
BLOCKCHAIN
NOVICE TO EXPERT
2 MANUSCRIPTS
BY KEIZER SÖZE

BLOCKCHAIN

Novice to Expert

2 manuscripts

by

Keizer Söze

Disclaimer

This Book is produced with the goal of providing information that is as accurate and reliable as possible. Regardless, purchasing this Book can be seen as consent to the fact that both the publisher and the author of this book are in no way experts on the topics discussed within and that any recommendations or suggestions that are made herein are for entertainment purposes only.

Professionals should be consulted as needed before undertaking any of the action endorsed herein.

Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States.

The information in the following pages is broadly considered to be a truthful and accurate account of facts and as such any inattention, use or misuse of the information in question by the reader will render any resulting actions solely under their purview. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall the reader or anyone else after undertaking information described herein.

Additionally, the information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its prolonged validity or interim quality. Trademarks that are mentioned are done without written consent and can in no way be considered an endorsement from the trademark holder.

Table of Contents – Book 1

Chapter 1 – Blockchain in a nutshell

Chapter 2 – The history of finance

Chapter 3 – Bitcoin basics

Chapter 4 – The trigger

Chapter 5 – The Inventor

Chapter 6 – I am not Satoshi

Chapter 7 – I am Satoshi

Chapter 8 – Satoshi is Hungarian?

Chapter 9 – Distributed ledger system

Chapter 10 – Miners

Chapter 11 – Block creation

Chapter 12 – Security on the blockchain

Chapter 13 – Business purposes

Chapter 14 – The future of banking

Chapter 15 – Overview

Table of Contents – Book 2

Chapter 1 – Fundamentals of Bitcoin mining

Chapter 2 – Blockchain attributes

Chapter 3 – Peer-to-peer network

Chapter 4 – Hashing

Chapter 5 – Cryptography

Chapter 6 – Digital Signature

Chapter 7 – Logarithm basics

Chapter 8 – Diffie-Hellman Key Exchange

Chapter 9 – Elliptic Curve Cryptography

Chapter 10 – Encoding arbitrary data

Chapter 11 – Checksum

Chapter 12 – Vanity addresses

Chapter 13 – Blockchain is a money

Chapter 14 – The great Ledger

Chapter 15 – The Blocks

Chapter 16 – Platform testing

Chapter 17 – SegWit

Chapter 18 – Soft fork VS Hard fork

Chapter 19 – Lightning Network

BLOCKCHAIN

for beginners

Volume 1

by

Keizer Söze

Introduction

Congratulations on purchasing this book and thank you for doing so.

This book is an excellent beginner's guide to understanding the technology called Blockchain. The contents avoid technical details to provide a better understanding to those who are new to this technology. There are certain terms that some technical background in Information Technology would help. However, it's not necessary. Everyday English has been used through this book to avoid confusion, and this book will take you by the hand and show you, step-by-step, how digital currency was born.

For better understanding, we go back in time, and summarize the history of finance, then explain what has triggered the birth of several cryptocurrencies in our current society. Next, we analyse the theory and the primary focus behind the inventor of Bitcoin. Then take a closer look at the possible candidates of the birth father of Blockchain in more depth. Next, we briefly analyse what the distributed ledger system is, and how it is operated. Followed by the introduction of the miners, who they are, and what is their responsibility. Then it moves on to the process of how each block gets created, then how they eventually create a chain, which we call Blockchain.

In the last chapters, we'll go into more detail of what security measurements we have in place on the Blockchain. Next, we will focus on the understanding of the reason why this technology will change the world, by looking at business purposes, and banking systems of the future. Finishing with a quick overview of what the Blockchain is in a nutshell.

There are plenty of books on this subject in the market, thanks again for choosing this one! Every effort was made to ensure the book is riddled with as much useful information as possible. Please enjoy!

Chapter 1 – Blockchain in a nutshell

Before I begin to explain to you what Blockchain is, first, I would like to touch on Bitcoin, as there is a myth going around that Bitcoin equals Blockchain. Well, that is incorrect. However, it is often referred to as the same thing. Bitcoin is cryptocurrency, digitized money, that is allowed and kept alive due to the technology called Blockchain.

When Blockchain technology began to exist, the first application that was tested on the platform was Bitcoin. Because Bitcoin was the first application on the Blockchain technology, one might say that Bitcoin is Blockchain, and that could make sense. However, Blockchain is *not* Bitcoin. I hope that makes sense. Blockchain is so complex that, still, there are very few human beings who understand each part of it. In fact, Blockchain is so complicated that we (humans) keep on finding more and more ideas that this technology can solve every day.

We could say that Blockchain is solving problems. However, for some large Financial Organizations, it's causing certain issues. Some of these matters, of course, are getting addressed and if you keep up with the news, you realize that more and more companies are beginning to use Blockchain Technology for many purposes.

The Blockchain is truly revolutionary, as it's not for solving just one issue for some people, but can fix many problems for everyone. It has re-invented the financial institution, and the proof of that is simply because Blockchain is running and has existed for nine years already, beginning in 2008. The blockchain is a globally distributed database that is completely decentralized, meaning it has no boss, or someone that we could blame or award. It is running on all computers, and it's unstoppable. The Blockchain is built up from multiple blocks that are un-replaceable. Therefore, it's chain system represents the single source of truth. Once there is a new block created and added to the existing blockchain, it replicates itself on its system, which resides on the internet, then just synchronizes the same details on all the computers that are running blockchain. This replication is what makes it un-replaceable. Therefore, it provides full transparency in all administration. Because there is no human intervention in the process of adding and further expanding when new blocks are created every 10 minutes, it exhibits an efficiency that no person has ever achieved. Because each time a new block becomes visible on all computers in the world, it allows full accessibility to all human beings.

Where blockchain stands right now, I mean in 2017, is more like where the internet was in 1992-1993. What happened back then is most people said, "it's nonsense," or "what's the point of it?" Granted, at the early age of the internet, there were only a few personal computers, very few websites, and the network was slow. In fact, it was so slow that if you wanted to download a one-page PDF document, you would probably go out for lunch, come back and you still had to wait another 30 minutes. The internet (Interconnected networks) seemed like a dumb idea to most people, even for those that had power in politics or others that already had existing large retail infrastructure. They believed that it was just background noise. Slowly, the internet grew and became bigger and faster. And once local support opened on the internet, everything changed. When you think about Blockchain, don't assume that it will not have the same power. Currently, we are innovating in large scale and technology grows with such a high speed that no human can keep up with it. Blockchain will change that dramatically, so instead of continuing to talk about the future, let's take a step back and understand the history of finance.

Chapter 2 – The history of finance

The purpose of this section is to understand the innovation of our existence. Therefore, let's take a step back a few hundred years.
Trading has always been present in our lives, as it is mandatory for our food chain, and probably will never go away. When you take a closer look at the basic human needs for survival, you quickly realize that the three most important requirements are: • Air

- Water
- Food

Because air and water can be found in many locations for free, I will take an example of food and start to analyse it in further detail.

Food items have been identified since the early ages as one of the primary human needs for survival. Therefore, we have understood that food has tremendous value. Like anything else that has value, it became part of the global trading chain, and it was one of the first early paying methods amongst humans in exchange for particular goods or services provided. Because food has always helped for basic survival, it was one of the best paying methods for an extended period. In fact, there are many locations existing in the world that still use this approach at present. As civilization has moved on, especially with more developed villages and cities, methods of payments have begun to change. Back then we had no freezers, or fridges, and using payments such as food items like

exotic fruits or any meat just went to waste. This caused lots of issues. Therefore, this problem had to be resolved. The solution was a new type of payment method, something that wouldn't easily rot or waste. However, had to be exchangeable for food or any other goods or services.

Precious metal

Shiny metals were introduced to the world as a new payment method, and such were silver or gold.

Of course, most people didn't like the idea at first. Still, it was implemented, and slowly it was excepted widely. It was exchangeable for food items, and other goods or services and it was truly revolutionary, and still today, when you look at the silver or gold value, they are continuously increasing. Humans have realized that it is getting much harder to mine gold and silver. Therefore, precious metal had to be discontinued as the major payment currency.

Paper money

The introduction of paper money seemed ridiculous, since as humans, we are uncomfortable with change and we are hesitant to adapt to anything that we don't understand–at least at first. After a while, all sorts of paper money was implemented in a centralized form, nearly every country in the world. The new payment method of paper money was alive and booming all over the globe. I mean paper money is OK, but we could mention countless countries where paper money has failed again and again due to its value decrease in long term. The

reduction in value of paper money has other roots too, such as easily counterfeited in large scale. Additionally, like anything else in the world, we have learned that goods with limited supply have an increase in value, especially in the long term. However, the opposite happens when paper money keeps on getting printed, decreasing in value. When it comes to paper money, it's a fascinating topic.

The fact that we have learned, on various occasions, that paper money is a failure, we keep on re-inventing new ones. We believe, this time, it will be a success. Look at the example of the euro that has taken over currencies such as:

- German Mark
- Austrian Schilling
- Italian Lira
- Spanish peseta
- Slovak koruna
- Maltese lira
- Dutch guilder
- Finnish markka
- French franc
- Greek drachma and much more (as well much more to come).

It appears paper money is still going to be present for a while. However, before jumping ahead, we had another currency introduced after the paper form in our new digital world called SWIFT.

SWIFT
Society for Worldwide Interbank Financial Telecommunication It began in 1973, and this newly created network now enabled all the financial institutions to transfer secured financial transactions in a reliable environment across the globe.

