden days', people would use a barter system to trade sheep and other animals as currency. As a child, it was hard to imagine how that could work, but this is essentially how money worked several thousand years ago. Sheep and livestock in general had their drawbacks. They are difficult to store, difficult to transport and not easily divisible. Other commodities were also used by different cultures at various times throughout history. Sea shells and rice were used, with precious metals such as gold and silver later becoming commonplace as they had many qualities that are useful for a currency: durability, portability, divisibility and scarcity.

To make a transaction using a precious metal such as gold, the value of an item could be specified to be worth a certain weight in gold. This was not a perfect solution as the process of evaluating the purity of a metal and its weight did not lend itself towards speedy transactions. Governments later improved this process by issuing standardised coinage, whereby the weight of the metal was contained within the coin and stamped by the government to prove its weight and authenticity. This is an interesting juncture in the history of money. It is interesting because although coins contained their prescribed weight in gold or silver, it was the government's stamp on the coin that imparted its value, rather than merchants having to analyse the purity and weight of the coin themselves. Hence, the trust had now been shifted to the government. It didn't take long for governments to realise that since the value of coins resided in their stamp of authenticity, it would be cheaper to produce coins that had a lower quantity of valuable metal than the designated weight of the coin. This step in the evolution of money was the change from the coin being a unit of weight to a unit of value.

As trade began to flourish throughout Europe in the Middle Ages, the concept of a 'bill of exchange' became prevalent, whereby a merchant could offer a line of credit to a trusted

buyer. Goods were supplied to a buyer against a bill of exchange, which constituted the buyer's promise to make payment at some specified future date. Provided that the buyer was reputable or the bill was endorsed by a credible guarantor, the seller could then present the bill to a merchant banker and redeem it in money at a discounted value before it actually became due. These bills could also be used as a form of payment by the seller to make additional purchases from his own suppliers. Thus, the bills – an early form of credit – became both a medium of exchange and a medium for storage of value.

In the twelfth century, the English monarchy introduced a system based on the same premise as the bill of sales whereby the monarchy could make payments based on expected taxes not yet received. These were known as tallies. The Treasury discovered that these tallies could also be used to create money. When the crown had exhausted its current resources, it could use the tally receipts representing future tax payments due to the crown as a form of payment to its own creditors, who in turn could either collect the tax revenue directly from those assessed or use the same tally to pay their own taxes to the government. Thus, the tallies became an accepted medium of exchange for some types of transactions and an accepted medium for store of value. The Treasury soon realised that it could also issue tallies that were not backed by any specific assessment of taxes. By doing so, the Treasury created new money that was backed by public trust and confidence in the monarchy rather than by specific revenue receipts.

Around the same time, banks began issuing paper notes quite properly termed 'banknotes' which circulated in the same way that government issued currency circulates today. Only notes issued by the largest, most creditworthy banks were widely accepted. The script of smaller, lesser known institutions only circulated locally. Farther from home it was only accepted at a discounted rate, if it was accepted at all. The proliferation of types of money went hand in hand with a multiplication in the number of financial institutions.

These banknotes were a form of representative money which could be converted into gold or silver by application at the bank. Since banks issued notes far in excess of the gold and silver they kept on deposit, a sudden loss of public confidence in a bank could precipitate mass redemption of banknotes and result in bankruptcy.

The use of banknotes issued by private commercial banks as legal tender has gradually been replaced by the issuance of banknotes authorised and controlled by national governments. The Bank of England was granted sole rights to issue banknotes in England after 1694, effectively ending the use of private currency in the realm. Australia didn't enact such a law until more than two hundred years later in 1910, with the United States following in 1913.

Government authorised currencies were forms of representative money, since they were partially backed by gold or silver and were theoretically convertible into gold or silver. Under President Nixon, the US Dollar was taken off the "gold backed" standard in 1971, causing the collapse of the International "Bretton Woods" monetary system. Most of the major world currencies were then floated on the open market, removing the link between precious metals

altogether, with the value of a currency solely based upon the economy and trustworthiness of the issuing government.

By understanding the history of money, we can also see its weaknesses. It's now time to look in greater detail how Bitcoin works, and some of the advantages it brings over existing forms of money.

CHAPTER THREE

A WORKING EXAMPLE

The technology behind Bitcoin is fascinating. I first heard about Bitcoin some years ago shortly after it began in 2009. A friend of mine, Joe, a person who enjoys touting the very latest technology trends, told me that 'some guy has worked out a way to create Internet money'. I had no idea what that sentence even meant, and I believe that neither did my friend at that time.

I didn't think about Bitcoin again until sometime later in November 2012, when I noticed an online advertisement for something to do with Bitcoin and thought I'd take a look. The first thing I noted was that Bitcoin, whatever it was, was trading at over USD 10, and had been for quite some time. I had expected it to be worth no more than a few cents, or even a fraction of a cent. Of course, knowing nothing at all about Bitcoin at that time, I couldn't have had any logical idea of what a Bitcoin should be worth, but assuming there were millions of them in circulation, USD 10 seemed like substantial value and I was curious to find out more. After reading pages of material on the Internet that I had found, I was still no closer to understanding what Bitcoin was or how it worked than when I began. Only after carefully re-reading and cross-referencing various sources did I begin to get a picture in my head. I certainly wouldn't have called it a deep or thorough understanding, I still had quite a lot of questions of my own.

It did capture my interest however, and being a software engineer I decided to write my own primitive piece of software that allowed me to send and receive Bitcoin (this was never publically released, just an experiment to see how it worked and to satisfy my own curiosity). I never finished writing the software, but I spent two or three weeks developing it and in doing so I eventually did come to understand how Bitcoin worked, and was deeply impressed and amazed with the underlying technology. It was amazing because it so elegantly brought together multiple disparate software principles into a system that nobody had ever thought of before that could now effectively be used as money.

Not wanting to humiliate myself by promoting this new concept which I still had reservations may turn out to be a perpetual energy machine, I waited until I had a thorough understanding of Bitcoin before passing what I had learned onto my business partner Adrian Przelozny. It was met with the same level of scepticism I had expected. A month later he mentioned it back to me, 'Bitcoin is really amazing – I bought some'.

So, what is it about Bitcoin that we both thought was amazing, and later lead us on the path of creating a company so heavily involved with Bitcoin? In Part II, we look at the technology behind Bitcoin, but to begin with I need to explain how it works at a high level. Bitcoin is something like a cross between physical cash and a cheque book. We can only take this analogy so far, but let's start with that.

Using that example, let's say I want to send my friend Joe USD 50. I could write a cheque with his name on it, the amount, and put my signature at the bottom of the cheque. In an ideal world, this is a great system. Joe receives the cheque and he is unable to adjust the amount. If the cheque were to be stolen, it's no good to a thief because it has Joe's name on it. And if my cheque book is stolen, it's of no value to anybody because it doesn't yet contain my signature. It's a great system in theory, however in practice there are a number of drawbacks. First of all the cheque itself is not actual money. A cheque is essentially a letter to the bank authorising the bank to release USD 50 of my money that it's holding on my behalf to Joe. Until Joe takes the cheque to the bank he does not know for certain whether I have the USD 50 available. The bank may then take several days or a week before the said funds are released to Joe. Signatures are also very easy to forge, so if someone were to get hold of my cheque book, it wouldn't be particularly difficult to write out a fraudulent cheque. In Australia, chequebooks have not been in common use for nearly a generation, their very concept is as archaic to us as trading gold bullion bars, yet surprisingly the system prevails in many parts of the world including the United States.

Let's compare that transaction to a transaction that uses Bitcoin, and let's say I want to send my friend Joe XBT[2] 50 Bitcoin. The first key difference between the chequebook example and Bitcoin is that in the chequebook example, the USD 50 was being held by the bank on my behalf. Bitcoin however, is like cash in that you may store XBT 50 Bitcoin physically on your computer[3]. So let's say I have XBT 50 Bitcoin in my digital wallet on my mobile phone that I want to send to Joe, to his mobile phone. I first ask Joe for his Bitcoin address. Once I send money to Joe's address, it can only be spent using a secret key that is located on Joe's phone. Nobody else can spend it without access to his phone.

So using the software on my phone, I initiate a transaction that sends XBT 50 from my personal Bitcoin address to Joe's Bitcoin address. I then digitally sign this transaction using the secret key on my phone and send that information across the Internet for all the world to see. That's right, I don't send anything directly to Joe, I send it out to the entire Bitcoin network.

What happens next is that when other computers on the Bitcoin network start receiving the details of my transaction, they verify that I have XBT 50 in my wallet and that my signature is valid. If everything is in order they mark the transaction as authentic and it soon becomes part of and stored within the official Bitcoin global ledger known as the 'Blockchain' (more on that later).

---

[2] XBT has been adopted as the standard currency symbol for Bitcoin. With other currency codes, usually the first letter represents the country that issued the currency. Some places still use the alternative code BTC.

[3] When I say computer, I am actually referring to any electronic device with suitable software installed. That may be a mobile phone, or laptop or other similar device.

Meanwhile, the software on Joe's mobile phone is also confirming with the rest of the world the details of that transaction I initiated. Almost instantly it is shown as an XBT 50 credit to the bitcoin address on his mobile phone.

Once I have sent the money to Joe, I can no longer spend those 50 Bitcoin again, as the Bitcoin network now recognises those 50 Bitcoin are no longer available to me, and now can only be spent using Joe's secret key. To look at that another way, the transaction I initiated was essentially a 'letter' to the Bitcoin network handing over my right to spend the 50 Bitcoin to Joe. Simple!

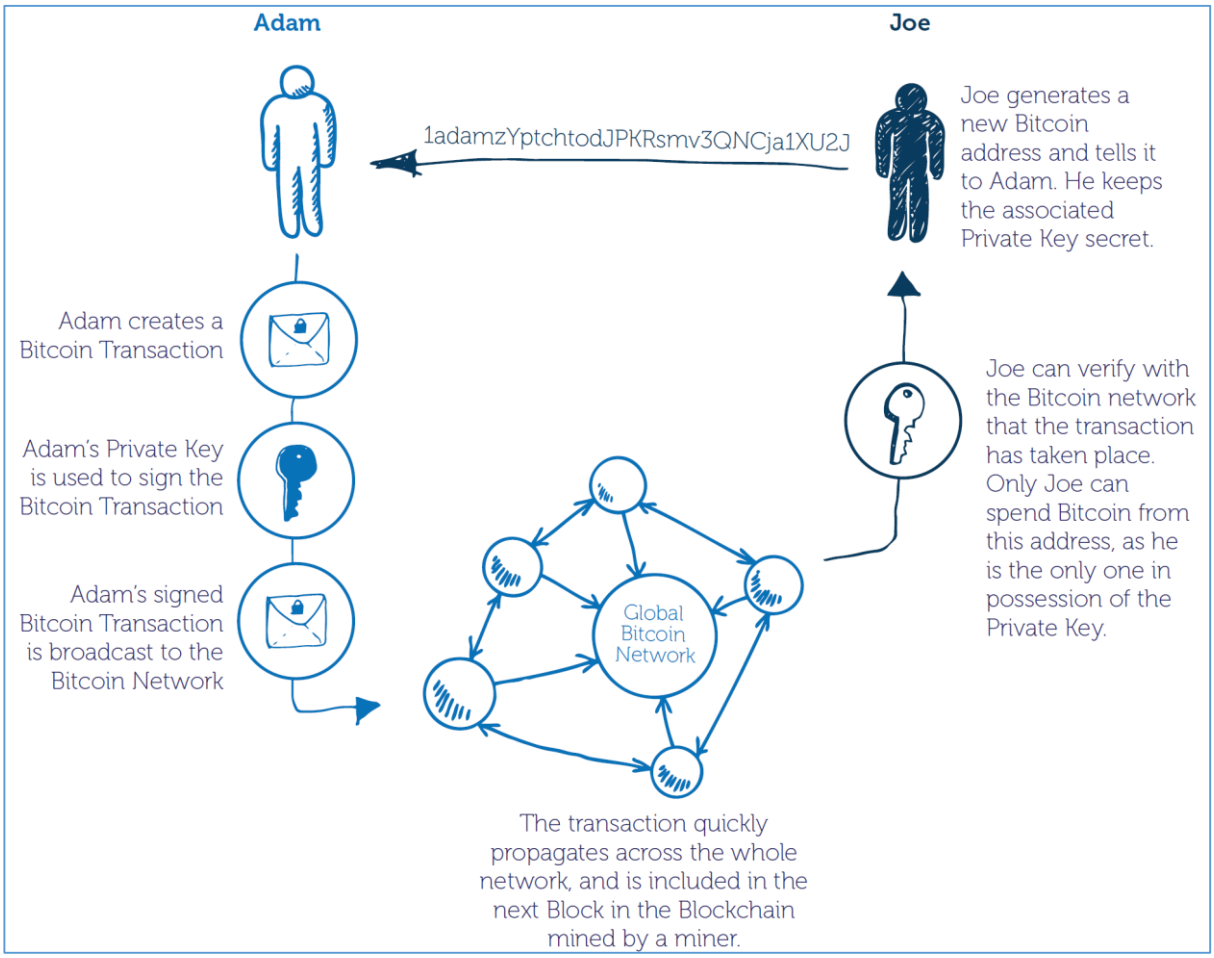

Figure 1 - Adam sends Bitcoin to Joe via the Bitcoin network.