This idea was, again, truly revolutionary. Using the internet to make payments is very helpful, not to mention, that nowadays using contactless cards is just super comfortable. The speed of implementation, when making payments, becomes very fast. When you are looking at an international bank transaction it might take 3-5 days, but you can do this using your laptop at your home or your mobile device, anywhere. However, at first–when it was introduced–it seemed alien and most people didn't believe that it would ever work. Slowly, we have learned that certain payments can be automated: such as paying your bills or a service that you have subscribed, and of course, most large companies are now paying all their employees through bank transfers. Well, there are still many companies who pay their employees cash in hand, as they don't wish to pay taxes. These companies choose to remain anonymous instead of sharing with the banks all their assets, for various reasons. As always, people had to adapt. The idea that all your wealth is contained on a piece of plastic card was daunting.

The world of payment has yet changed again. Centralized banks have scaled, and they have introduced many different systems that one may choose. Some of the most known of virtual payment methods are: • Visa Debit

- Credit Card
- Debit Card
- ATM machines

Due to the dot-com boom and the revolution of the internet, other digital payment methods were introduced by various third-party companies, providing additional secure transactions for a particular fee in exchange.

Although higher priced, we have now reached the point of enabling international operations with people or companies that we never have to talk to or see. Even if we were to have a problem trusting a business or particular goods; we could still proceed to make transactions, due to the third party that guarantees the payment will be only completed once goods have arrived as described. For example, you make a payment for an individual product using PayPal, simply because you know that, worst case, you can ask for a refund and PayPal will help you out—making sure that you get your refund if the goods or services are not as described when you placed an order.

Such well known centralized financial systems are: • PayPal
- Payoneer
- Alipay
- eCash
- M-Pesa and much more Digital currency

In 2008 there was a new currency introduced, but this time it was something very different. It was the first digital currency, called Bitcoin. It was not introduced by a well-known company or bank, neither any government, but in a software form—running on the protocol called Blockchain.

As always, not many people were interested in adopting it at first; they didn't understand its purpose. It might require a bit of research to understand. We know that cash works and that many other currencies exist. We can make payments using our bank cards, and so many other options, when it comes to making a payment—so why bother, right? Well, Bitcoin was the first digital currency that was introduced. However, as of June, 2017, there are more than 730 different types of digital currencies that exist. What does it mean to us now? I have friends that don't work in the IT Industry, and when I asked them about Bitcoin or cryptocurrencies, they frequently look at me like I'm speaking alien.

The reality is, that although some might have heard of cryptocurrencies, they still never bother to investigate the potentials—and how much it can, and will,

form our future.

What I am trying to tell you is that when looking back in time and analysing the history of financial institutions, you may realize that the form of payments has significantly decreased from their physical value. They not only become smaller, lighter, or thinner, but more virtualized, and now to the point where we, people, don’t even have to make them—as the digital currencies are running on our current internet (interconnected networks).

Chapter 3 – Bitcoin basics

It is the first known digital currency that is running on a technology called blockchain. It is entirely decentralized. Therefore, no one has control over it. It also is known as electronic money or digital currency. However, it is a peer-peer payment system. Therefore, it's software. It has no real presence whatsoever, as it's growing on your computer's hard drive. In fact, on every computer that exists in the world.

This currency will never be touched by anyone as it only exists in a digital form. Regards to its value, it does seem to fluctuate. However, it has kept itself steady for a long period: moreover, continuously increasing. Back in 2008, it began to compete with the dollar—when one bitcoin was equal to 0.05 dollars. However, in June 2017, one bitcoin has reached $2,912.00; its highest value as of yet. Over the years, bitcoin not only proved that it could reach its highest over and over again, but it has increased its value higher than what we have ever experienced with any other currency on Mother Earth.

As of June 2017, looking at the currency exchange, bitcoin against the dollar for the last ten years, I can tell that it will keep on growing.

My personal opinion is that we will keep on seeing bitcoins increase in value, especially around each four year mark. Why would I say that? Well, let's just say that I have my reasons.

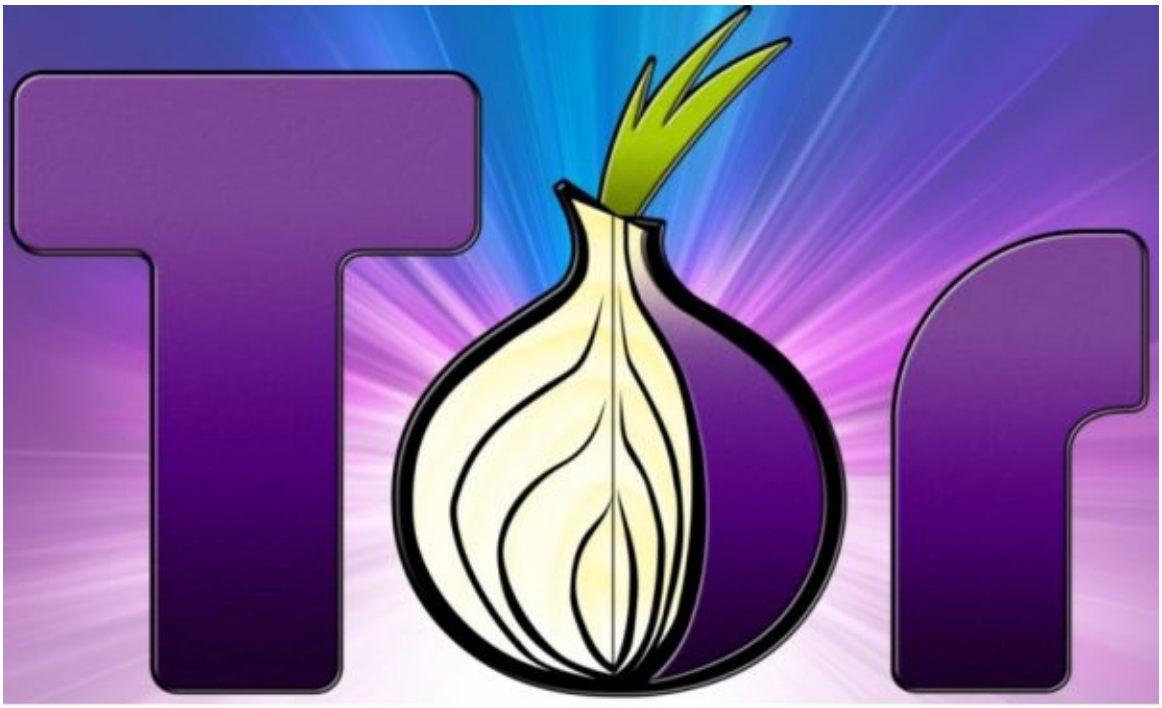
How many bitcoins are out there?

Good question, and you can calculate it yourself. Of course, it all depends on the date and time you're reading this book.

So, let's look at some of the facts that we know for sure before beginning any complex calculations. The first 50 bitcoins were created on the 31st of October 2008. Then, 50 more bitcoins were created every 10 minutes until 2012. After 2012, the amount of bitcoin production reduced to half—meaning every 10 minutes, 25 new bitcoins were created until 2016. Since 2016, the process has followed the same principles—meaning, every 10 minutes, 12.5 bitcoins will be created until 2020. This process will keep on going until 2140, until there will be 21 million bitcoins on the market.

Bad reputation

In case you haven't heard of the Dark Web, let me explain a little about it. I could dedicate a whole book for the Dark Web, and I might in the future. I am not interested in trading drugs or guns online. However, just because that is a list of things that can be purchased on the Dark Web, does not mean I will ever be participating in those markets.



What you must understand, is that the Internet as we know it—through search engines like google, yahoo, or bing—isn't the only web out there. There is another, and It's known as the dark net; it can be reached through another search engine called TOR. TOR network is also known as an onion router or onion network. TOR is capable of hiding the IP Address of the end user; therefore, making whatever is done on the internet completely untraceable.

Even your internet service provider wouldn't know what website you visited, except that you have visited the TOR network. You might look around and see for yourself, what kind of services are offered there, but it's up to you. I have visited the dark web before to get a feel for it, and the more you look around, the more you will find ugly services. And I am sorry to mention these, but the things I have seen are disgusting, and for those who can be easily upset, I would not recommend it at all. My point is, that the guns and drugs traders on Tor ask for payment in the form of Bitcoin. Bitcoin is untraceable, as well as the TOR network. Therefore, the Dark Web is a haven for criminals.

Do criminals use Bitcoin too? They sure do. In fact, they have no other choice when it comes to illegal goods or services online. Before you close this book and walk away from the idea of using bitcoin because criminals are using it too, please think twice. Bitcoin wasn't created for criminals. Bitcoin was designed for everyone, and please don't forget about those 3 billion people that bitcoin can save when it comes to financing.

Another issue that happens over and over, is bitcoin accounts get hacked, and people are left with empty wallets. Please don't misunderstand this point. It's not the bitcoin that is hacked, but the end-user level victim's Computers, or mobile devices. The value of bitcoin has become enormous; and hackers do educate themselves too. Therefore, they have changed their game once again, and realized that hacking Bitcoin accounts is profitable and untraceable; so, why not do it—especially do it on a grand scale? This issue has been addressed, and if you decide to own a wallet, you must make sure that you always back up your wallet, as well, always have all the security features enabled. Some of these security features are like 2-step authentications that don't require much learning or time, still, better to be secured then assuming that hackers will never find you. So, because many people have fallen victim to bitcoin account hacks, they have stopped trading or investing in bitcoin or any digital cryptocurrency.

Wikileaks

You might be familiar with the website WikiLeaks—a non-profit organization responsible for publishing secrets and classified information anonymously. Of course, individual governments are not happy with the website and they have issued the site to be shut down. The site requires basic maintenance, as well as security, and the only contributors able to help have had to use bitcoin. As a result, the website has stayed alive to this day. This is one of the most famous examples. However, there are countless causes that people have been able to provide help to others, even to the other side of the planet, using bitcoin.

Rumor about decrease in value The most common speculations and accusations against bitcoin are its possible fluctuation. Why is that? Well, people often say, “What if there is another type of cryptocurrency that could compete with bitcoin using the same underlying technology, the Blockchain? Would bitcoin lose its value?” The accusations are indeed possible, but looking at the history of bitcoin value, only significant increases happened, even with 734 other cryptocurrencies . I am not a futurist, but after analysing the facts, I think it’s fair to say, that the bitcoin is on the rise, and will not stop for a long time.

What can you buy?
Well, you can buy anything on the dark web—of course—I do not recommend that, as you might come across criminals who would try to steal or hack into your bitcoin wallet. Some cyber criminals would even try to blackmail you. However, if you do not provide your details, you should be just fine. Realistically, more services are excepting bitcoin, such as Hotels, Restaurants, Coffee shops, even some takeaway shops are now offering payment method using bitcoin.

Large retail companies are also accepting bitcoin, such as Shopify, TigerDirect, and many more. To see how wide range it can be already, you have to look around where you live. The big cities have all sort of offerings, such as: • Theatre

- Taxi Service
- Bicycle rent
- Private Jets
- Pubs

Also, you may consider other large companies that are now accepting Bitcoin, such as: • Dell

- Microsoft
- Zynga
- Reddit
- Wordpress.com
- Subway
- Expedia.com
- Virgin Galactic
- OK Cupid
- Stream
- Alza
- Lionsgate Films
- Badoo… and many more

By using Gift cards, multiple applications also allow customers to purchase on websites, such as: • Amazon.com

- Walmart
- Target
- Nike
- GAP
- BEBE
- Sears
- Papa Johns
- Best Buy
- iTunes
- eBay
- Starbucks
- Zappos
- CVS Pharmacy
- The HOME depot… and much more.

I wanted you to see that some of the largest companies are already adapting to the idea of accepting bitcoin. Moreover, to understand the range of goods and services that can be purchased, please see the list of categories that you may

choose from: Airline
Automotive
Beauty
Clothing
Department Stores
e-Commerce
Electronics
Gas
Gifts and Toys
Grocery
Health
Home and Garden
Home improvement
Hotel
Jewelry
Movies
Pets
Restaurants
Shoes
Sporting goods

As you see, the categories keep on growing, and if you are more interested in what stores you can pay using bitcoin, you might check what you have nearby you, or what online platforms can deliver to your area.

Why is not everyone using Bitcoin?
Well, the reality is that most people who are already aware of the existence of bitcoin, are too lazy to do some research for better understanding of the potentials.
Personally, I first heard about bitcoin in 2013, and I didn't look at it that much. What I understood, was that bitcoin was some form of online payment method, and mostly criminals were using it because it's untraceable. That's it. I keep up with the news, and somehow, no one seems to talk about it unless there is a significant Cyberattack, and the hackers would demand ransom, or some payment, in the form of bitcoin.

Anyhow, at the end of 2015, I heard about bitcoin again when I was studying about Network Security, so I mentioned it to my friend Rob. He said that, yes, he

was aware of bitcoin, and it’s worth was like $300. When Rob said it, I couldn’t believe that one bitcoin was worth $300! Of course, I still didn’t understand what bitcoin was. I thought that it was like a real physical coin, I still had no clue that it only exists in a digital form. Then another friend Viktor, who overheard what we were talking about, said that he couldn't believe that I had never heard of bitcoin before! So, I said, “Yes, I did hear about it, but I didn’t know that it’s worth so much.” I started thinking more and more about it, and I began to do some research. A little later, I had an idea to make bitcoin using my old laptop! So, I told Viktor and Rob that I heard that computers could generate bitcoin, and if it’s worth like $300 each, I might be able to produce one or 2 every week. Obviously, I had no clue what I was talking about, and they told me off that it’s not that easy. However, they couldn’t explain it to me, how it’s exactly done. They said that I was thinking like a hacker, and I shouldn’t be like that, as it’s for criminals. But I stated that it sounds like an exciting technology. They replied, “OK, so why do you need bitcoin? What do you want to buy? Do you want to buy something on the dark web?” They made me speechless, so I didn’t say anything anymore. However, I secretly begin to learn as much as possible about bitcoin and of course that lead me to another interesting technology called Blockchain.

My point is, that most people have been misled by fake news, and for those that might be interested, it takes a long time to understand how bitcoin or blockchain works. Therefore, most people give up research, and will not get involved in any way.

Chapter 4 – The trigger

Some of you may remember, back in the day, when everything was going just fine until Lehman Brothers collapsed. It was the 15th of September 2008, when the largest bankruptcy that has ever happened in US history occurred. Of course, Lehman Brothers was operating in other countries too, and the outcome of that day was no different anywhere else.

I am from London, UK, and happened to be working at Canary Wharf at the time. In fact, those days I was working as an Assistant Manager in a restaurant called Nando's. What happened was that people were coming to our restaurant in groups, holding boxes containing their belongings from the office. They told us that it was the last time they'd be eating there. Because we had been working super hard and isolated from the news, we didn't understand at first what these customers were talking about.

We quickly looked up the news at Canary Wharf and realized that Lehman Brothers UK had gone into administration (bankruptcy) less than 45 minutes ago. We then understood and realized that these people who used to have lunch

in our restaurant, would now not be able to come around anymore. That morning, 2,000 people lost their jobs. And the next day, on the 16th of September, another 2,500 more followed. We agreed as a management team to provide free soft drinks for those who just lost their jobs, to show our sympathy. Of course, we lost all those customers too and many more. Anyway, I just wanted to share my experience that I encountered right at the beginning of the recession in 2008. Following the Lehman Brothers, there were many more Banks and Financial Institutions that had no choice but to choose administration. For months, every news channel was full of the latest stories that another large company had lost all its assets, again and again. At the same time, unemployment began to rise, then slowly, lots of people started losing their homes due to uncompleted payments.

Most of the small businesses had to shut down. There were fewer customers in the restaurant, and people were thinking twice before spending money on anything. The financial crash caused plenty of misery, and not only in the US or the UK, but many other countries too, that are still in a state of recession ever since. Property prices began to drop, and finding a new job wasn't easy, even overqualified people were applying for jobs everywhere. However, there were not enough job vacancies to fill the increasing demand.

I, like most people, was following the news—that most of the time is manipulated and it's only purpose it to create drama and fear amongst hard working people… I am doing my best not to hurt any company's image, but controlling the media is an excellent way to manipulate people, their beliefs, and freedom. Using media—such as news channels and newspapers—to reach people, is indeed one of the best ways create slaves, by making them believe that the world is exactly what the media is providing. Just think about an average day when you meet like 5-10 people. Someone, if not many of them, will tell you a story that starts like this, "Did you hear Bla Bla Bla…"

Of course, next, someone else will ask, "Where did you hear that?" The answer will be similar to something like this, "I heard it on XYZ news channel, or in the news, or read it in the XYZ newspaper." Everything is such big news for days, sometimes weeks, then suddenly—all is forgotten. How come?

Funny enough, around the same time, in an unfrequented online forum, a paper was posted to a cryptography mailing list on metzdown.com, titled as: Bitcoin.
The subtitle was: A Peer-to-peer Electronic Cash System.

So, what's that? It's not from the CNN, or BBC, NBC, CNBC, or whatever you name it news channel. Therefore, it must be nonsense, right? Yeah, it's most likely fake news, and whatever it is, it seems too complicated. Therefore, it didn't pique anyone's interest. This white paper was published in October 2008, less than two months after the biggest financial crash in history. The author named himself Satoshi Nakamoto and explained a couple of points related to this new digital currency called Bitcoin. He stated, that he believed he had found the solution for the biggest issue that we face, a technology that is called blockchain. Also, he explained not only how it works, but that this system has already been created and is running in a software form using the current internet as it's platform.

There are many speculations about this, and you might find multiple answers about what exactly happened; the most important among those are—why now? How come such a serious document was published just after the largest financial crash in history? Well, we might find out someday soon, but the possibility remains that we may never know what triggered the Blockchain technology to be born.

Chapter 5 – The Inventor

First, I would like you to understand that this book has been written in the second quarter of 2017. Therefore, by the time you are reading this book, it's possible that new light might be shed on who Satoshi Nakamoto is.
With the current knowledge at hand, let's try to understand who Satoshi Nakamoto is.

First of all, Satoshi Nakamoto is an inventor of bitcoin, as well the blockchain technology. All through it's a false name, this is how he introduced himself to the internet. It is a men's name. However, it is possible the Satoshi Nakamoto might be a woman. This is one of the biggest mysteries in the technology world. Yet, most people don't want to know exactly who Satoshi is; nevertheless, they are thankful for the technology he created.

Unfortunately, many people think that because Satoshi Nakamoto has invented Bitcoin and the blockchain technology, he is also the owner of those too. The reality is that Satoshi Nakamoto has no control over the Blockchain—neither bitcoin; therefore, it really doesn't matter who Satoshi Nakamoto is.