Let's look at that more closely, and analyse some of the differences between Bitcoin and the chequebook model. In the chequebook model, there is a central bank that processes the transaction. In the Bitcoin model, there is no central transaction processor or authority – it uses a decentralised model where everyone in the network may verify the authenticity of the transaction, including the recipient. This is a fast process. For low risk, small value transactions this process takes no more than a few seconds. For high risk, large value transactions the transaction can be safely accepted as final in around half an hour. Compare

that to a bank cheque or international SWIFT wire transfer which typically take anywhere between 1-5 days.

Another similarity you might notice is that a Bitcoin transaction is signed just as an old-fashioned cheque is signed. The difference however is that forging a written signature can be done by a six year old child, whereas the forging of a digital signature used within a Bitcoin transaction is almost impossible[4].

Another interesting point is that both the cost of the transaction and the execution time is consistent, irrespective of the value of the transaction[5]. Using the example above, I could have sent Joe a fraction of a cent worth of Bitcoin to pay for some royalties he may be collecting from his platinum selling record, or I could have sent him two billion dollars to buy his successful company outright. In either case, the transaction fee would be the same, most likely free, and the execution time almost instantaneous. Effectively moving money freely and securely internationally, at the speed of an email.

Finally, it is worth noting that because the Bitcoin network spans the internet, it makes no difference where Joe and I are physically located. We could be sitting in the same room, or on different sides of the world – it does not matter. The speed and cost of the transaction would not be affected in either case.

---

[4] Technically no form of software encryption or digital signature has proven to be 'impossible' to break, but it's reasonable to say that the difficulty in forging a digital signature is approaching impossible for all practical purposes.

[5] We will see later that as a precaution against fraud, it's prudent to wait up to half an hour to confirm a high-value transaction, but as a general rule all transactions are visible within seconds.

CHAPTER FOUR

HOW BITCOIN ARE GENERATED

In the last chapter we looked at an everyday example of how Bitcoin can be used to send money between parties. One question I am commonly asked however is how Bitcoin are generated and injected into the economy, and from where Bitcoin derives its value. Before answering that question, let's think back to the history of money discussed in Chapter Two.

Until the twentieth century, money was at least partly backed by precious metals such as gold and silver. Along with a number of other important qualities which made gold and silver useful as a currency was the fact they were relatively scarce. There was a stable, yet slowly increasing supply of gold and silver as they were mined from the ground. Mining took a lot of time, effort and cost. It was also often a very dangerous and dirty environment to operate in. If gold and silver had been abundant and easy to acquire, then everyone would have done it, and they would cease to be valuable and hence not work well as a form of currency.

Although Bitcoin and gold mining are significantly different in practice, the principle behind it is the same, and hence the generation of Bitcoin has come to be known appropriately as 'Bitcoin mining'. Like gold, anyone can mine Bitcoin given the appropriate resources. If you wanted to mine gold today, you could, but remember that most of the gold near the Earth's surface has long been mined already. Therefore you would need a small fortune and a lot of geological and logistical expertise – as a result, most people are consumers of gold but not miners!

The way Bitcoin mining works is that the Bitcoin network injects a relatively small amount of Bitcoin into the economy at regular intervals. The Bitcoin protocol specifies a mathematical problem that is designed to be solved every ten minutes. When the problem is solved, the person that owns the computer that solved the problem is issued a set amount of Bitcoin. In the beginning, there may have been one person's laptop attempting to solve this problem. Therefore, the problem would have been relatively easy so that this off-the-shelf laptop could solve the problem within ten minutes, before repeating the process. At this point, with Bitcoin in its infancy and nobody else using it, one Bitcoin would have been worth absolutely nothing whatsoever. Therefore this mining exercise, which cost a small amount in electricity, elicited an amount in Bitcoin that had no value.

As time passed however, two, then three, then a thousand off-the-shelf laptops and home PCs were attempting to solve this problem which cycled every ten minutes. With a thousand computers all attempting to solve the problem, the network adjusted the difficulty level to be a thousand times more difficult than in the beginning. Therefore, each individual has approximately one in a thousand chance of solving the problem and receiving any award at all.

I don't know exactly what Bitcoin was worth at this point in its history, but it had become worth something, if only a little. Running a computer twenty-four hours a day doesn't normally cost much when browsing the Internet, but running a computer twenty-four hours a day that is dedicated to solving a mathematical problem will see the CPU running close to 100 %. This draws a large wattage from the power supply costing a significant amount in electricity. People began to calculate their cost of running these Bitcoin mining machines and what their statistical likelihood was of solving the problem over a given period of time. And henceforth, Bitcoin had some value, if only due to its scarcity rather than its initial usefulness within such a small circle of people.

People then realised that rather than using any old laptop or PC for Bitcoin mining it would be more efficient to build computers specifically for the purpose of mining Bitcoin and nothing else. People began to run not one, not two, but entire farms of computers in their apartments and living rooms that were all mining Bitcoin and consuming electricity. Some smart person later worked out that the GPU (graphics processing unit) on consumer graphics cards was far more efficient at solving the specific type of problem presented in Bitcoin mining and software was written to take advantage of these graphics cards and mine Bitcoin faster.

As you can see, not only had the number of people mining Bitcoin increased, but so were the number of machines each person was running and the power of those machines. The problem being solved every ten minutes was now hundreds of thousands or perhaps millions of times more difficult, and the miner using a humble laptop would have very little chance of mining anything at all.

After the phase of GPU mining, as it was known, hardware manufacturers started designing ever-faster chips solely dedicated to Bitcoin mining, rendering GPU mining slow and obsolete. Bitcoin mining today is an industry all of its own, with companies invested in millions of dollars' worth of mining hardware. So just like using a small shovel to dig for gold today, you can't expect to start mining Bitcoin on your home computer and expect to make money, it requires extensive resources. Several Bitcoin mining operations have been established in Iceland, where their geothermal electricity supplies a cheap source of power, combined with minimal server cooling requirements due to the low temperatures there.

That said, if you can't afford a gold mine, you could probably afford to buy some shares in a gold mine. By the same token, there are now many companies providing what's known as a 'Bitcoin mining pool'. The way it works is that if you join the pool of thousands of users that are all using their home computer to mine Bitcoin, you are guaranteed a small percentage of Bitcoin relative to the amount of mining your individual computer has contributed – don't expect to get rich however!

I've talked a lot about how Bitcoin mining works, and the history of Bitcoin mining, but the process of Bitcoin mining plays two other important roles in the Bitcoin network aside from generating new Bitcoin for miners. First of all, in addition to solving the mathematical problem, Bitcoin miners also process transactions. In Chapter Three I gave the example of sending XBT 50 to my friend Joe, and that transaction was sent out across the Bitcoin

network. The details of that transaction will reach the multitude of Bitcoin miners actively mining, and when one miner successfully solves the mathematical problem, he will also process that transaction, along with all of the other Bitcoin transactions of the past ten minutes and include them in the Blockchain (the Bitcoin ledger). In other words, these miners serve a necessary function in the Bitcoin network, aside from injecting money into the economy, they provide the payment processing functions that allow Bitcoin transactions to work.

There is a third key role this mining process plays. The more miners on the Bitcoin network, the more difficult the mathematical problem becomes. The more difficult the mathematical problem is to solve, the more secure the network becomes and resilient to fraudulent transactions. We'll leave that point there for now, and come back to it again later in the book.

CHAPTER FIVE

WHY USE BITCOIN

Now that you have a rudimentary understanding of some of the principles behind Bitcoin, it's time to look at some of the advantages of Bitcoin over other types of money, and why you might choose to use it. Bitcoin is advantageous over regular currency under almost all circumstances where an electronic transaction is possible. Before looking at those advantages however, it's worth noting what the alternatives are. When we talk about alternatives, we're not only comparing Bitcoin to other currencies such as the US dollar, Pound or Euro, but we also need to look at different types of transactions. The way we use money depends greatly on the amounts involved, the type of goods or services we are buying, and the relative location of the parties.

In the simplest case, we have a physical cash transfer where notes or coins change hands. Cash transfers work best for amounts between around USD 0.05 up to around USD 1,000. It's obviously possible to transfer larger amounts, but in most cases people find it more convenient to use other payment methods once the amount is greater than USD 1,000. For smaller amounts, we are limited to the smallest denomination of that currency. Cash transfers are limited because they require both parties to be in the same location.

For larger amounts between individuals, a bank cheque is often used. Bank cheques generally cost around USD 5 and therefore are not very economical for values below USD 500. For most practical purposes there is no upper limit with a bank cheque, but it is a rather cumbersome process that requires both parties to go to a branch of the bank, generally limiting the use of bank cheques for transactions within the same country. Parties must also meet either face-to-face to hand over a cheque, or wait several days in the mail.

For merchants, EFT or credit card facilities are convenient. This is a relatively expensive option for merchants as they must pay to establish merchant facilities with their bank, as well as pay their bank several percent on the transaction value in commission for processing the transaction. Furthermore, the merchant risks what's known as a 'chargeback', where the transaction was made fraudulently and the merchant is responsible for refunding the money. This is of particular concern for merchants operating online businesses where they only receive the credit card details, rather than sighting the card itself. EFT and credit card facilities are generally limited to amounts between USD 10 and USD 10,000.

International SWIFT transfers are the principle method of transacting money between countries. SWIFT transfers are generally uneconomical for values below USD 1,000 due to the high fees charged by banks. SWIFT transfers are a very slow form of transaction, generally taking several days for the recipient to receive their payment. They are also prone to mistakes, and hence further delays, during the transfer process.

I've described some of the more common methods of transferring money between people, but that is by no means a comprehensive list. There are also large remittance firms such as Western Union, as well as a great number of niche international remittance providers which can send small amounts of money faster and more economically than SWIFT or Western Union. Another group of companies includes the likes of PayPal, which act as a payment processor and insurance provider between merchants and banks. And again, that's not everything. You might start to realise now that our notion of a transaction really depends on what we are trying to do, and that we have a wide variety of loosely-coupled systems that have their own pros and cons depending on the circumstances.

Back to Bitcoin. Bitcoin allows me to send any amount of money, *anywhere* in the world, *instantaneously* and for *free*. What other transaction method has such scope?

Let's continue. Bitcoin allows merchants to accept payments without the risk of a chargeback. To put that another way, once a merchant has received a Bitcoin payment, there is no risk that a bank or third-party may later claim the payment as fraudulent; Bitcoin payments are final. Of course merchants and consumers may still opt to pay for a third-party escrow agent if they prefer. This is a great boon for customers as well, particularly those making online purchases. If you've ever bought something online with a credit card, you'd know only too well the frustration at having your card rejected because you're travelling at the time or perhaps making what the merchant considers to be a high risk purchase. For example, if you're purchasing a few thousand dollars' worth of equipment the merchant may ask you to prove your identity and address. This is inconvenient and frustrating for both the merchant and the customer, resulting in unwanted delays and effort on both parties to process the transaction. With Bitcoin, the transaction is instantaneous, free and presents *no risk* to the merchant.

The benefits are greater still if you're a merchant that deals frequently with international customers, such as anyone in the tourism industry. Imagine the case of a boat charter operator. Their customer charters a boat for a week in advance of their holiday. Rather than bother themselves with a wire transfer fee, unfamiliarity with a foreign currency and several days for the money to clear, a deposit in Bitcoin may be transferred from anywhere in the world freely and instantaneously, in a currency both the customer and merchant are familiar with. If the charter happened to be a surprise engagement present for the fiancée, it wouldn't appear on any credit card statements either.