But yeah, we still want to know who is behind the curtains; so, let's think about it again. Satoshi Nakamoto is reasonably a man or a woman—of course—he could be a couple, a group of people, or even a group of women for all we know. Satoshi Nakamoto might be ten people together, but also could be a massive team of 100 individuals. Satoshi Nakamoto might be a child, or he could be old men. Satoshi Nakamoto might have died right after he released his white paper; therefore, he had no time to show his real face.

I do understand if you are getting bored of these accusations, so let's begin thinking in a different perspective. Satoshi Nakamoto might not even be human. Well, you might think of me being over the limit. However, it's just so odd that we couldn't figure out who Satoshi Nakamoto is in the past decade; not where he resided, but who he is—honestly—we have no idea. Someone might know exactly who he is. However, there is no confirmation that would ever have enough evidence to prove who Satoshi is.

I've always loved to watch sci-fi movies, and I came across one called Arrival. Some of these super old movies, still hold up today. For example, back in the day, some sci-fi stories featured individual objects, or tools that we might use in the future, and some that we've already been using for years. I don't want to get into too many specifics; however, think about facetime talk back in the 80's. It was a concept that one day we might be able to do that. And nowadays Skype and Facebook Video Chat is in our daily lives. In fact, there are millions of people connected and capable of being on skype video chat for hours, using our cell phones. The first iPhone was created and launched to the market ten years ago, in 2007. Since, we have gone through some dramatic changes, and the next decade will be even more impressive.

So back to the picture called Arrival, I hope that you have seen it already too, and that I will not spoil it for you. However, if you haven't seen it yet, you might want to skip the next few lines.

In the movie, we have received a visit from Aliens that are here to help us by providing visibility in the future. Again, sorry if you have not watched the movie yet, you will probably hate me for this. The concepts of the film are excellent, no wonder it received an Oscar, even though it might have deserved more than that, but that's just my opinion. When I think about this sci-fi movie, I am thinking about the fact that it is very similar to the same concepts. We have received a technology called Blockchain from an unknown person—or I should say from an

anonymous source—that will change our world dramatically! I wonder how the film creators came across the idea… I am not suggesting that there are Aliens out there, but I can't deny it either. What I can tell you is that IT Professionals, Software Developers, Experience Programmers, even Cybersecurity Experts are fascinated by this technology, and often refer to it as an ALIAN TECHNOLOGY."

The blockchain is huge, and it certainly takes months, if not years, to fully understand it's technical details, and how it fits together. Another thing is that, more and more often, it is said that this technology is just too complex for one man to build. Therefore, there is no way that Satoshi Nakamoto was working on it alone.

So back to the million-dollar question, "Who is Satoshi Nakamoto?"
Let's look at some of the claims over the years so that you can decide for yourself.

What you have to understand is that Satoshi Nakamoto went silent in 2009, and remained like that for the next five years, or at least on the forum where he previously posted and was always active.

Chapter 6 – I am not Satoshi

Supposedly, Satoshi Nakamoto was a 41-year-old man at the time of the publication of the Bitcoin white paper.

He is from Japan. However, the first code that was written for the blockchain was drafted in English that is so perfect, it just wouldn't make sense for a Japanese man to write like that. It would indicate that he must have hired someone, or was working with someone, who has perfect English, to write the code.

In 2014 there were a few newspapers that began to write about Dorian Nakamoto, who at the time lived in the United States in California. Dorian's birth name was Satoshi. Additionally, other circumstances would make him appear to be a real inventor of Blockchain.

Apparently, the first reporter who wanted to reach him, asked him, in the form of an e-mail, if he had anything to do with bitcoin. The response from Dorian was the following: "I am no longer involved in that, and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection.''

Of course, that was suspicious, and reporters were all over Dorian's house in California. After realizing that it was very serious, he looked at his e-mail again, and tried to explain himself.

First, he has denied any involvement in regards to bitcoin. In fact, he said that he had no clue what bitcoin is until his son told him about the news, so he looked it up on the internet. He also went public and explained the following: "I have nothing to do with bitcoin. Nothing to do with developing. I was just an engineer, doing something else. If you look at the time spent in 2001, I wasn't there. I was working for the Government through a contracting company.
I just believe that somebody just put that fictitious name in there.''

There were also published documents on that he has been doing classified work for the United States Government, as well the United States Military. He also has signed documents that he could not be allowed to admit any involvement in his previous works regards to secret projects.
After this event, there was an unexpected message on a P2P forum where the Real Satoshi Nakamoto use to post after five years of silence.
"I am not Dorian Nakamoto.''

Chapter 7 – I am Satoshi

Craig Wright, who is a well-known Australian Businessman, in 2015 became a next possible man who just might be the real Satoshi Nakamoto.
From an anonymous source, documents had begun to leak about Craig Wright to Wired magazine. Most of them had some evidence that seemed as if Craig Wright might be Satoshi himself.

One of them, released back in August 2008, Craig himself has stated that he is thinking about releasing a Cryptocurrency paper. This, of course, become a very attractive candidate for the original white paper that was published by Satoshi Nakamoto and was released in October 2008, just a month after.
Another leak, that was also issued by Wired magazine, was another statement by Craig Wright, but this one as dated back to January 2009. This time he wrote that the bitcoin is about to launch. Indeed, it was January 2009 when the first bitcoin began to operate.
Additionally, Wired magazine also stated that they had received several e-mails and transcripts that collaborate the link.

“There is a leaked message from Wright to his lawyer dated June 2008 in which Wright imagines a P2P distributed ledger.’’

There were many leaks in regard to Craig Wright, especially in the Wired magazine. However, it all changed in May 2016. Craig Wright has stated on his blog that he is now willing to admit publicly that he is Satoshi Nakamoto.

This was another turning point; however, people have remained sceptical. Two days later Craig wrote on his blog that finally, he would release a series of pieces that will lay the foundation for his extraordinary claim. Although, instead of providing evidence, Craig has replaced that post with the following:

“I am Sorry I believed that I could do this. I felt that I could put the years of anonymity and hide behind me. But the events of this week unfolded, and I prepared to publish the proof of access to the earliest keys, I broke. I do not have courage. I cannot.

When the rumors began, my qualifications and character were attacked. When those allegations were proven false, new claims have already started.

I know that this weakness will cause considerable damage to those that have supported me, and particularly Jon Matonis, and Gavin Andersen. I can only hope that their honor and credibility is not irreparably tainted by my actions. They were not deceived, but I know that the world will never believe that now. I can only say I’m sorry.
And goodbye.’’

Because Craig has not provided any evidence that he is the real Satoshi, the bitcoin community has painted him as a liar.
Next, was another fantastic action from Craig. He asked the BBC for an interview.
He then explained that he is Satoshi Nakamoto, and he invented bitcoin. Craig also stated that he would not accept any prize or award for this creation, as he is not interested in money or anything from anyone, and certainly doesn’t require any help from anyone.

When the reporter questioned him why he was hiding for all those years and how come he has identified himself just now, he had a relatively simple answer. Craig said that he didn’t decide to confront the cameras, as he has people who chose this for him, which, he is not happy at the current present, as this situation will hurt many of his friends and family, as well as his staff members.

Next, the reporter asked him what he wanted with the concept of being the creator of Bitcoin, but his answer was that he doesn’t want anything, just to carry on working on his projects. Craig explained that because he has created bitcoin, or published a document for free publicly, so that he can help people, it does not

mean that he should become a well-known star, and certainly no one should force him to admit what projects he is working on. Then he added that he was the main person behind the creation of Bitcoin. But, he had help finalizing it.

Next, the reporter pointed out something that most people are interested about. As the inventor of bitcoin, Craig must have that 5% of all bitcoin that was saved, and that is a huge amount of money. As anytime when traders are selling bitcoin for the dollar, the value of the bitcoin drops. However, as the inventor has so much of it, there is a fear that if the designer would sell all that when the price is high, the bitcoin would probably fluctuate.
So next, the reporter asked him how much bitcoin does he have, and how much has he deployed so far. Craig only answered that it doesn't matter how much he has, instead what matters is when will he actually deploy them.
Then Craig finished his speech by explaining that he knows that some people will believe him, and some will not, but he does not care, because he will never be in front of the camera.

The reality is that Craig is very convincing and, personally, I don't know what to say. I won't[A1] judge him or Dorian, but the world we live in is certainly strange for sure. Just think about it. First, we expect someone who claims no involvement whatsoever, then we find a man who admits that he is him, and we don't believe him. It sounds like we are never going to find out who the real Satoshi is, right?

Craig has demonstrated how he started the first bitcoin transaction. However, he only allowed one person to see it, and that was a reporter who has no technical knowledge. Average tech gurus are not convinced. Also, Craig has claimed that he never wanted to come out and be in front of the cameras. Still, now that he did it—claimed that he is the real Satoshi—he tops it off with providing evidence that he made the first bitcoin transaction and has options on how he should demonstrate that proof. One right way to do it, is to have someone like a bitcoin expert see it, who could also verify that he is not lying. His way is a bit fake, as no one can confirm 100% that he is really who he claims he is.

So, what's the point? Well, some people have been speculating that if Craig claimed the title of Satoshi, the real Satoshi would be sending a message in some form so he could be tracked down. However, there has been no news ever since from the real Satoshi, like in the case of Dorian.
When you think about it, if you were, secretly, one of the wealthiest men on

earth, would you go to the BBC and tell this to the World? Speaking to the World does not just entail being popular in front of average people, it puts Craig at risk, right away, of being targeted by Cybercriminals and Black hat hackers. It's so simple that anyone would understand it immediately. So, when you're thinking about someone who is genius enough to implement a technology that will change, in fact already changing the world, wouldn't you think about Hackers?

As I mentioned, most IT Professionals just aren't convinced enough; therefore, the question remains about who the Real Satoshi Nakamoto is.

Chapter 8 – Satoshi is Hungarian?

Some people believe the genius behind the blockchain technology is Craig; some believe it's Dorian. However, most people from the bitcoin community don't think that any of them has anything to do with bitcoin or blockchain. In fact, 70-80% of people believe various other possibilities, so let me explain some of them for you.

Nick Szabo
According to certain researchers, one of the biggest theories is that Nick Szabo may have written the bitcoin white paper. When they compared more than ten possible people who might have anything to do with bitcoin's creation, Szabo's published writings were the closest, linguistically, to the original white paper that was published by Satoshi Nakamoto.

Nick Szabo is a computer scientist; in addition, he is also an excellent cryptographer and well-known Bitcoin expert. Additionally, he is famous for his speeches in regard to Blockchain technology, digital currencies, and smart contracts.

Many people have interests in any of these topics. Especially, well known

speakers about Blockchain or bitcoin. However, not many people are aware of what some of these so-called experts did before the birth of Bitcoin. On the other hand, Nick Szabo had an idea about a decentralized digital currency back in 1998 that he called "Bit *Gold*." What a coincidence, right? Nick didn't only have the idea, but he also developed a mechanism for, and eventually created, the Bit Gold. Nick did not post on his blogs every day. In fact, he wasn't known to publish anything: however, when bitcoin was created, back in 2008—just two months after the official release of bitcoin—Nick began to write about Bit Gold in more depth. There actually isn't much known about him, an excellent example is that Nick's date of birth has not even been confirmed by anyone so far, and because of this, other curious people have begun to investigate Nick even further.

According to Wikipedia, Nick was a law professor at George Washington University; however, after contacting the University, they found no record of anyone with the name Nick Szabo. This, again, has suggested that his real name might not even be Nick Szabo, as it just might be his pen name.

There is very little known of Nick as there is no verifiable age, education, location, or even former work profession; therefore, within the technology world, he has become the number one candidate for the birth father of bitcoin.

Apparently, anytime he has been asked if he had anything to do with Bitcoin, he has always denied it, and for a while now, once again, he has gone silent. Unfortunately, when it comes to the media, there is so much fake made up news that it's just unbelievable. At the beginning of the 21st century, the internet was the only actual source of news; however now that most newspapers have moved online, it takes an enormous amount of time to research the true. That's being said, most of those who were always trying to find the truth, indeed, don't read newspapers and fake news channels, and I am talking about IT Professionals that only study about technology. Even though when a technological invention, such as blockchain, comes into the news, these nerds become obsessed to find out who exactly is such a great designer, and they begin to do their research until finding the truth. So far as it seems, most tech gurus are pointing to Nick Szabo as a real creator of bitcoin.

As I mentioned before, when it comes to possible candidates of the father of Blockchain technology, there are many assumptions. It all depends on who you ask; however, I wanted to introduce some of the main characters who might have

some involvement in bitcoin creation.

Teamwork

Many people believe that blockchain, due to its complexity, might have involved many characters, instead of only one certain individual. When Craig has been asked, he said that he had help. However, he was the main person behind it all. Therefore, many have begun to believe not Craig, but that Satoshi Nakamoto could be representing a group of individuals instead of man's name.

In Japanese, Satoshi means clear thinking or wise, Naka means inside, and Moto says Foundation. These three words can be put together in many ways. However, one of the most common would be that he, or the team, is announcing something like: I am wise, and I fully understand this system from inside out. You may replace the I with we. However, Blockchain was certainly not a product of a mistake. The creation of this technology indeed required clear thinking and must be able to understand fully every single detail of it, and lastly, Blockchain is a large foundation.

Of course, the opposite thinkers are confident to say that due to the Blockchain's structure, the idea must have been born in a single mind. Therefore, having a team thinking together, creating something similar, would not be as detailed as it is. I am talking about people that are not average techies, but software developers, and were part of building the internet since the early ages. Again, Nick Szabo comes to mind, instead of an Australian business magnet, neither an old Japanese man who was not involved in anything for an extended period.

I will now close this chapter, and let your imagination decide who Satoshi Nakamoto is. Still, as I mentioned before, it may all depend on the date of reading this book; but for now, nearly a decade after the Invention of Blockchain technology, we still have no evidence to prove 100% who Satoshi is.

Chapter 9 – Distributed ledger system

This book is a beginner's guide. Therefore, I will do my best to explain what the ledger system is with the least technical terms as possible.

First, I would advise you to think of the ledger system as a family tree; but, instead of people's names, the huge ledger system holds information about payment value and addresses. In regards to the amount values, the ledger holds all the records of payments back to the first transaction that was ever made. In regard to the addresses, there are no URL's or location addresses. Instead, these are bitcoin, or any other cryptocurrency, addresses. The ledger holds a series of transactions of all cryptocurrencies.

Additionally, the current values are continually computed of the previous transfers. One part of the ledger is representing the value that has been assigned, some other parts of the ledger represent the date and time of each transaction. This is very similar to any of the current Banking systems.

You can see who transferred to what account, what date and time, as well how much was each transaction; however, the ledger has no banker. Also, the addresses are not representing names of the individuals, neither who holds what

amount; therefore, you can call this an anonymous ledger system. What you have to understand is that when it comes to an individual's bank account who has no relatives, the bank could seize that account. In addition to banks, even the Police, FBI, or any government official can take any bank account if they find a possible reason for it. When it comes to a bitcoin account within the great ledger, the only person who can access it is the person who has the password to that account.

Of course, it's dangerous; if you accidentally lose the password to your bitcoin wallet that the ledger holds, whatever value it has will be lost forever. With your bank account, if you lose your password, you call the bank, they ask security questions, and once you prove that you are the owner of that account, the bank will provide you access. On the other hand, having a bitcoin account, no bank will be able to help you to access your account. The ledger is visible to anyone, as it's completely de-centralized. Therefore, everyone can see your bitcoin account, as well how much value that wallet has. However, no one can tell that account is connected to you.

Due to the blockchain technology, every transaction is confirmed for its validity and goes into a block; then each block will join to the previously validated blocks, then eventually they all will form a chain of blocks, that we call blockchain. Every bitcoin citizen is required to keep a copy of the blockchain, after each block that gets created by the system, every blockchain member receives a finalized sealed block.

Then the system checks each block automatically and adds each block to each citizen. This is how blockchain holds every transaction and every value that was ever created. These methods ensure the legitimacy and correction of every transaction without any central authority. If all that sounds alien to you, just understand that is completely automated by the system, and you, as a bitcoin citizen, do not need to do any calculation, and it would probably take a very long time anyways.

Each transaction, once validated, is sealed into the ledger; this process is carried out by the miners. When a new validated block arrives, each new block must be added to every citizen's blockchain; however, before accepting the new block, everyone checks the logical continuation of all the values in the new block, to make sure that all the transfers of costs are legitimate. This also prevents any replication of transfers or any counterfeiting done by hackers, or people with bad

intentions, trying to steal bitcoin or any other cryptocurrency. This is a crucial step, as this validation will remain within the great ledger and within the blockchain forever. This process uses hashes for competition, to validate each block, and make sure that each citizen receives the same record.

Hopefully, I didn’t confuse you by adding some extra bits on how the ledger becomes distributed and what process it uses for the purpose of validating each transaction. The reality is, that technically multiple protocols are working together to achieve each validation process. Also, you have to understand that thousands of the operations are made in each of every second. Consequently, I have avoided the technicality as much as I possibly could.

Chapter 10 – Miners

Let's first think about how new value enters the system. Back in 2008, Satoshi Nakamoto only created 50,000 bitcoins to start the process. If you think about it, had he built all 21 million in the first place, the bitcoin would be worthless, and the idea would have been dumb. Instead, Satoshi started with a moderate amount of bitcoin creation.

Yet, as the bitcoin community grows, more and more value would be required for the system to be kept alive. There is a particular process that is needed for the system to be maintained; Satoshi has come up with the solution by creating a role. This solution is not only solving one, but two issues: 1. Permanently validating transactions 2. Adding new value into the existing system The role is called miner.

Miners can be individuals, or any bitcoin citizen. However, over time, many large companies have been formed, such as Genesis Mining, where you, as an individual, can join and rent their mining facilities. There are many other miners who over the years have created a pool, and many of them also offer to join these pools for certain reasons that I will discuss shortly.
First, let me explain why they are called miners and what it is they do. They are

called miners as the analogy has been used with gold or any other precious metal. They work together to create new value, similar to gold miners who are digging underground. However, bitcoin miners are sealing each transaction into the ledger. Therefore, we could call miners, finalizers or authenticators.

To get rewarded for such work, the miners receive bitcoins, and this is how new value is added to the system. The miners validate, authenticate, certify, and finalize the transactions by specific processes. Once the miners have created a new block that is accepted by the citizens, the record of the transaction cannot be modified, making it permanent information. This will also become irreversible. Therefore, no one can ever challenge it or change it, in the future.