Another great advantage of Bitcoin is that a Bitcoin transaction does not require either party to provide any sensitive information to the other party. This is completely contrary to the way credit card or EFT facilities work. Every time you make an in-store purchase with your credit card or EFT card you must hand over the details of the card, along with your PIN or signature. It's interesting to think how sensitive we are about hiding our PIN from other people, yet we are happy to enter it into a machine owned by a complete stranger. PIN skimming devices are not uncommon in Australia, but they are far more pervasive in other parts of the world, and of particular concern to international travellers. Using Bitcoin

removes this risk entirely. You may make a purchase anywhere in the world, paying money to a complete stranger without any concern that your details may later be used fraudulently.

Another example where Bitcoin has a significant advantage over other transaction methods is for paying small amounts. A child might want to go into a store and buy ten cents worth of chocolate or lollies, or a vendor may want to sell a mobile phone ringtone for fifty cents online. Without Bitcoin, such small purchases can only be made with cash, as most other facilities require a minimum purchase amount to be viable due to transaction fees. Bitcoin facilitates what's now referred to as 'micro-payments' for small amounts such as this, or even smaller amounts less than even a single cent. Furthermore, Bitcoin is not a line of credit, it is the digital equivalent of cash, and therefore you don't need to be an adult to use it.

What about the case of a traveller who needs to urgently send a hundred dollars back to his home country for his mother? A SWIFT transfer would be both costly and take several days. A service like Western Union may be quicker, but would be more expensive still. Bitcoin is instantaneous and free.

Bitcoin may be sent between parties anonymously. There are limitations to this anonymity, which we will take a closer look at in a later chapter, but suffice to say that when I make a transaction in Bitcoin I don't need to be concerned with the payment processor, bank or credit card company all keeping a record of my entire history of purchases. Nor do I need to reveal my identity to the merchant, and there are many valid and legitimate reasons as to why I might prefer to remain anonymous.

One of the other great advantages of Bitcoin is that there is a controlled supply. As we discussed briefly in the previous chapter, Bitcoin are generated through the process of mining, and the rate of Bitcoin generation is controlled by the Bitcoin protocol itself. We look at this in more detail later, but we can say that the Bitcoin supply is predictable and controlled and it cannot be manipulated by any individual, organisation or government. We've seen many times throughout history, including recent history, examples of governments negatively affecting the supply of money by generating more of it to suit their own economic interests at the time. These interests are often in stark contrast to the interests of the people that are holding the currency. We've seen how this can lead to an inflationary spiral that can destroy an entire economy. Bitcoin is not subject to this kind of manipulation, as the supply is controlled by the protocol itself and known in advance by all those who use Bitcoin.

We said earlier that Bitcoin has similarities with cash, however cash has limited options when it comes to protection from accidental loss and theft. Bitcoin is not immune to these sorts of loss, however it does have many inherent properties that allow people to protect their money from being lost or stolen. This makes it a far safer option to carry in one's back pocket than a wallet full of cash.

Traditional currency was never designed for the electronic age. It is a system of money that has been in use for hundreds, if not thousands of years, that long predated the invention of electricity, least of all the advancement of computers and the Internet. It has been in use since a time when trade was done face-to-face, with no concept that a song could be sent from one side of the world to another for a small fee between two parties that have never

even spoken. Throughout the twentieth century, financial institutions adapted their ancient systems to the electronic age, and developed new systems that met the demands of the day. As these systems aged, and the demands for electronic commerce expanded, new systems were built atop the old systems, performing tasks that they were never originally designed for. The result is a creaking banking system that was never designed for the wide variety of electronic transactions that the world performs today, as well as a complete reliance on the financial institutions who profit greatly from this dependence.

Bitcoin was designed for electronic transactions from the beginning, and this is why it shines. It allows for instantaneous electronic transactions anywhere in the world, for any amount, without the need for trust between the two parties or any dependency on a third-party. Once digital currencies reach critical mass, it will seem silly that we're even asking such questions today.

PART II

HOW BITCOIN WORKS

CHAPTER SIX

ASYMMETRIC KEYS

At the heart of it, Bitcoin is an open protocol. By protocol, I mean that Bitcoin is a set of rules which all Bitcoin software must comply to. By open, I mean that the protocol, or rule set, is publically available for anybody to review. This protocol allows all Bitcoin software (what we typically refer to as 'Bitcoin clients') to communicate with each other over the Internet in a standardised way.

The first question then is, if Bitcoin is an open protocol, or set of rules, what prevents others writing software that breaks the rules. The answer is nothing. Anyone can write software that uses the Bitcoin protocol and communicates with other Bitcoin software over the Internet that attempts to 'break the rules' in their favour, however clients that don't conform to the Bitcoin protocol are ignored by other clients.

To provide an analogy, imagine players in a postal chess tournament, where players are in different locations and their moves are submitted by correspondence. Both players know what the entire board looks like, and the other player is free to move as he chooses provided it is within the rules of Chess. If it isn't, the move is simply ignored or rejected by the other player. This is the same principle behind Bitcoin: any of the 'players' (Bitcoin clients), know exactly what the 'board' (Blockchain) looks like, and can independently verify from other sources that any other 'move' (transaction) is valid.

If we want to understand Bitcoin at a deeper level than an analogy, then we must understand the concept of asymmetric cryptography (also known as public key cryptography). Asymmetric cryptography is a key part of Bitcoin and without it, Bitcoin could not exist. Asymmetric cryptography is not a new concept, and is actually an integral part of the security of many software systems. We use asymmetric cryptography each time we visit a secure (SSL) website, such as an internet banking site.

Before I explain what asymmetric cryptography is, let's imagine a problem. Let's say Alice, in Australia, wants to send a letter to Bob in England. The contents of the letter are top secret. How does Alice send a letter to Bob, without risking that somebody else along the way may read the contents of the letter? Without asymmetric cryptography, the only way to do this is for Alice and Bob to have a prior understanding of how to encode the letter. The letter could then be encrypted and Bob would know how to decrypt it when he receives it. But what if Alice and Bob did not have a pre-arranged encryption key; what if Bob had never met Alice before? In this circumstance, without asymmetric cryptography it's not possible for Alice to send Bob a letter securely.

So that brings us to asymmetric cryptography and how it solves this problem. Some time ago, some clever mathematicians worked out a way that a pair of keys could be generated that were mathematically connected to one another. In this context, a key can be thought of

as a very large number – a number with several hundred digits[6]. These are known as a public key and a private key or collectively known as asymmetric keys. It turns out that these keys have some very useful properties!

Using the public key, it is possible to encrypt a message in such a way that it may only be decrypted using the private key. Therefore, Bob may now generate a pair of keys, and he may tell the world what his public key is, as it is not possible[7] to derive his private secret key from this. If Alice wants to send Bob a secure message, all she has to do is encrypt the contents of her letter with Bob's public key using a common algorithm, and Bob will be able to decrypt the message with his private key, which he does not reveal to anybody else.

You use asymmetric cryptography technology every day when you use Wi-Fi, Bluetooth or secure websites where the data is encrypted to prevent what's known as a 'man-in-the-middle' attack. To put that another way, asymmetric cryptography is used to prevent the contents of your conversation, email or transaction from being intercepted by somebody else.

So now we know how Alice can send a letter to Bob securely, but when Bob receives the letter how can he be sure that the letter was sent from Alice, and not somebody else? It turns out that these asymmetric keys are able to address this problem also. Alice also generates a pair of keys: a public and private key. Like Bob, Alice reveals her public key to the world. Alice is then able to 'digitally sign' the contents of her letter using her private key. Then using Alice's public key, Bob can determine that the letter was indeed signed by Alice, as nobody else could have signed the letter without access to Alice's private key. Therefore, Alice's letter can only be read by Bob and Bob can ascertain that the letter was written by nobody besides Alice.

This is a very useful and powerful concept – one that still impresses me today, despite its ubiquitous use. You can appreciate the usefulness in military communications, and in fact for many years the United States attempted to ban the export of software that used strong asymmetric cryptography.

---

[6] It's worth pausing to consider just how astronomically large a number is with several hundred digits in it. That is many more orders of magnitude larger than the number of atoms in the observable universe.

[7] As we made note of in Chapter Three, there is nothing truly 'impossible' in cryptography, however in practice some things are considered difficult enough that for all intents and purposes we may consider them impossible.

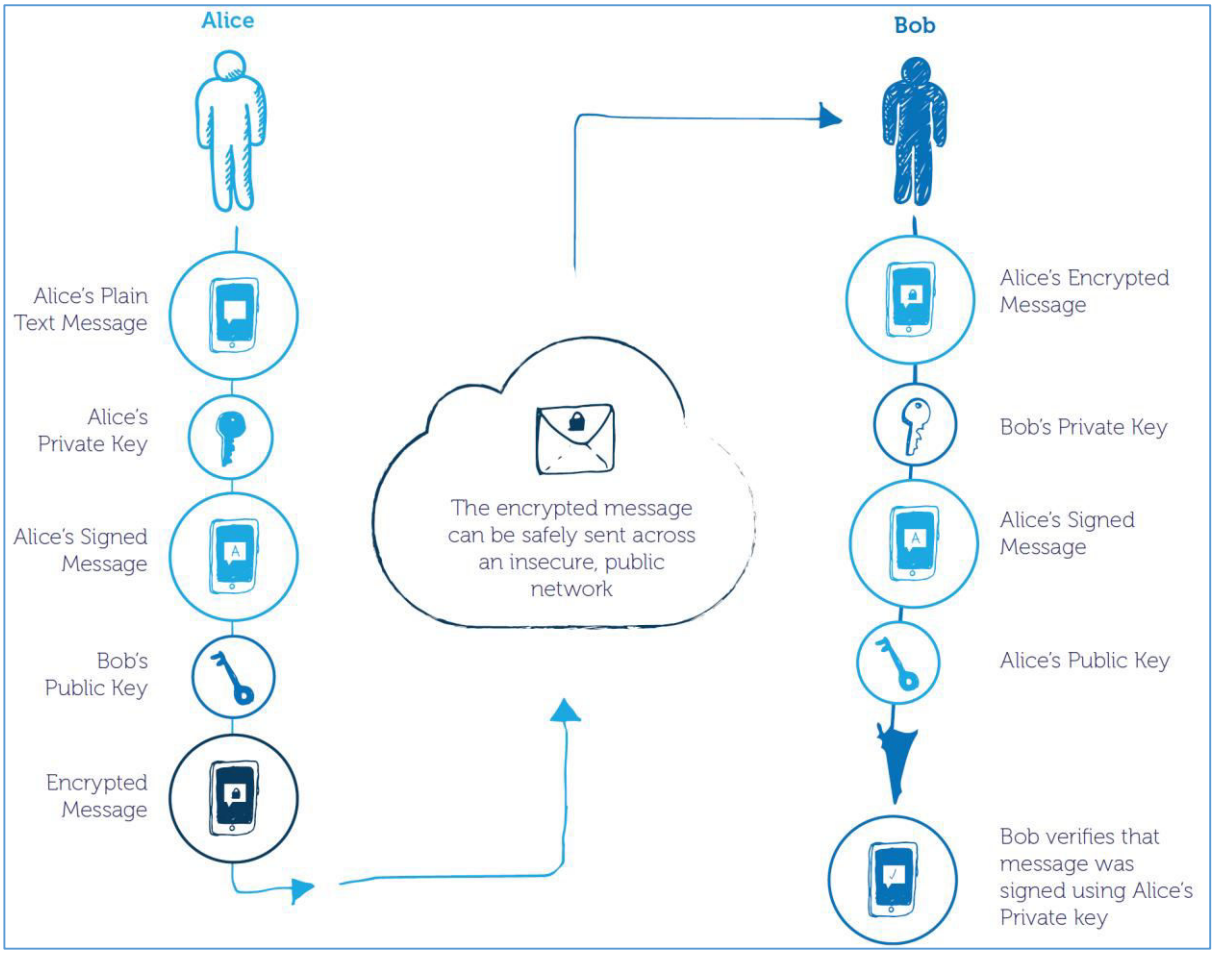

Figure 2 - Asymmetric cryptography in action. Alice sends a signed and encrypted message to Bob.

Now that we understand asymmetric cryptography, how does this relate to Bitcoin? Remember in Chapter Three, we made the analogy that in some respects, Bitcoin worked similarly to a chequebook? We said that one user sent Bitcoin to another user's Bitcoin address, and that the transaction was then signed by the initiator of the transaction. Well, this is the point where it should start to come together: that Bitcoin address is a derivative of a public key.