The miners sealing, are sealing the blocks, which in itself can take an enormous amount of computing power, assuring that they cannot be easily replicated. There are multiple methods that each miner may use for the validating processes. Some of the miners may use different software, even creating their own in-house made software to speed up the authentication process. However, it doesn’t matter what software they use, as all of their work will be checked. It starts when a miner begins to gather transactions that have been broadcasted on the network, then starts checking those transactions, and eventually sealing those collections of transfers and operations into a new block.

A miner receives bitcoins as a reward for each sealed block that is added to the blockchain.

Chapter 11 – Block creation

Explaining each block creation can be done in multiple ways; however, some sound very confusing, but it also depends on how much you understand technology. Therefore, hearing or reading it the first time can be difficult to comprehend.

I already explained that miners have an unusual role for validating each transaction in the form of a block. Now, let's discuss what it takes to create each block.

1.
Start a new block. Even if the miners are half-way done validating a block, eventually, they will drop everything and concentrate on starting a new block.

2.
Select a new transaction. This is when the miners are choosing from thousands of operations that are broadcasted over the network.

3.

Check priority of the transaction. This time the miners can go back to number one by starting a new block if they find that the transaction they have selected previously is not that significant. However, if the priority is high, the miners may go on and move to the next step.

4.
Check that the transaction is valid. This is a process that every miner must check, there is no exception of avoiding this step for any miner. However, if the transaction is found to be faked, or not valid, the miners have to stop the process, and go back to number 1 and start a new block and get another, hopefully, valid transaction.

5.
Accept the transaction. If the previous transaction was tested as a valid transaction, it must be accepted.

6.
Seal the transaction. Again, if the transaction has been found valid and accepted, now it’s time to seal that transaction.

7.
Add the transaction to the transaction tree inside the block. This process can only be done once all previous steps have been verified.

8.
Check for the size of transactions. The miners need to check if there are enough transactions within the transaction tree, to seal the block. If there are not enough transactions yet, the miner will not be able to seal the block until there are enough transactions. Therefore, the miners must go back to number 2 of selecting a new transaction again, and again, until there are sufficient transactions for sealing the block.

9.
Check interruptions. This is the process where the miner must make sure that no other miners have sealed the block in the meantime with the same transactions inside the block.

10.
Seal the block. Once there are enough transactions for sealing the block, the

miners will seal the block.

11.
Broadcast the block. The miners must broadcast the new block that has been sealed; however, if the miners have been interrupted within the block sealing process, they might have to start a new block all over again.

12.
Start a new block. This is the next step in the process; however, as you see, we are now back to step number 1. As I mentioned, miners might get interrupted while they are sealing the block and once they broadcast it, if another block has already been sealed by another miner with the same transactions within a block, the block will not be accepted. Therefore, you must start a new block.

Each block is created about every 10 minutes. As a result, 144 blocks are created each day.
As I mentioned before, the miners who have successfully added a new block into a blockchain get rewarded a degree of bitcoin.
The reward for each new block creation used to be 50 bitcoins from 2008 until 2012. The reward for a new block gets halved every four years; therefore, from 2012, until 2016, the award for each new block used to be 25 bitcoins.
Currently, since 2016, until 2020, the reward to a miner for a new block that is added to the blockchain is 12.5 bitcoins; however from 2020, it will be only 6.25 bitcoins until 2024. This process will be continued until 2140 until the last bitcoin will be created.

Chapter 12 – Security on the blockchain

Some of you might think, “OK, fine, blockchain is a high technology that will positively change the world.” But, the question remains, “Is it secured?”
The short answer is yes. But first, let’s think about what the system has currently achieved. The reality is that anything can be hacked and compromised that is connected to the Internet, or connected to a system that has the connection to the web.

Sure, many devices do not use any connection and still can be broken into once you have physical access to it. Such might be a laptop or desktop computer that can be broken into using a Linux cd, and booted using that. If you want to go further, let’s take banks, for example. They are getting compromised all the time; of course, they have stopped announcing these types of incidents, as they would have no customers left if they would carry on doing so. The director of the FBI was hacked by a teenager in the end of 2015, and most people think it’s funny. Still, when you think about the security within the FBI, it is very well organized, yet still hackable. The FBI might not be the best example to mention, as even Kevin Mitnick hacked the FBI for three long years, and listened to the agents’ phone conversations, talking about himself. When you look at the NSA, aka The National Security Agency, you probably have heard of Edward

Snowden already, who walked out with documents that are considered to be secret; that still shows that even the NSA has weaknesses. And confidential, or even secret, documents can be leaked. All those expensive Firewalls, Intrusion Prevention Systems, or Intrusion Detection Systems are worthless if they are not upgraded correctly. Also, you have to understand that having all that security does not mean anything if someone has a social engineering skill set and figures out the password to any of those devices. The result would be dramatic, and they always are, but most of the great financial institutions have stopped talking to news channels about being compromised by hackers, as it would only damage their image, and it would become an embarrassment.

Because companies keep all their data centralized, hackers only have to go after a specific organization to compromise its systems; that is why hackers know for a fact that anything can be broken into. To hack into any system, it's only a matter of time and proper planning; however, when it comes to a system like blockchain, it is highly unlikely. Although experts say that it is not impossible, it still would require an enormous amount of computing power. Blockchain has no firewalls or any Detection or Prevention system that would protect it. Instead, blockchain's power comes from the fact that it is completely decentralized. What I mean by that is simple really. However, I will do my best to explain it in everyday English.

Because blockchain is an open source technology, anyone can run the software. You may choose not to ever buy bitcoins, or invest in any cryptocurrency. However, you might become part of the blockchain community by running a software called blockchain. The software itself is free to download and use, and you will have no obligation to anyone whatsoever, but once you decide to run it, you simply become part of the blockchain community. Once you become such member, your device will become part of the blockchain and each time a new block is created your device will also get a copy of that transaction.

As your device has now became part of the blockchain, this is another device that should be hacked to compromise the block chain thoroughly. Because your device is now running a blockchain software, it's now also contributing to the existing decentralized system. There are no centralized copies and every user is trusted in the same way as the rest of them. What I mean is that no master node exists, as every single device has the same replicated information, making it nearly impossible to hack. The blockchain is running for almost a decade, and it has never been compromised, not once. It is fascinating, as the blockchain has a

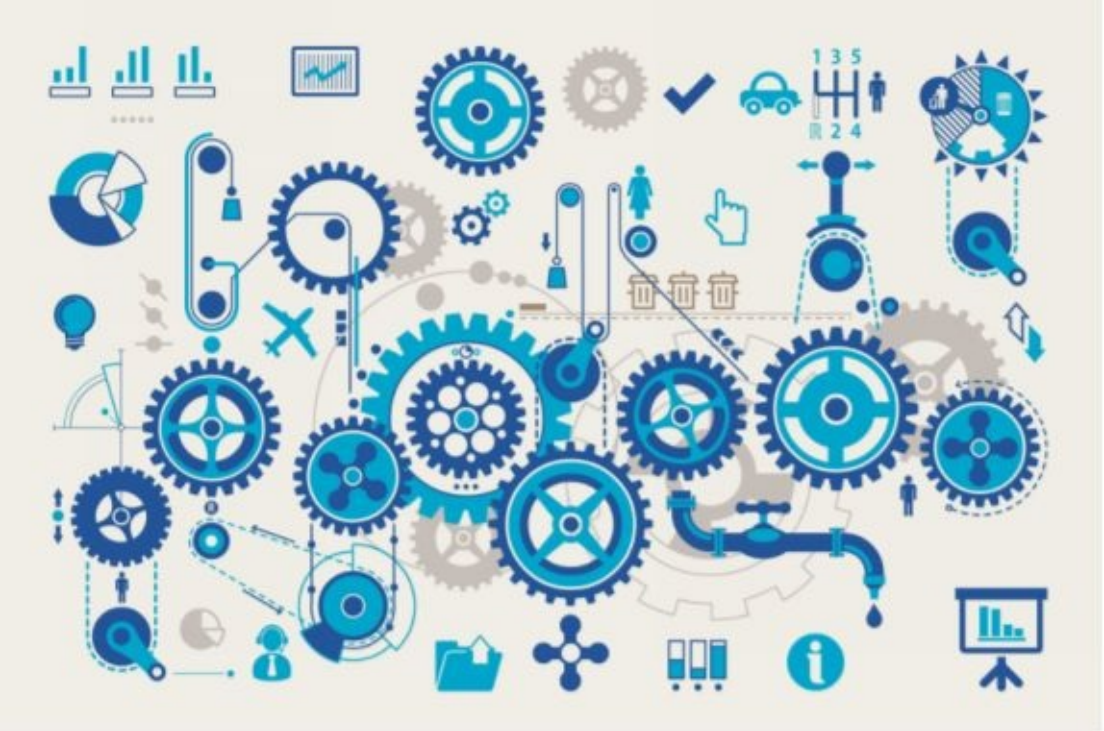
bounty of 7 Billion dollars to anyone who can compromise the system, offered anonymously. Due to the price on blockchain's head, it has become the primary target for many black hat hackers, as well as large criminal organizations, and Cybergangs, for years.

Still, blockchain has not been hacked yet, not even a slowdown of any kind has ever happened. This shows that the core functions have been structured very well; but, as I mentioned before, anything can be hacked, as it's only a matter of time. IT professionals always believe that with technology expanding rapidly, in the future, anything is possible. Quantum technology defines the way how the blockchain system can be hacked. However, it would require hacking the million-plus machines currently running the blockchain software. Additionally, to actually hack all those devices, it would need to be implemented extremely quickly to be successful.

Speculations about Satoshi himself are still in a shadow; moreover, as we don't know who he is and what he is capable of, one thing is for sure: he designed the system. Therefore, he would have access to the very first block that he created, and he would be able to manipulate the blockchain system if he wanted to. As time has passed, multiple blockchain technologies now exist, and bitcoin, itself, has grown its value; people have also begun to invest large amounts into various cryptocurrencies. Over the years, people have lost interest in who Satoshi Nakamoto really is, or he, just simply, has been forgotten; however, if he or she is alive and decides to manipulate the system, it could be possible, and not I'm sure that the outcome would favor most.

Chapter 13 – Business purposes

In technology, there are many geeks, myself included. However, some people differ from one another.
How can I define a geek to you? Well, there are many different kinds out there, so let me begin with friendly geeks at first.
Video games have changed the world, and many youth, or even adults, have become obsessed with their favorite games. For those who have never played online games straight through a whole night or day, or both, for days—might find it difficult to understand why certain people become addicted to video games.



Those who just love to play and spend money on games is one thing, but there are other types of geeks too. Some nerds are *obsessed* with new tools and software and believe they MUST be tried out ASAP, even if some of this software is downloaded from torrent websites illegally. Of course, there are other geeks too, who would not necessarily download everything for free, but instead would purchase the original software or tools to feel better by having the real thing. The authentic software always provides a better feeling, as well, many geeks buy it out of respect for the creators, contributing to the software

developers and designers.

When it comes to blockchain, there are multiple companies that have been formed recently which are designing a particular protocol that would allow certain online games to be played by using their own in-house built cryptocurrency. Topping it off, they have created excellent online games that once the gamers join and play, they would participate in their cryptocurrency by providing CPU or GPU power from their Game PC-s, PlayStations, X-Box-s and so on. Because these protocols would be fully utilized and continuously contributed, it's value would begin to increase dramatically. As you can see, blockchain would allow creating not only a new cryptocurrency, but an online gaming community, who would use a particular blockchain technology.

I have mentioned an example of gaming. However, there are many companies that are now into similar blockchain technology, such as music on demand, movies on demand, social networking sites and so on.
One of the biggest inventions so far, using the blockchain is the creation of smart contracts, such as Ethereum. There are many other alternative blockchains that exists to date, and each will shape our future at some point.
To mention some other important choices, there are various decentralized crowdfunding, healthcare, supply chain, blogging sites, and real-time sharing; but the biggest of all is IoT.
IoT, also knows as Internet of Things, for blockchain is increasing rapidly in recent years. Internet of Things is also called smart devices, or connected devices, that are physical devices, or even driverless vehicles. The purpose of these devices is to log in to the network and begin to share data one to another. Automating everyday life is a small-scale business, such as software, electronics, and sensors that would interconnect to each other. However, when it comes to large scale, that’s where the bit money is, such as virtual power plants, smart homes, intelligent transportations, or even smart cities capable of operating using blockchain technology. There are big scale business plans for big boys, that require years of planning; however, the technology to allow it, now exists. These projects would provide opportunities for direct integration of the physical world into computer-based systems, resulting in improved efficiency, accuracy and economic benefit in addition to reducing human intervention.
M2M – Machine to machine communications already exist. However, blockchain will enhance this beyond, by speeding up virtualizations and trust collecting data into blocks, helping to use our data more efficiently.

Chapter 14 – The future of banking

Currently, there are thousands of banks all over the world. Therefore, the current banking system will not stop tomorrow. It will require having at least a decade, if not two. However, the technology already exists to use other methods than banks, all that is needed is for blockchain technology to be applied by all our business partners, or employees, or employers. It is straightforward, really. Yet, most of us are very comfortable with the current system; therefore, the change might take a long time.

Gold

When gold was retired as a currency and paper money was applied, it took many long years to implement and make everyone understand that wages are now not paid in gold, but paper. As I mentioned before, gold is still an excellent payment method in most countries; however, it is not accepted everywhere.

When you go to the local supermarket, you cannot pay by gold, well some places are possible; nevertheless, most places will not accept it. Same as when you purchase something online, you cannot pay in gold, and there are other reasons too because it is an old method.

First, let's look at the flexibility of the gold. Imagine that you want to go to the

local Coffee shop to have a cappuccino. The idea to pay in gold for a cappuccino, is daunting. How would you break or cut the right amount of gold to the shop owner, besides the point, what if you make a larger cut than you have intended in the first place? The point is, that any precious metal as a payment method cannot be widely implemented. It's heavy; it's difficult to cut or break to the right amount of pieces required; therefore, the idea of using it in the future for money is just not suitable.

Cash

Unfortunately, paper money, cash, keeps on getting printed all the time. Therefore, it's impossible to tell how much is on the market. The more and more it's printed, the less it's worth. From history, we have learned that after a while there is so much cash getting printed that eventually, it all becomes worthless. Inflation becomes the main issue, lots of people become poor with all their saved money in the bank, then governments begin to print new paper money for the so-called new economy.

The problem is that this system has failed miserably—on multiple occasions; as a result, we all know that it's worthless. The problem is that this system is centralized by governments and banks that average people have no power to go against. Digital currency on the other hand is unstoppable, and such like bitcoin, can change the current system very quickly.

Another issue with paper money is that it is very easily counterfeited. There are countless incidents every day involving all kinds of paper money. It doesn't matter how well paper money is made; it can be duplicated. Consequently, counterfeiting will always be around. Cryptocurrency on the other hand cannot be faked, cannot be copied, cannot be counterfeited. Because blockchain represents trust and the exact amount of digital money, keeping just that in mind, you have to understand that cryptocurrencies easily can overtake any paper money, especially if it's centralized.

Yes, it's true! Only 21 million bitcoins will ever be created. So how can there be enough for everyone? Well, each bitcoin has 100 million Satoshis. I am not very good at math, so I have used a calculator to understand how much Satoshi will ever be produced, and the number looks like this: 2,100,000,000,000,000.

There are close to 8 billion people living on earth. So next, I have divided the huge number by 8 billion, to understand how many Satoshis each person on earth could have distributed equally. The number I got is: 262,500
The reality is that currently, 60% of the population will never even have $20,000.00 saved in their whole lives; But, before you think that is the final outcome; let me tell you something else. Blockchain technology allows each Satoshi to be broken into other fractions such as another 100 million pieces, and if that's still not enough, those fractions can be further divided into another 100 million of even smaller portions, and so on, and so on. That being said, I hope that you understand that Bitcoin itself, can supply the whole world when it comes to a new currency. But, there are many other currencies already, and the banks have begun to think about creating their own digital currencies too.

Ripple
Currently using swift, making international transactions can be a pain. Instead of taking a few seconds like bitcoin and other cryptocurrencies, it can take 3-5 working days.

Besides taking too long to transfer money, it might also be unavailable to individual countries, not to mention the fees. Making payments with several cryptocurrencies that are using the blockchain as their platform, are not only super-fast, but have very cheap costs—if any. Additionally, anyone can have a bitcoin wallet online.

Anyone—meaning ANYONE. When you go to the bank to open a new bank account, you must fit all the criteria that the banks ask for. Such might be, that you must have a valid address, you must be 18 years old, you must have proof from your employer that states your occupation as well your wages and so on. Instead of all these headaches, if you have a smartphone, you are able to open a bitcoin account without any of the aforementioned criteria. Then, in a few seconds, you can begin to even make international transactions.

As you can see, the current issue is that If I want to buy something from you, I have to make a transfer from my bank through PayPal, to your bank, which eventually would pay you. It takes at least one other so called trusted 3rd party to make a payment. However, blockchain would validate that transaction for us. Therefore, we wouldn't require banks or any other trusted 3rd parties anymore. All that is necessary is internet access for few minutes.

You have to understand that more than 2 billion people currently have no bank account, for various reasons. They might not be qualified enough; they might not even have the proper clothes to enter a bank. Of course, they might just choose not to have a bank account, but mostly, so many people just live too far from any bank. Therefore, they have decided not to have one. They might have internet access here and there, so this might as well become their bank, right? Why not? It would be very beneficial to them, and it's already happening with lots of people.

What the banks have realized is that it might be a good idea to create their own cryptocurrency, so in case blockchain takes over the world, at least they are prepared for the big boom.

Ripple network, born in 2012 as a new currency exchange protocol, it’s currency called Ripples. It supports traditional fiat currencies such as US dollars, euros, and British pounds; however, it’s also exchangeable to most cryptocurrencies as well as commodities. When it comes to market capitalization, Ripple has indeed taken a huge step by proving itself to be a good investment for traders. As of June, 2017, Ripple is the third largest after Bitcoin and Ethereum.

There are multiple large banks that already participate in Ripple, and this new payment protocol guarantees almost no fees for any international payment transfer. Before you invest in Ripple, I would highly advise you to do your research. The issue here is that ripple is centralized. Therefore, it offers greater security once it comes to your ripple account; however, when it comes to potential growth in the future, that is an entirely different question. Because the banks have taken control of ripple already, they can manipulate it's value anytime they want; therefore, it’s your choice how much you want to support the banks and for how long in the future.

Chapter 15 – Overview

I hope that you have grasped a little of what the blockchain is, and what direction is it going. I will write another book shortly and explain blockchain in more depth. However, this book is a beginner's guide. Therefore, I have done my best to avoid technical terms as much as possible.