Let's use our original chequebook example in more detail, now that we understand the concept of public keys. I have XBT 50 on my mobile phone, and I would like to send that to my friend Joe's mobile phone. Joe first presses a button on his phone to generate a new Bitcoin address. What he's really doing is creating a pair of asymmetric keys. The private key is stored on Joe's phone and a derivative of his public key (the Bitcoin address) is then displayed on his screen and given to me. Using Joe's Bitcoin address, I initiate a transaction on my phone specifying the amount of money I want to send him. I then digitally sign that transaction with my private key and send that transaction out across the Internet. Remember we said that writing a cheque is the equivalent of writing a letter to the bank authorising the bank to release funds from our account to the specified person. In Bitcoin, a transaction is essentially a public declaration ceding control of the XBT 50 registered to my Bitcoin address,

to the Bitcoin address that I specify. Only by having my private key do I have the authorisation to sign the Bitcoin over to Joe's address, and I give this authorisation by digitally signing the transaction.

Once the transaction is sent, Joe can confirm with the Bitcoin network that he now has authorisation to spend the Bitcoin – the transaction is final. Of course, despite all of these technical steps, this is all done automatically behind-the-scenes, with the press of a few buttons on the phone.

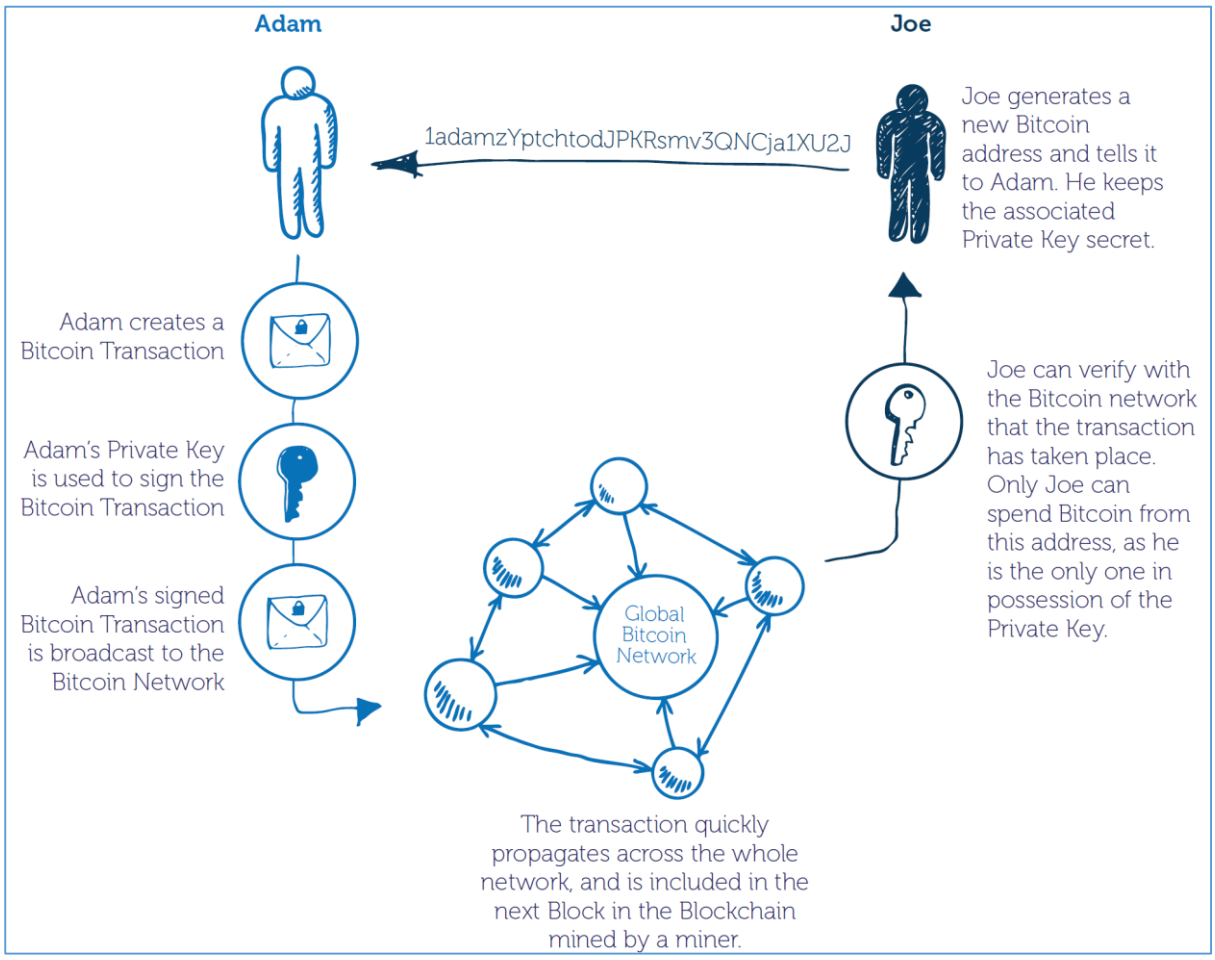

Figure 3 - Adam sends Bitcoin to Joe via the Bitcoin network.

CHAPTER SEVEN

HASHING

In Chapter Four we looked at how Bitcoin were generated and injected into the economy. We explained that Bitcoin are generated approximately every ten minutes through the process of solving a mathematical problem. In this chapter, we will look in more detail how that works. To understand Bitcoin mining, we need to familiarise ourselves with another Computer Science concept: hashing, or the cryptographic hash.

Hashing is a very interesting concept that like asymmetric cryptography is one of the key ideas in the field of software security. Like we've done before, let's start by presenting a problem. If I have a computer system, how can I securely store every user's password in such a way that if the system was compromised, the user's passwords would not be? In other words, it's a bad idea to keep a database that contains thousands or millions of user's passwords for reasons that should be apparent.

The answer involves the cryptographic hash. The process of hashing takes some input, such as a password, and runs that input through an algorithm which outputs a large number, appropriately named the 'hash' (or 'hash value'). There are two distinguishing features that define a hash. One, for a given input, the hashing process always results in the same output. For example, if you enter in a password that is run through a hashing algorithm that generates a specific number, the same number will be generated each time. The second distinguishing feature of a hash is that it is a one-way process. It is impossible to take the hash value and reverse engineer it to discover the input. These two features are what define a cryptographic hash. If the process was reversible, it would no longer be referred to as a hash, but plain old encryption/decryption, and that's another topic altogether.

It turns out that the process of hashing a value has a lot of useful features in Computer Science. One of those problems, as we posed above, was how could we securely store users passwords in a system. Rather than store a user's password, we first hash their password[8] and store the hash value. When the user attempts to log on next time with a password, we don't need to know what the password entered was, we only need to know that it was the same as they entered the previous time. In other words, if the hash of the password entered matches the hash stored in the database, we know the user must have entered the correct password –

[8] The process of hashing a user's password is slightly more complicated, and involves adding what's known as a random 'salt' value to the password. This ensures that two people that have the same password will have different hash values, which leads to a more secure system.

although we don't know or care what that password actually was. If our system were later compromised, an attacker would only have a list of password hashes, which are non-reversible and of no value.

If you're like me, you may find this process quite fascinating, but you may be asking yourself – if passwords are hashed, how is it that when you forget your password for a particular system the company can email you your password. It's a very good question. This means that the passwords are not being hashed, and the system in question is highly insecure. Sadly, many systems today overlook this. It is one of the reasons why it's important to use a different password for each system that you access. When it is revealed in the news that a system was 'hacked' and thousands of passwords were compromised, it was because the designers of the system failed to secure their users' passwords using the hashing technique which is universally considered best practice.

For interest's sake, if you do forget your password on a system that *does* properly hash their users' passwords, the correct approach is for the system to reset your password to something temporary, and allow you to change it to something else when you log on. It should be noted however, this approach does not guarantee that the system actually hashes users' passwords.

Now, how does this all relate to Bitcoin mining? Well, we said that reverse engineering a hash is impossible. Technically speaking, it is theoretically possible via what's appropriately known as a 'brute-force' attack – trying every input combination possible until the same hash value is generated. In practice however, the number of combinations are astronomically large which, for all practical purposes, makes it impossible. It should also be noted that multiple input values may result in the same hash value, known as a collision, but these are extremely rare if an appropriate hashing algorithm is used and not important for the point of our discussion here.

Now let's suppose that there were only a million hash values possible, a number between zero and a million. In reality of course we know that there are far more than a million hash values possible, but let's go with a million to illustrate my point. The chances therefore, of correctly guessing the correct input for a given hash value would be a million-to-one. With enough guesses, and enough time, I would eventually find an input that gave the same result as the hash value that I am trying to match.

Let's suppose that process of trial and error took twenty-four hours to find a match (a modern home computer would loop through a million iterations in less than a second, but let's stick with twenty-four hours for our example). Keeping in mind that in our example we said that all hash values were numbers between zero and a million, what if we then said instead of finding an input that resulted in a single hash value, we wanted to find an input that hashed to a value of less than or equal to 10. That is to say, we'd like to find any input that resulted in a hash value of 1, 2, 3, 4, 5, 6, 7, 8, 9 or 10. It's now ten times more likely that a given hash value would result in a match, thus it would be on average ten times quicker for our computer to discover a match – now taking approximately 2.4 hours rather than 24 hours.

If I wanted to create a problem that was faster to solve, let's say solve within 10 minutes, I could relax my threshold to any hash value between 1 and 150. The problem is now 150 times simpler than our first example, and a quick calculation would show that the problem should be solvable by our (slow) computer in approximately 10 minutes. What would happen if a second, similarly powerful computer came along attempting to solve the same problem? It would now be twice as quick to solve. If I wanted the problem to still take 10 minutes, I would have to make the problem twice as difficult by specifying that the hash value must be less than 75 instead of 150. As more and more computers attempt to solve that problem, and as computers become more and more efficient at solving the problem, we make the problem more difficult by specifying a smaller range of hash values that we will accept.

And, in case you haven't already guessed it, this is the problem the Bitcoin network presents to Bitcoin miners. The difference of course is that there are far more than a million combinations, numbers so big that we don't even have words for them in English. All the Bitcoin miners across the world are, at the time of writing, collectively attempting approximately 350,000,000,000,000,000 inputs per second in an effort to find an input value that hashes to the target range of hash values specified.

The Bitcoin network regularly assesses the difficulty of the problem, and if the problem was being solved faster or slower than the prescribed 10 minute interval, then the problem is adjusted accordingly by either expanding or reducing the range of possible hash values that are accepted. Of all the computers around the world attempting to solve the problem, only the first to solve the problem receives the Bitcoin 'reward', and then the process begins again. The next questions then are: how does the rest of the Bitcoin network confirm that the problem has been solved, and how are the Bitcoins actually generated through this process? The first question is simple. The computer that solves the problem announces the solution to the Bitcoin network, and the other computers on the network verify the solution. Although reverse-engineering the input for a given range of hash values is a slow, trial-and-error process, once the solution is found it is easy to verify by running the proposed solution through the hashing algorithm and ensuring the resultant hash value is within the target range. Newly mined Bitcoin are then credited to the miner's specified address, injecting new Bitcoin into the economy. Just as monarchs of old issued tallies for taxes that were never to be collected, and banks issued banknotes for funds they did not have, the Bitcoin network slowly generates new Bitcoin. One key difference between Bitcoin and other systems however is that in all previous systems the rate of currency generation had been at the whim of a monarch, government, bank, or in recent terms a government controlled central bank. The generation rate of Bitcoin is algorithmic, and is not subject to manipulation by individual market participants – it is predictable. The Bitcoin protocol defines that rate of generation, and over time the rate of generation is reduced until ultimately no more Bitcoin are generated at all. It is possible to calculate for any date in the past or future the approximate number of Bitcoin in circulation.

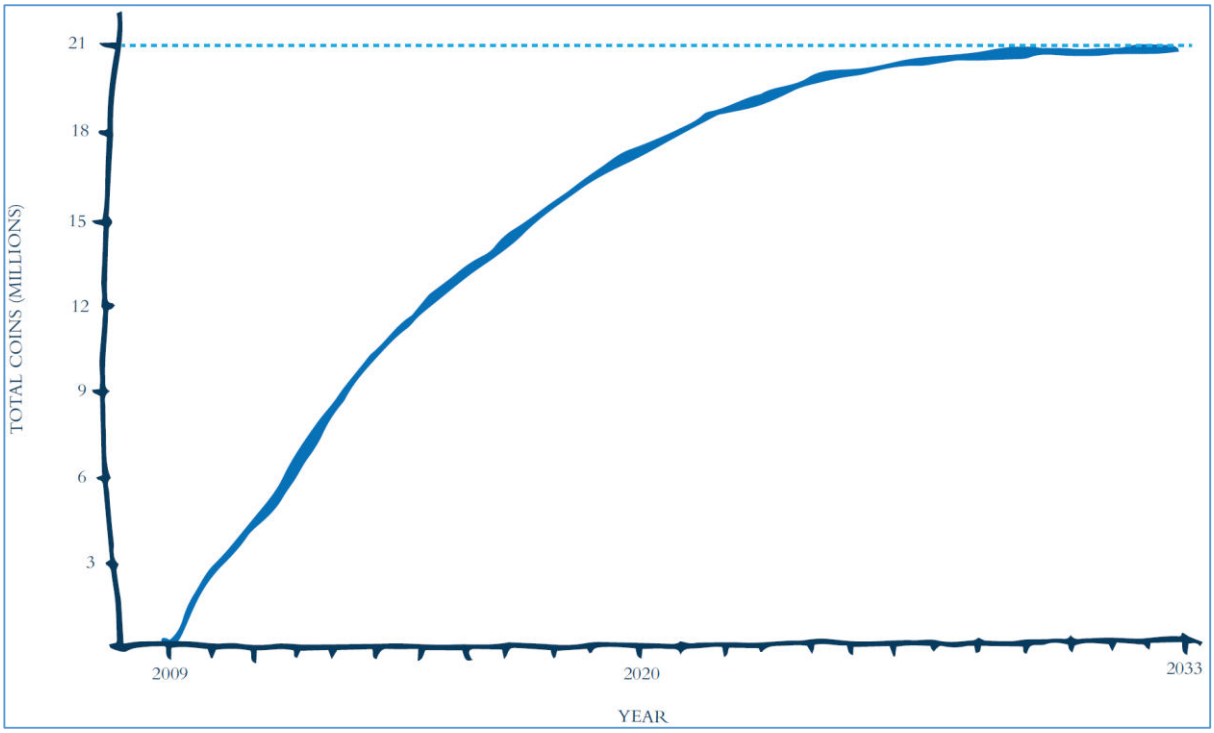

Figure 4 - Total Bitcoins over time

CHAPTER EIGHT

DECENTRALISATION

Let's pause on that line of thought for a minute, and now look at decentralisation. Decentralisation is a fairly recent concept in Computer Science that we have seen increasingly more uses for over the past decade. One of the first examples of decentralisation was peer-to-peer (P2P) file sharing. Various implementations of this have existed over the years, with the most prevalent now being the BitTorrent network. If you're unfamiliar with BitTorrent, let me give you a brief introduction. The traditional method of downloading a file from the Internet is fairly straightforward. One computer (referred to as the server) has a file that you want, and another computer (referred to as the client) requests that file from the server, and the server sends the file to the client. This model is still prevalent today and most of the time when you are browsing the Internet it works as described. It's known incidentally as the client-server model. This model has some limitations however. One of those limitations is that the file can't be downloaded any faster than the server will allow. Normally this isn't a problem, but what if the server has a million people that want to download the same file? The server has a limited amount of bandwidth and therefore that limited bandwidth has to be divided between all the people downloading the file. Incidentally an individual server cannot support a million simultaneous connections, and so there would need to be a farm of servers hosting the file which results in a large expense for the person that owns the servers, or a slow speed for the clients downloading the file.

This is where a distributed P2P network can make a difference. It works like this: let's say I have a file I want to make available to others. Using P2P software, that file is divided into hundreds of parts (the exact size and number of the parts depends on a number of different factors). People can now download that file from my computer, one part at a time, in any order. I don't have a lot of bandwidth, so initially this will be quite slow for the first couple of people that attempt to download the file from me. As soon as one other person has one part from me, other people can now download that part from either myself or the other person. Over time, more and more people download parts from my computer and parts from other people's computers until the original file becomes distributed across many people's computers. If somebody new comes along now and attempts to download this file, the software will simultaneously pull the file from many different computers all at once, possibly never even connecting with my computer which had the file originally – in fact, at this point, I could turn off my computer altogether and providing that the full copy of the file is out on the Internet, people could continue downloading it without interruption. This has proven to be a very successful system for files that are in high demand. In recent times, we've seen this decentralised approach used for other software applications that were not previously conceived, the most recent of which is the Blockchain.

CHAPTER NINE

THE BLOCKCHAIN

We've now looked at and discussed the three core Computer Science concepts behind Bitcoin: asymmetric cryptography; cryptographic hashes and P2P networking. As interesting as those concepts are, they are not revolutionary in the context of Bitcoin. All of those concepts have been applied in many different ways for a long time. What pulls it altogether however, is the fundamentally new idea that is the basis for Bitcoin. This idea is known as the Blockchain.

The Blockchain is a decentralised public ledger: let's break that down. In a regular business, or more appropriately a bank, a ledger refers to the set of records that hold details of customer transactions and account balances. In a modern bank, these records are held in large software systems. As you can probably guess, these are very large, robust systems that need to support many millions of customers making millions of transactions daily. You may have already experienced some of the symptoms of the difficulties banks have in managing such large sets of data reliably. For example, you may not be able to download a history of your transactions from your bank's internet banking portal beyond a certain time period in the past. Or, perhaps you find that some transactions may not immediately appear in your transaction history until they are processed overnight. These and other similar quirks are all compromises made in order for banks to manage these (often ancient) systems, containing massive amounts of data.

We said that the Blockchain is a decentralised public ledger. We know then what a ledger is, a set of records that hold details of customer transactions and account balances. Now let's explain what we mean by 'decentralised' and 'public'. Unlike a bank, this ledger is not held on a central server controlled by any individual or organisation. The Blockchain ledger is publically available and stored locally by many of the Bitcoin clients freely available for download on the internet. This may seem hard to believe, but you have understood correctly: the entire history of every Bitcoin transaction made by anyone in the world since the beginning of Bitcoin (the first transaction occurred on the 12th of January 2009) is publically available for anyone to review, and not only that but most desktop or laptop computers running Bitcoin software contain a copy of this ledger. You probably have a lot of questions right now such as how this is possible, or why this is even a good idea. Let's start with how it's possible. Well, it is a large amount of data, but not impossibly large. Financial records take up a very small amount of space and to put it into perspective all the Bitcoin transaction records since the beginning, at the time of writing take up approximately the same amount of space as a dozen or so HD movies. If you ever download a Bitcoin client that keeps a copy of the Blockchain locally, it does take a long time to initiate the first time its run, as it downloads the entire copy of the Blockchain. Having said that, it's not absolutely necessary

for every computer in the world to keep an entire copy of the Blockchain locally. It's certainly not feasible on mobile devices, and we are already seeing a trend of Bitcoin clients keeping only some relevant details locally, rather than holding the entire Blockchain. It does illustrate my point however that the Blockchain is publically available to the world, and there are in fact many free websites that make it easy to browse the history of all Bitcoin transactions ever made by anyone at any time.

You may be a little concerned at this point that by using Bitcoin there is a public history of all transactions you have ever made. That's only partly true, and a point we will discuss further in the chapter on Anonymity. The public ledger only contains Bitcoin addresses and amounts. It does not contain any personal or identifiable information. In other words, if I send 50 Bitcoin from address A to my friend Joe who has address B, the entire world can see that 50 Bitcoin has been sent from address A to address B, but nobody can identify that address A belongs to me and address B belongs to Joe. So when I look at the Blockchain, all I can see is the balances of addresses, and transactions from one address to another – none of which impacts the privacy of the people involved in those transactions.

Another point to realise, which we haven't discussed yet is that unlike email, where you may only have one address or no more than a handful of addresses at most, there is no limit to the number of Bitcoin addresses that one can have. In fact, it's encouraged, and most Bitcoin clients are set up this way by default, that every transaction utilises a new address. Let's look again at the example of sending 50 Bitcoin to my friend Joe, now that we know a little more. When I ask Joe to tell me his Bitcoin address, he generally would not tell me an address that contains the sum total of his wealth, he would create a brand new address that contains no Bitcoin at all and I would send the 50 Bitcoin to that address. Bitcoin software does not require you to individually manage balances for each of your Bitcoin addresses, it can tell you the total balance of all addresses you have ever created. From my end, it's unlikely I have a Bitcoin address that contains precisely the amount of money that I want to send to Joe. For example, I may have Bitcoin address A that contains 30 Bitcoin and Bitcoin address B contains 35 Bitcoin. In this example, the software would automatically generate a transaction that took 30 Bitcoin from address A, then 20 Bitcoin from Address B, send those 50 Bitcoins to Joe and also send the remaining 15 Bitcoin back to a new address C that it has automatically generated on my behalf. Both Joe and I may have hundreds or thousands of addresses containing small sums of money that together comprise our total Bitcoin wealth. Neither of us can see the other's addresses except for the ones involved in our transaction.

The exception to that rule might be if I received a single transaction for a large sum of money, let's say a million dollars' worth of Bitcoin. If I then wanted to spend 1 Bitcoin from this address, the recipient would be able to see that I have nearly a million dollars' worth of Bitcoin at my disposal, which I may not like to reveal. Suffice to say, for those fortunate enough to be in that position there are techniques available to disguise this wealth by essentially spreading the value across many multiple addresses – modern software makes this process trivial.

Now that we know what the Blockchain is, how does it actually work? The question could perhaps be posed as: how do we keep a consistent record of transactions in a decentralised environment? The first point to understand about the Blockchain is that it's called the Blockchain because it's made up of a chain of sequential blocks. A block is a group of transactions. Can you guess how often blocks are generated? Approximately every 10 minutes. You may now start to realise there is a connection between the Blockchain and Bitcoin mining, and if you guessed that, you'd be correct.

CHAPTER TEN

BITCOIN MINING

Remember in Chapter Four we said that Bitcoin mining achieves two other purposes along with injecting new Bitcoin into the economy. It processes payments, and it provides security to the network. Let's now look at how Bitcoin mining achieves these things. When a transaction is initiated, we mentioned earlier that it is sent out across the Bitcoin network. What does that actually mean? All Bitcoin clients (i.e. software) attempt to connect to multiple other Bitcoin clients referred to as peers. It is common for any individual client to connect to 10-20 other peers. Some of those peers are regular users making transactions, and a small number of those peers may be miners. When a Bitcoin client receives details of a Bitcoin transaction, it is passed along from client to client until in a short space of time it is received by at least one or more Bitcoin miners.

Bitcoin miners do something else besides solving a hashing problem and injecting Bitcoin into the economy, they provide the important function of creating the Blockchain, one block at a time. When a Bitcoin miner receives the details of a transaction, it is first validated to be authentic, and then recorded to a block locally on the Bitcoin miner's machine. If the Bitcoin miner is successful in solving the hashing problem, the solution to the problem is included as part of the block along with all the transactions made in the past 10 minutes. The block is then closed and distributed across the Internet and the process starts again. Anybody else on the network can independently validate that the transactions in the block are authentic, and that the solution to the hashing problem, referred to as the 'proof-of-work' is valid. Any subsequent miners that solve the problem are disregarded, their blocks no longer relevant and the process starts again. Therefore the Blockchain is a sequence of blocks that contain all the transactions for a given ten minute period. Each block is mathematically linked with the previous block, so it is trivial (for a computer!) to validate the entire Blockchain as being valid without analysing individual transactions.

And that brings us to the third objective that Bitcoin miners achieve: security for the network. The act of solving the cryptographic hashing problem doesn't serve only in the interests of the miner, it also serves to protect against a dishonest miner spending their money twice, appropriately known as a 'double spend'. Taking my earlier example of me sending 50 Bitcoin to Joe, and in return Joe giving me a book that I had purchased from him (based on today's prices, this would be a pretty expensive book). At the same time, what if I attempted to send the same 50 Bitcoin to another party, before the initial transaction had time to be processed and be validated? Assuming I have already received my goods from Joe, it would be problematic if the Bitcoin network somehow accepted my payment to the other party and later rejected the initial payment I made to Joe. Decentralised Bitcoin mining solves this problem.

When I send out my transaction to Joe on the Bitcoin network, the transaction almost instantly becomes visible to Joe (typically within a few seconds). At this point, the transaction is visible, but it has not yet been included in a block by a miner. If this were a low value transaction, or a transaction between trusted parties, visibility of the transaction on the network would generally be regarded as acceptable, however with a concerted effort on my part it might be still possible to double-spend the funds by initialising another transaction on the network that spends the same funds – but for low value transactions, the effort involved in doing so probably would not be worth my time (there are of course also the legal ramifications of getting caught). After approximately 10 minutes, we can expect that my transaction would now have been officially included in the latest block on the Blockchain by a miner. At this point, the transaction is said to have had 'one confirmation'. Now, when you consider that there are thousands of dedicated computers around the world mining Bitcoin, the probability of me attempting to defraud Joe by double-spending my funds and successfully mining a block that rejects the transaction to Joe is very difficult to do. For medium value or high value transactions it is generally considered prudent to wait for 3-6 confirmations, or in other words wait for 3-6 sequential blocks to be mined (between 30-60 minutes) to be absolutely confident of a transaction. For somebody to successfully double-spend in this scenario, they would need to have successfully mined 6 blocks in a row rejecting the transaction. And for this to occur, they would need to have control of around 50 % of the entire global computing power of the Bitcoin network. As you can see, this makes the act of double-spending extremely difficult and costly, generally outweighing the benefits of any double-spend in the first place. You can also see that as the Bitcoin network grows, the number of miners increases and the difficulty of the hashing problem becomes more difficult, it becomes ever-increasingly difficult for a dishonest miner to double-spend. This is how Bitcoin miners secure the network.

In summary, Bitcoin mining achieves three things: it processes transactions, it secures the network and injects Bitcoin into the economy. It's an elegant system.

CHAPTER ELEVEN

THE MINER'S INCENTIVE

Now is the time to point out that a miner has the option as to whether or not to include a transaction in their block. A miner is free to reject every transaction if they wish and simply solve the hashing problem. This is called 'mining an empty block', and it happens occasionally. So the question then is why would a miner bother to include transactions in a block at all? There are a number of reasons. First of all, in relation to the work the miner is performing in attempting to solve the hashing problem, including transactions in the block is a trivial operation that puts a negligible demand on their computer. Secondly, it is in the interest of Bitcoin collectively to include transactions in the Blockchain. If miners didn't include transactions on the Blockchain, Bitcoin wouldn't work, and if it didn't work then Bitcoin would be of no value. If Bitcoin were of no value then the miners would be spending all of their effort mining something that was worth nothing. You may argue that it is collectively better for the community for Bitcoin miners to include transactions in a block but detrimental to an individual miner for spending their resources processing those transactions. That is partially true, but as per my first point the effort involved is negligible. There is also a third point. Miners are unable to charge a fee to include transactions in a block, but people initiating a transaction may voluntarily offer a fee. Miners then have the option of rejecting transactions that either don't include a fee component or rejecting orders with a fee lower than a particular threshold. So, what is the typical fee today? Much of the time it is zero. In today's economy, the miner's incentive is primarily driven by the value of the Bitcoin earned for successfully mining a block. The transactions are included as part of the goodwill of the miners in the interests of growing the Bitcoin economy and the growth of Bitcoin. In some cases, Bitcoin clients automatically include a small fee (no more than a few cents) to ensure that transactions won't be rejected by miners and are more likely to be included in the next block that is mined.

Over time, the number of Bitcoin earned for the successful mining of a block will gradually be reduced, until around the year 2140 when the reward for mining a block reaches zero. It is expected that over that long period of time, as the reward incentive for mining Bitcoin is slowly reduced, that incentive will slowly be subsidised and eventually replaced with the incentive of transaction fees.

Due to the fact that the entire Bitcoin economy is an open market, and that transaction fees are voluntary, the fees will always be in line with supply and demand, resulting in a competitive marketplace with low transaction fees.

CHAPTER TWELVE

TL;DR

TL;DR: a well-known expression meaning 'too long; didn't read'. It's the brief summary at the end of a long prose that provides a much abridged version of the content. Unfortunately however, if you've come to this section without reading the preceding Part II chapters outlining the core Computer Science principles behind Bitcoin, then this section will be difficult to understand, and you will be forever limiting your understanding of Bitcoin to analogous comparisons. If you have read Part II, then this section serves to bring all those ideas together into a coherent understanding of Bitcoin.

We first learned that asymmetric cryptography is the technology behind public and private keys; and by using this relationship we are able to mathematically verify the authenticity of a Bitcoin transaction that has been digitally signed by the sender's private key. We then learned about the cryptographic hash, which is an irreversible algorithm performed on a piece of data. By trial-and-error (over a quadrillion attempts per second), miners on the Bitcoin network are able to attempt to calculate a cryptographic hash on random pieces of data until the resultant hash value falls within a pre-defined limited range – a problem designed to take on average ten minutes for the entire Bitcoin network to solve. The difficulty of that problem both protects the network from 'double-spends', as well as controls the supply of Bitcoin. In addition, the miners are also processing Bitcoin transactions which form a block. A miner who successfully mines a block (by solving the cryptographic hashing problem) has his block recognised by the Bitcoin network and it is forever included on the Blockchain – Bitcoin's public, decentralised ledger. And that is the briefest description of how this complex, elegant system works.

PART III

A BROADER LOOK

CHAPTER THIRTEEN

MT. GOX

If you knew nothing of Bitcoin before reading this book, you still may have heard the name Mt. Gox, thanks to the mainstream media. Mt. Gox forms an interesting part of Bitcoin history, so it's worth understanding what happened. Mt. Gox is a bankrupt Japanese Bitcoin exchange that was run by a French national by the name of Mark Karpelès.

Prior to 2013, Bitcoin was barely known outside of a small handful of people around the world. It had not reached mainstream and there was no discussion about it by any of the major governments around the world. If you wanted to buy Bitcoin during this time, you were pretty limited for options. At that time, Mt. Gox was by far the largest Bitcoin exchange in the world, claiming to have more than 80 % of the market of people trading Bitcoin. I suppose this was close to the truth, as there were not many other alternatives during that period.

Due to Mt. Gox having the overwhelming majority of Bitcoin trade, and most people understanding very little about Bitcoin, Mt. Gox's name became almost synonymous with Bitcoin itself. Incidentally, there is a well-known story as to why Mt. Gox was called Mt. Gox. Apparently when the site was created, the original owner had already purchased the domain name *mtgox.com* for another project he was working related to a card game called 'Magic: The Gathering'. The domain name therefore represented 'Magic The Gathering Online eXchange'. The idea for that site was later abandoned and the domain name was reused for a Bitcoin exchange became known as 'Mt. Gox'. The original owner sold the majority of his company sometime later to Mark Karpelès.

Now, I suppose that in the early days of Mt. Gox, perhaps nobody envisaged the site would come to much – perhaps they did, but I doubt they could've expected the incredible growth of Bitcoin starting in early 2013. For various reasons, Bitcoin began to flourish taking the value of a single Bitcoin from around USD 10, to around USD 250 in a few short months. The price would later rise to over USD 1,000 by the end of that year. And where did people go to purchase their Bitcoin? One of the only places they could – Mt. Gox.

I have to point out that I have no inside information on what Mt. Gox did or didn't do, I only knew Mt. Gox as one of their customers and from discussions with others in the industry. It was around this time in early 2013 that my business partner Adrian and I used Mt. Gox to purchase some Bitcoin of our own. Having spent the majority of our careers designing software systems for financial institutions, the Mt. Gox platform seemed unprofessional and amateurish. It took several weeks for them to open and verify our accounts, their customer service was poor and their site had not been updated in quite some time. On top of this, there had been stories of Mt. Gox systems failing under moderately heavy load, and reports of their systems being 'hacked' and people losing their money. Certainly not the type of financial

system that I would trust my money with. That being said, we did want to buy some Bitcoin. Our strategy was to deposit relatively small sums of money, purchase Bitcoin, and then withdraw the Bitcoin immediately and repeat. This way, should there be any issues with Mt. Gox our losses would be limited to our last deposit amount. Unfortunately for many other Mt. Gox customers, they did not take the same approach. In mid-2013, it was obvious that Mt. Gox were in trouble as withdrawals were initially suspended and shortly after that, the company declared bankruptcy, admitting to the loss of nearly all Bitcoins held on behalf of their customers which at the time of their bankruptcy was worth approximately half a billion US dollars, or around 7 % of all Bitcoin in circulation.

On any scale, this event was a disaster for Bitcoin in general. It was a disaster for anyone that had accounts with Bitcoin and it was a disaster for the reputation of Bitcoin which many had seen as a failure in itself due to Mt. Gox's mismanagement. I don't know why Mt. Gox lost the funds they did. In one of their announcements they suspected they were stolen, but ultimately it's just speculation as to how it came about – the point is they were gone and many people had lost a lot of money because of it.

With remorse for those affected by the Mt. Gox collapse, the announcement of their bankruptcy was in some ways welcome. Their delays and suspension of withdrawals which lasted many months was causing an ongoing issue for the Bitcoin community, and significantly bad press in the media. Mt. Gox were a ticking time bomb. Their collapse allowed for a clean slate, and other companies, with far more credibility than Mt. Gox to replace them and take Bitcoin forward.

It could also be said that it was partly Mt. Gox's poor platform that guided us into the direction of creating our own Bitcoin exchange, Independent Reserve. We knew that for Bitcoin to be ultimately successful, there needed to be a stable, robust platform for which people could purchase Bitcoin and that Mt. Gox was not that platform.

CHAPTER FOURTEEN

SILKROAD

If you didn't hear about the Mt. Gox collapse in 2014, then perhaps you heard about Silkroad. Incidentally the name 'silk road' originally referred to a series of trade routes connecting Asia to Europe throughout many periods of history. It was named as such due to the lucrative trade in Chinese silk along its routes, and contributed much to the expansion of trade between the two continents.

The Silkroad we are referring to here however was a special type of website. It was special because it could not be accessed using a regular web browser. It could only be accessed using specialised software known as 'Tor'[9], which anonymised one's identity allowing people to access the site without it being traced back to them. The Silkroad website was essentially a marketplace where you could buy and sell goods. Due to the fact that it was set up with the express intent of anonymising people's identity, the goods for sale were largely black market items that were not available on regular websites where the authorities could monitor activity. Thus, the predominant products available on Silkroad were illegal drugs, prescription drugs, firearms and other illegal products.

Silkroad used Bitcoin as its currency, due to the fact that Bitcoin could be transferred between market participants anonymously[10]. Unfortunately, this tarnished Bitcoin's reputation as the media made the false inference that because Silkroad uses Bitcoin as its currency then all Bitcoin users are pirates and drug dealers on Silkroad. In October 2013, the FBI were able to track down the administrators of the site and the site was shut down[11]. What happened to the Bitcoin price? It took a slight dip and then continued to rise. The reason being that the vast majority of Bitcoin users were not pirates and drug dealers, and the fact that Bitcoin continued to flourish despite the absence of Silkroad was a testament to this fact.

There are a few lessons we can take away from this. First of all, all currencies are and will continue to be used for illegal purposes to a certain extent – that's a testament to their usefulness as a currency. In November 2013, a United States Senate enquiry had the

---

[9] 'Tor' is an acronym for 'The Onion Router' and is a project originally developed by the U.S Navy, designed to anonymize and encrypt online communication. The software is now widely used on the internet to provide anonymous web browsing to people wishing to protect their privacy online.

[10] Refer to 'Chapter 18 – Anonymity' for a deeper discussion about this topic.

[11] Silkroad has since been replaced by other anonymous black markets that sprang up in it's wake.

Financial Crimes Enforcement Network point out that any illegitimate use of Bitcoin was insignificant compared with the USD 1.6 trillion in 'global criminal proceeds' in 1999.

It's also worth noting that any trades made on Silkroad between two anonymous parties resulted in zero violence in the community, contrary to the violence that is sometimes associated with cash trades made on the street.

CHAPTER FIFTEEN

OTHER DIGITAL CURRENCIES

Bitcoin is not the only digital currency, however it was the first and most successful internationally, and has an overwhelming 98 % majority of the market in terms of market capitalisation when compared to other digital currencies. Bitcoin first became operational in 2009, and it wasn't until 2011 that we saw any other alternate digital currencies, such as Litecoin, which is largely a clone of Bitcoin, with a few of its settings slightly tweaked.

I believe that the developers of some of these earlier currencies were well intended, however today there are more than 500 'alternative to Bitcoin' digital currencies around the world that most people (including myself) have never heard about, and I believe a good number of them to be nothing more than a scheme for the original developer to profit by.

Having said that, despite the great evolution Bitcoin has been to the history of money, it is still not perfect and it is inevitable that the Bitcoin protocol will be refined over time (as it has been), and that potentially new digital currencies may be viable concurrently with Bitcoin or ultimately replace Bitcoin. The concept of the Blockchain is fundamentally sound and most, if not all, digital currencies are based on the same core principles as Bitcoin.

CHAPTER SIXTEEN

SECURING YOUR BITCOIN

We've mentioned already that Bitcoin shares some of the properties of physical cash. Bitcoin however has a number of properties that allow you to protect them from accidental loss or theft in a way that regular cash cannot.

To begin with, you can 'back up' your wallet. That means exactly what it sounds like, in the same way you can back up your photos, or your emails, you can create a copy of your digital wallet and store it in multiple locations. This is the simplest way to protect your Bitcoin against accidental loss. If you lose your phone with your Bitcoin wallet, or your computer storage fails, you can recover all of your money from the backup. What's even better is that you don't need to back up your wallet after every transaction. Most modern Bitcoin wallets are designed in such a way that once your wallet is backed-up, even if it contained no funds at the time it was backed-up – future funds received will still be recoverable, so you only ever need to back up your wallet once. Some wallets are designed in such a way that you can even generate new addresses, and you still only ever need to back-up your wallet once and it is backed-up forever[12].

Backups protect your wallet against accidental data loss, but they don't protect your wallet against theft. However wallets are easily encrypted and can be protected with a strong password. This way if somebody steals your phone with your Bitcoin on it, they won't be able to spend the Bitcoin without your password. Meanwhile, you can recover those stolen Bitcoin from your backup, and just to be safe, transfer them to a new wallet. That way if a thief does manage to guess your password, the Bitcoin have already been sent to a new address and your old wallet is completely useless to them. All of these features do not require specialised skills to master, they are generally included as part of most Bitcoin software and are very easy to use, even for the novice.

These facilities are great for protecting funds up to a reasonable amount, however when dealing with a large value of Bitcoin, let's say a million dollars' worth, we may want to take additional precautions. After all, what if an attacker gained access to our computer, and was able to install a key-logger to secretly record your password you've typed in? History has shown there is no limit to the cunning and nefarious techniques thieves have dreamt up when it comes to stealing money. One only needs to look at some of the famous Las Vegas casino

[12] These are known has 'Hierarchical Deterministic' wallets or 'HD Wallets' for short.

heists for the lengths people have gone to when large sums of money were at stake. Still, Bitcoin provides some excellent options when it comes to security. One such way of protecting a large sum of Bitcoin is via what's referred to as 'cold storage'. The term cold storage, in this context, refers to keeping Bitcoin stored on a computer or device that is in no way connected to the Internet. A computer or mobile phone that is connected to the Internet has the potential to be hacked by anybody anywhere in the world if a weakness is found. But, by storing Bitcoin on a computer that is not connected to the Internet, you immediately limit the potential threats to only those posed by people who have physical access to that computer. Of course, that computer should still contain a wallet that is encrypted and protected by a strong password. Modern software easily facilitates the ability to store your Bitcoin in cold storage.

Bitcoin has even more advanced security features also, such as 'multiple signature' (colloquially known as 'multi-sig') addresses. In all our examples so far, we have described myself sending 50 Bitcoin to my friend Joe, in a transaction which is signed by the corresponding private key which I have. In the case of multi-sig addresses, transactions can be configured to require two independent people to sign the transaction, or three people, or two out of three people, or any combination of signatures that you can dream up. For example, you may have a Bitcoin wallet that requires a signature from both yourself **and** your business partner before the transaction is approved, or yourself **or** your business partner. Or perhaps you have a board of directors and that a transaction must be signed by any three of the seven directors. Such facilities are extremely powerful and allow you to secure Bitcoin in a way that cannot be done with physical cash.

The final method that we will talk about for securing your Bitcoin wallet is what's known as a 'paper wallet', and the paper wallet is the most primitive of all devices for securing your Bitcoin. You may simply print out the private key on paper, which in the event you are affected by an EMP [13] that destroys all your electronic devices, you can recover your funds using the private key that you printed out on paper. Of course you could go further and print half your private key on one page, and half on another page and keep them in secure, separate locations – the options are endless.

---

[13] An 'EMP' is what's known as an "Electromagnetic Pulse', and consists of a short, intense burst of energy which may cause data stored on computer drives to be lost irrecoverably. These may occur naturally, like for example from a lightning strike or could be man-made, in the form of a weapon.

CHAPTER SEVENTEEN

SMART CONTRACTS

So far in this book, we have discussed the most common and basic type of transaction – party A sending money to party B. We've looked at how Bitcoin achieves this, and some of the great benefits this provides over regular currency. However, by using this example, we have only just scratched the surface of what Bitcoin and Blockchain technology are truly capable of achieving. Introducing the idea of smart contracts. Bitcoin is capable of creating complex transactions that involve multiple parties. Let's look at an example.

Let's say a car manufacturer builds a new car. As part of the build process a new Bitcoin address is generated, and a token amount of Bitcoin are deposited to address (i.e. 0.0001) so that it is recorded to the Blockchain. That public address is assigned by the manufacturer to that car. The private key is then given to the dealer, who may store it on his mobile phone so that his phone also acts as a car key, enabling him to open and start the car.

When the dealer goes to sell the car to a customer, a transaction is written in such a way that the purchase price is transacted to the seller and the vehicle is transacted to the buyer – potentially an address he has access to from his mobile phone. Both parties must sign the transaction in order for the transaction to become valid and be included on the Blockchain. With the transaction complete, the buyer may now present his mobile phone to the car via NFC [14]and the car would recognise its new owner and start the ignition. In this example, the transaction between the two parties happened simultaneously, and therefore neither party was required to trust the other party. Furthermore, the buyer may review the entire transaction history of the car on the Blockchain to ensure that it is authentic and he can ascertain that the seller was the true owner of the car.

Let's expand on this example. What if the buyer couldn't afford the car, and so he needed to borrow money to make the purchase. A Bitcoin transaction could be constructed in such a way that a creditor retains the ownership of the vehicle until either the agreed amount was repaid within a specific time limit, whereby the vehicle is then automatically transferred to the debtor, or else the debtor forfeits their collateral and the creditor retains ownership of the vehicle.

---

[14] NFC is what's known as 'Near Field Communication' and is a technology increasingly common on modern phones which enables communication between devices in close proximity to each other.

The concept of a multi-party agreement is not new, banks lend money all the time. Using Bitcoin and Blockchain technology however, the process becomes far more efficient and there is less trust required between two parties to fulfil the obligations of the contract which are enforced automatically by the Bitcoin network. It will be interesting to see what new uses for Bitcoin the Blockchain people will discover tomorrow.

CHAPTER EIGHTEEN

ANONYMITY

One of the big questions that has been raised in relation to Bitcoin is whether transactions are anonymous, and if they are anonymous, the potential for Bitcoin to facilitate money laundering and other crime. The answer here is that it is, and it isn't. Let's take a look at that more closely.

Let's say I make a purchase of a large item worth a million dollars from a total stranger, and he gives me a new Bitcoin address into which I am to deposit 10,000 Bitcoin. At this point, this is an anonymous transaction. Presuming the other party has generated a brand new address, I have no way of identifying who the other person is, and nobody can associate the receipt of 10,000 Bitcoin to that person. Assuming the other person holds on to those funds and never spends them, they remain anonymous. At some point however the stranger will likely want to spend his 10,000 Bitcoin, or perhaps sell his Bitcoin for fiat currency[15]. Now if the stranger were to find another stranger on the street and trade his 10,000 Bitcoin for a million dollars in cash, then things are still pretty anonymous. Generally however, particularly with larger sums of money, a person is going to need to spend that money with a legitimate business or exchange it at a reputable exchange. At these points, particularly currency exchanges, a strong identity check is required by individuals opening accounts to comply with AML/CTF [16] regulations enforced in the traditional finance sector. Once money starts being transacted through these mainstream channels, it's now possible for an investigator to start connecting the dots and trace a history of transactions. So, is it anonymous? It can be, to a similar extent that cash is anonymous. Cash can be anonymous too, but if you one day turn up to a bank with a million dollars in cash the authorities may raise an eyebrow.

---

[15] 'Fiat Currency' is money that a government has declared to be legal tender, but is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material that the money is made of.

[16] AML/CTF stands for 'Anti Money Laundering / Counter Terrorism Financing' and consists of a set of legal requirements that banks and other financial institutions are required to follow in relation to ensuring that their customers do not use money for illegal purposes. Because Bitcoin exchanges deal in traditional currency as well as Bitcoin, they are usually also required to follow various procedures to identify their customers and report suspicious transactions.

CHAPTER NINETEEN

REGULATION

A question a lot of governments around the world are now asking themselves is whether Bitcoin should be considered legal tender, and if so, should it be regulated, and if so, to what extent.

The answer in my opinion is that Bitcoin requires balanced and carefully considered regulation. Regulation that does not stifle a new industry, yet at the same time protects consumers from industry malpractice. The other point to consider is that we can't take yesterday's laws that applied to an entirely different financial paradigm, and apply them to Bitcoin. Bitcoin works in a fundamentally different way to fiat currency, and regulation needs to be developed that supports the decentralised, digital model.

The question then becomes, what does that regulation look like? Well I believe it's absolutely necessary to allow Bitcoin and other digital currencies as legal tender, the concept of a state issued currency may one day be a relic of the past. Governments and economies should embrace this new world currency and watch as trade flourishes as people are able to make transactions across the world in the blink of an eye without being retarded by yesterday's creaking banking systems. And Bitcoin aside, I can tell you first hand as a software engineer that spent many years developing software for financial institutions that the majority of the systems that I have seen are truly ancient. Mainframe systems that were developed more than 30 years ago that require specialised (read old) engineers to maintain them. This is one of the many reasons banks are slow to adopt new technologies as their systems are not readily upgradeable.

The embracement of Bitcoin can lead to increased trade worldwide, perhaps bringing entire nation-states out of poverty, turning them into flourishing economies.

Where I believe regulation *is* required, is with financial institutions that are holding Bitcoin on behalf of others, much like a bank. We have already witnessed the first great financial collapse in Bitcoin with the fall of Mt. Gox, and as recently as a week ago to the day that I am writing this, we saw Bitstamp, a European based Bitcoin exchange, lose five million dollars' worth of Bitcoin from their digital vaults. To their credit, in the case of Bitstamp, the majority of their funds was held safely in cold storage and they are honouring their account holders' balances. It does highlight however that without some oversight on the security measures these organisations have in place, consumers cannot have confidence in the institutions responsible for holding their Bitcoin.

It's important to point out that this is not a weakness with Bitcoin itself, it is merely a sign of immaturity in the Bitcoin financial sector. Already within the past twelve months since the collapse of Mt. Gox we have seen the entire industry take great strides in security best practice, and no doubt we will continue to do so. It is in everyone's best interest to have a

strong, stable, secure Bitcoin financial sector – and it is in this area that a balanced level of regulatory oversight would not be amiss.

It is important for regulators to be mindful of the fact that as a new industry, it is developing at a very fast pace and new practices are being evolved all the time. It would be a step-backwards for regulators, with a limited understanding of an evolving industry to take a strong-hand in implementing impossible to meet regulations or regulations that are detrimental to the growth of Bitcoin. Their best move is to stand back for now and watch things carefully, and as the industry matures to step-in where appropriate. This principle could probably apply to most industries.

CHAPTER TWENTY

TIMELINE

There have been many events which have significantly shaped the face of Bitcoin, from the original inception in late 2008, to the flourishing industry it has now become. The following are some of the key points in this timeline.

Oct 2008 An anonymous whitepaper was published entitled 'Bitcoin: A Peer-to-Peer Electronic Cash System', describing essentially what would become Bitcoin. The white paper was published by a person using the pseudonym *Satoshi Nakamoto*.

Jan 2009 The first block on the Bitcoin Blockchain was mined, known as the 'genesis' block, and version 0.1 of the Bitcoin software (including source code) was made publically available. The software was written anonymously, and due to its rather unconventional programming style combined with a strong theoretical know-how and completeness, it has been speculated at length as to whether it was written by an academic with little programming experience or possibly a team of people.
It was here, on the 12th of January 2009, that the first Bitcoin transaction took place - from Satoshi Nakamoto to Hal Finney.

Oct 2009 A website known as New Liberty Standard published what it thought was an appropriate exchange rate for Bitcoin at the time, based upon a formula that included the cost of electricity to run a computer mining Bitcoin. Their suggested exchange rate was USD 1 = XBT 1309.03.

Feb 2010 The first Bitcoin exchange was born, known as 'The Bitcoin Market'. The exchange did not last long, and due to problems it was experiencing with fraud it closed down just over a year later in 2011.

May 2010 A software engineer in the United States named Laszlo, famously bought a couple of pizzas from Jercos for 10,000 Bitcoin. The pizzas were otherwise valued at USD 25 (equivalent to a Bitcoin price of USD 0.0025).

Jul 2010 Bitcoin was mentioned on the famous IT website *Slashdot*, causing a ten-fold increase in price in less than a week. The price rose from around USD 0.008 to USD 0.08.

Mt. Gox was launched in the same month by Jed M^cCaleb after reading about it on Slashdot. It's interesting to note what Jed M^cCaleb said sometime later in 2011 after selling Mt. Gox:

"*I created mtgox on a lark after reading about bitcoins last summer. It has been interesting and fun to do. I'm still very confident that bitcoins have a bright future. But to really make mtgox what it has the potential to be would require more time than I have right now. So I've decided to pass the torch to someone better able to take the site to the next level*."

To put that another way, M^cCaleb developed Mt. Gox in a matter of weeks or months by himself in his spare time – all credit to him as it was a hobby and at the time Bitcoin was of no real worth. He also recognised this fact at the appropriate time when he sold it. Compare this to a modern exchange such as Independent Reserve, which took a team of professional developers over 18 months to build with all of the appropriate measures designed into the system for ensuring its security, scalability, stability and robustness. It's no wonder that without extensive re-development work, Mt. Gox would not have been capable of supporting a multi-billion dollar industry in the future.

The other interesting thing to come out of July 2010 was that this was the month somebody had developed a way of using a computer's GPU (graphics processing unit) to mine Bitcoin faster than what was possible using the conventional CPU mining approach.
The bitcoin global mining network hash rate now totalled 1 Giga Hash (GH), or 1,000,000,000 (1 billion) hashes per second.

Aug 2010 A vulnerability in the Bitcoin protocol was discovered and subsequently exploited. This lead to the creation of over 184 billion Bitcoin generated in a single transaction. Within hours, the exploit was spotted and the vulnerability was corrected. The transaction history from that transaction forward was permanently erased. This has been the only major security flaw discovered and exploited in Bitcoin's history.

Nov 2010 The market capitalisation of Bitcoin for the first time exceeded one million US dollars. The price on Mt. Gox reached USD 0.50.

Dec 2010 The global mining network hash rate exceeded 100 GH for the first time.

Feb 2011 Silkroad, the online black market trading using Bitcoin as a form of payment, opened for business. In the same month, Bitcoin reached parity with the USD on Mt. Gox for the first time.

Mar 2011 Jed McCaleb sold Mt. Gox to Mark Karpelès.

Apr 2011 Bitcoin reached the mainstream media for the first time, with TIME publishing an article about Bitcoin, '*Online Cash Could Challenge Governments, Banks'*.

Jun 2011 The price of a single Bitcoin surpassed USD 10 on Mt. Gox for the first time. In the same month, Mt. Gox began to show signs of trouble with a serious security breach in their system resulting in over 60,000 users' personal details compromised, as well as fraudulent sell orders of hundreds of thousands of Bitcoin, causing the price to plummet to just USD 0.01.

June also saw the largest ever Bitcoin theft. It was reported that 25,000,000 Bitcoin were stolen, worth over a quarter of a million US dollars.

WikiLeaks began accepting Bitcoin donations the same month.

Jul 2011 Only a month after Mt. Gox's security breach, a Polish Bitcoin exchange, at the time the world's third largest, lost 17,000 Bitcoins they were holding on behalf of their clients.

Aug 2011 Another Bitcoin company that processed Bitcoin transactions lost over 150,000 Bitcoin worth over USD 2 million at the time.

There were a number of other incidents similar to this during this time. You can see it was a bit of a bad run for Bitcoin, so it's worth taking the time to analyse what exactly we mean by a 'loss' and why these kept happening. It should be noted that in each of these examples (apart from the vulnerability discovered in August 2010), the flaw had not been with Bitcoin itself but with the incompetence of the individuals that were running the companies that had been entrusted with the responsibility of holding Bitcoin on behalf of others. During this period, and to a large extent today, these companies had no regulatory oversight, yet people had entrusted them with millions of dollars' worth of their own Bitcoin.

At the most fundamental level, a Bitcoin wallet containing a person's Bitcoin is essentially a file, or series of files on a computer. In order to protect those files, we need to back it up and encrypt it, as described in the chapter 'Securing your Bitcoin'. An organisation responsible for millions of dollars' worth of other people's Bitcoin essentially has the same task to do, however the practices in place should be somewhat more robust (compare the protection of notes in your wallet, to a bank vault, to the gold in Fort Knox – as the value and the responsibility increases, the level of security measures needs to be raised appropriately). If the files containing Bitcoin private keys are damaged or corrupted (e.g. due to faulty hardware), or a thief manages to gain access to the computer and steal the files, then that is how Bitcoin are lost.

Today there are fewer incidents of such security breaches, but it is still a constant threat and companies and individuals need to be mindful of this.

Oct 2011 An alternative coin to Bitcoin, called "Litecoin" was released by an ex-Google staff member.

May 2012 An online gambling game known as SatoshiDICE accounted for more than half of all Bitcoin transactions during the month.

Jun 2012 Well known online Bitcoin wallet Coinbase was founded in San Francisco, United States.

Nov 2012 First Bitcoin mining reward halving day - where the XBT 50 mining reward dropped to XBT 25 reward per block (the halving day ouccred at mined Block 210,000).
The popular online blogging platform, 'Wordpress' began accepting Bitcoin as a payment alternative.

Dec 2012 The first Bitcoin exchange to be licensed as a European bank 'Bitcoin Central', began operating within the European regulatory framework.

Jan 2013 The first "Application Specific Integrated Circuit" or ASIC Bitcoin Mining machines were released. Just as the GPU surpassed the CPU, the ASIC is now the most powerful and efficient machine available – specifically dedicated hardware to mining Bitcoin.
BitPay, a United States based Bitcoin payment processor announced that it had surpassed 10,000 Bitcoin transactions for its merchants.

Feb 2013 The price of a single Bitcoin reached an all-time high, breaking the USD 31.91 peak held on Mt. Gox 601 days earlier in June 2011.

Mar 2013 A famous fork in the Blockchain occurred, caused by two different versions of Bitcoin software behaving differently. What this meant was that some users running an older version of Bitcoin software saw some transactions, while users with the new version saw a different set of transactions. The fork was quickly rectified with Bitcoin miners all reverting to an earlier version of the software. The price of Bitcoin dropped temporarily during this period, but quickly rallied to its price prior to the fork.

By the end of the month, the price had risen further with the total market capitalisation of Bitcoin reaching over one billion US dollars for the first time.

Apr 2013 The price continued to rise dramatically during April, reaching over USD 250. The Cypriot financial crisis had been cited as a potential catalyst for the unprecedented rise. After peaking, the price settled at around USD 120 for the next few months.

May 2013 Something that struck me as interesting during my research, was that a US based computer game company, ESEA, was using their customer's computers via a carefully engineered malware program to secretly mine Bitcoin into their own accounts. They were caught and subsequently sued for over a million dollars, with a class action suit outstanding.

This is certainly not the only reported example of such activity. At one of my previous places of employment, an employee was fired for secretly using high-end company workstations for Bitcoin mining.

Probably less interesting, but more relevant was that the first Bitcoin ATMs were unveiled in San Diego, United States during the same month.

Also during May, we saw Coinbase receive USD 5 million in investor funding, the largest investment to date in the Bitcoin industry.

Jun 2013 Our company, Independent Reserve, was founded in Sydney, Australia after spending six months analysing Bitcoin and the Bitcoin market to see how we could best fit into the new economy. We decided that a robust Bitcoin exchange was needed in Australia, to form a strong foundation that other Bitcoin based businesses could utilise as the basis for their own offerings.

Aug 2013 A United States federal Magistrate ruled Bitcoin to be legal tender. At the same time the German government legitimised Bitcoin, declaring digital currencies to be a 'unit of account'. Bitcoin also arrived on the Bloomberg terminals in August, with the currency code XBT.

Sep 2013 The global Bitcoin mining power reaches 1 Petahash for the first time, or 1,000,000,000,000,000 (1 quadrillion) hashes per second.

Oct 2013 The infamous Silkroad website was shut down by the FBI. Rather than cause a market collapse as sceptics had predicted, the value of Bitcoin took a brief dip before continuing to rise as it became evident that the majority of transactions were not related to Silkroad, and that Silkroad was a relatively small player in the Bitcoin economy.

During the month, the global investment bank Merill Lynch called Bitcoin a potential '*major means of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers*'.

Also during October, China's largest search engine, Baidu, became the first service of its kind to accept Bitcoin.

Nov 2013 Head of US Federal Reserve, Ben Bernanke publically declared that Bitcoin '*may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system'*. A United States Senate hearing into Bitcoin also strongly weighed in favour of digital currencies, with the Financial Crimes Enforcement Network declaring Bitcoin to be innovative and useful, and it cautioned that premature regulation could stifle Bitcoin innovation. They also pointed out to detractors that any illegitimate use of Bitcoin was insignificant compared with the USD 1.6 trillion in 'global

criminal proceeds' in 1999. The positive results from the US Senate hearings saw the Bitcoin price surge to a record USD 1,242 in November.

At the same time, billionaire entrepreneur Sir Richard Branson announced on CNBC that his commercial space flight venture 'Virgin Galactic' will accept Bitcoin as payment. He called it 'a new exciting currency'. Virgin had already accepted its first payment worth approximately USD 250,000.

At this point in the history of Bitcoin, Bitcoin was being used to move more money than Western Union at approximately USD 245 million a month.

Dec 2013 One of Elon Musk's (PayPal, SpaceX, Tesla, SolarCity) Tesla Model S electric cars was sold in the US for Bitcoin. The value of the car was approximately USD 103,000 at the time.

However, whilst Bitcoin was flourishing in the West, in the East, China's Central Bank banned financial institutions from handling Bitcoin transactions, causing the price to crash to nearly USD 500. Due to the ruling, Baidu were forced to stop accepting Bitcoin payments.

Jan 2014 The global bitcoin mining power reached 10 Petahash for the first time.

Mar 2014 The UK tax office declared that Bitcoin was to be treated as a currency for transaction purposes.

Jun 2014 Expedia, one of the world's largest travel agencies began accepting Bitcoin payments.
The global bitcoin mining power reached 100 Petahash for the first time.

Jul 2014 Dell, one of the world's largest computer manufacturers began accepting Bitcoin payments.

Sep 2014 PayPal, one of the world's largest payment processors gave its merchants the option of accepting Bitcoin payments.

Oct 2014 Independent Reserve, Australia's most secure and advanced Bitcoin Exchange to date launched in Sydney.

Nov 2014 The Australian Senate began an inquiry into the use of Bitcoin and digital currency in Australia.

Dec 2014 Microsoft, one of the world's largest software companies, began accepting Bitcoin for some online purchases.

Jan 2015 The New York Stock Exchange, along with a consortium of international banks invested USD 75 million into the Bitcoin industry.

Aug 2015 The Australian Senate inquiry into Digital Currencies released its recommendations, calling for Bitcoin to be treated as regular money for taxation purposes and that Anti Money Laundering laws should be applied to Digital Currencies. This outcome was seen as a very positive step by the Bitcoin industry in Australia, as it brought further legitimacy to the young currency.

AFTERWORD

By Adrian Przelozny

I truly hope that you enjoyed reading Adam's book as much as I enjoyed the time I spent editing and finalising his manuscript. Adam and I had worked on so many different projects together over the past 14 years, that it often felt like he was right there with me, working together on this book, arguing with me about the specific wording of a sentence or trying to convince me that his interpretation of an obscure grammatical rule was more correct than mine.

Whilst working on the book, I debated whether or not to include additional chapters or expand too much on any of the sections. I know that Adam would have probably written more, had he gotten the chance, but I decided that it was best to keep this book authentic, to showcase Adam's work and thoughts. This to me was more important than adding another chapter on say 'Sidechains' or 'The Future of Bitcoin', and it is my opinion that the book stands strong as it is, without the need for additional content.

It saddens me that Adam was not able to see his ambitions realised and see this book go to print. I know it would have filled him with pride to have seen this project through to completion. It was the culmination of many hours of writing, along with years of research and hard work in IT and the Bitcoin industry, that allowed him to gain the knowledge and insights to write this book.

I know he would have been happy with this publication, which will see his name live on for many years to come.

- ***Adrian Przelozny***