Overall what you have to understand is that blockchain and bitcoin are not the same things. Blockchain is a technology, and its first application was on the platform named bitcoin. Bitcoin is blockchain. However, Bitcoin itself, is only a cryptocurrency that is capable of replacing fiat currencies. Nevertheless, not that many people will like the idea at first. Blockchain has solved the problem that we have always faced, that is trust. Using blockchain technology enables us to avoid trusting third party services. Therefore, any payment or exchange over the internet will be between 2 parties only. This is revolutionary as we can expand the trust gap, and the market of the future not only will be faster and cheaper, but will have no limitations, such as age, race, sex, occupation, nationality, or anything like that.

If you tell your friend, who has never heard of blockchain and thinks that he or she is not affected, try to explain that everyone is affected by the blockchain. Although blockchain will not take over the world from one day to another, and it

might require a decade, or two. However, everyone is affected.
Blockchain is also known as the future of money; even though streaming money sounds weird to some, it not only will happen, but has already begun for nearly a decade, and will not stop. Data protection using blockchain will be very secure and always will provide the truth.

Because this high technology enables us to become our own banker, we might not require having banks anymore in the future. Still, because we have to look at what we have, certain IT skills will help us to be safer from cyber criminals. Once you understand how easy is to keep your valuables safe online, you also will realize that it is even easier than opening a bank account.

Therefore, the changes for the young and the next generation will speed up the process of learning about the crypto world. Of course, some people may have to learn the hard way, as many people have been hacked, and only after, begin to invest in learning and implementing security. Still, the time of blockchain has begun, and it will change the world.

Average people, with no technical background, wouldn’t believe it, and probably say that blockchain itself isn’t capable of anything. However, software developers, security experts, large financial institutions, FinTech start-ups, and banks, already have paid a keen interest, as well have begun to invest and create their own protocols. Intel, Microsoft, Cisco Systems, Dell, and many more large, high-end technology firms, are already all over the blockchain and its little intricacies. Therefore, the days are counting, to reach the big bang of the transformation, the technology of the future, or, I should say, the next internet!

Conclusion

Thank you for purchasing this book. I hope this title has provided some insights about what is really behind the curtains, when it comes to the future of money. I have tried to favor every reader by avoiding technical terms on how the Blockchain works. However, my upcoming book on Blockchain will provide more details on the original protocol that is open source, as well how you can create your own digital currency from scratch.

Additionally, I will provide more details on how you can safely begin to invest in cryptocurrencies, and how they differentiate, one from another.

I will also provide guidance, on how you can become a miner by renting equipment, as well how you can start mining digital money using your laptop, or even your Android phone.

Lastly, if you enjoyed the book, please take some time to share your thoughts and post a review. It would be highly appreciated!

Mastering
BLOCKCHAIN
Advanced guide

Volume 2

by

Keizer Söze

Disclaimer

This Book is produced with the goal of providing information that is as accurate and reliable as possible. Regardless, purchasing this Book can be seen as consent to the fact that both the publisher and the author of this book are in no way experts on the topics discussed within and that any recommendations or suggestions that are made herein are for entertainment purposes only.

Professionals should be consulted as needed before undertaking any of the action endorsed herein.

Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States.

The information in the following pages is broadly considered to be a truthful and accurate account of facts and as such any inattention, use or misuse of the information in question by the reader will render any resulting actions solely under their purview. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall the reader or anyone else after undertaking information described herein.

Additionally, the information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its prolonged validity or interim quality. Trademarks that are mentioned are done without written consent and can in no way be considered an endorsement from the trademark holder.

Introduction

Congratulations on purchasing this book and thank you for doing so.

This book is an advanced guide to better understanding the technology called Blockchain. The contents are highly technical; therefore, it is recommended to read volume 1 first. This book uses precise details to provide a better understanding of Blockchain to those who are new to this technology; however, the second part of the book goes into detail in more depth of what makes blockchain tick. There are certain terms that some technical background in Information Technology would help. However, it's not necessary. Everyday English has been used through this book to avoid confusion, and this book will take you by the hand and show you, step-by-step, how blockchain attributes are working together.

Blockchain is based on multiple existing technologies working together, and this book will reveal each of them for your understanding. Reading about each technology explained in this book will get you closer to mastering blockchain and understand in depth how it improves data integrity, as well as enhances data security. It will then move on to explaining the advantages of terminating trusted third-party services and replacing them with mathematical algorithms and digital signatures. Next, it explains what 100% Data Availability is, using a fully decentralized peer-to-peer network, and how data will always be available.

Finishing off, by explaining Lightning network and how it's going to help us by using faster and cheaper payment transactions, and how employee payments can be made, not daily, but every second.

BITCOIN IS BLOCKCHAIN!

While some people think that Bitcoin is the main focus, Blockchain is Bitcoin's legacy. Blockchain is the technology behind Bitcoin, the revolutionary "virtual currency" that is changing the way people do business.

WHY WOULD YOU READ THIS BOOK?

• Technology giants such as Intel, Microsoft, Cisco Systems, and Dell already invested in learning about Blockchain.

• The world's largest Banks and Financial Institutions already created their own Cryptocurrency, using Blockchain technology.

• Fin-Tech Companies realized that Smart contracts are changing the way of doing Business, using the Blockchain platform.

• There are thousands of new start-ups investing every day into blockchain, adapting to the technology of the future!

WHY ALL THE HYPE?

• A single Banking system can save between 8-15 Billion dollars per year, using Blockchain • Terminating trusted third-party services, and replacing them with mathematical algorithms, and digital signatures.

• Faster and cheaper payment transactions, in fact, employee payments can be made not daily, but every second.

• Better Data security by eliminating single point of failure.

• 100% Availability, using a fully decentralized peer-to-peer network, data will always be available.

Blockchain will revolutionize a wide variety of businesses. Blockchain technology is influencing the future of doing Business, therefore, instead of falling behind, take advantage now, and learn how to master Blockchain today!

Communication will be affect, and in fact, is already in motion and visible everywhere: • Person to Person

• Business to Business - B2B

• Machine to Machine - M2M

This book has lots of in depth information that will help you to understand blockchain technology. It is a detailed guide on all Blockchain attributes, and how the technology works behind Bitcoin!

This Advanced Guide is an excellent choice to gain a better understanding of: • What Blockchain is,

- How it improves data integrity,
- How it fundamentally changes the future of doing business, • How it enhances data security.

There are plenty of books on this subject in the market, thanks again for choosing this one! Every effort was made to ensure the book is riddled with as much useful information as possible. Please enjoy!

Chapter 1 – Fundamentals of Bitcoin mining

I'll presume that you have basic understanding what blockchain is, as this book will focus in depth on the knowledge and nitty gritty details that people don't like to talk about. As with every existing technology, when it comes to blockchain, it is also true that there are only a select few individuals who are interested in how things work. Therefore, I would like to congratulate you on deciding to take your interest to the next level. Most people are only interested in listening to music, they never learn how the CD player works. Of course, there are new ways of listening to music or audiobooks. Still, this is one of my all-time favorite examples that I have always used throughout the years when I'm just about to explain something to someone who isn't interested in what I am about to say.

The reality is that you don't have to understand how the CD Player works, neither how the music is transferred wirelessly, using Bluetooth technology, to your speakers that provide you with your favorite tunes. This is fine; however, each time you learn a new word you are creating an additional brain cell, leading to you increasing your IQ, and in turn, you become more intelligent. Furthermore, you will decrease your chances of losing all your brain cells. It has been researched that once an average human being turns 30-40 years old, brain

cells begin to die, literally keep disappearing, and there is not much you can do about it. Each decade an average human loses between 5-10% of his brain capacity; of course, it depends on many circumstances. But, the overall average is 7%. Brain cells will die—no matter what. However, what you can do is to keep on creating additional brain cells by learning new words and new skills, really anything that is new to your brain. It has also been researched that learning a new language can help you grow your IQ, creating a tremendous amount of new brain cells.

Which new language? You might begin to learn German, Italian, or French. However, when it comes to technology, there are other languages too: C+, C++, Python, SQL, JAVA, Pascal, PHP, and hundreds more that you can grasp. Each minute of your interest and learning will divide you from the crowd.

This book will focus on the Technology called Blockchain. Although it is relatively new, once you take a closer look at it, you will understand that the underlying technologies that allow the block chain to run, have existed previously. I will reveal each of these technologies in great detail as well; due to Blockchain's innovations, there are some new protocols that must be addressed in the following chapters.

If you have not read my first book, Blockchain for beginners – Volume 1, I would highly recommend starting with that first, so this book will not be that difficult to understand. Nevertheless, I will provide a little overview of what the blockchain is in few sentences. However, if you have read Volume 1 already, you may skip to Chapter 2 now.

Overall, what you have to understand is that blockchain and bitcoin are not the same things. The blockchain is a technology, and its first application was on the platform named Bitcoin. Bitcoin is blockchain. However, Bitcoin itself is only a cryptocurrency that is capable of replacing fiat currencies. Nevertheless, not many people will like the idea at first.

Blockchain has solved the problem that we have always faced, and that is trust. Using blockchain technology enables us to avoid trusted third party services. Therefore, any payment or exchange over the internet will be between 2 parties only. This is revolutionary, as we can expand the trust gap and the market of the future not only will be faster and cheaper, but will have no limitations, such as age, race, sex, occupation, nationality, or anything like that.

Blockchain uses a distributed ledger system to keep all records that have ever been registered on the blockchain. The records are trusted by proof of work (more on this later).

Miners also play a significant role, and the two most important issues they are responsible for solving are:

1. Permanently validating transactions
2. Adding new value into the existing system

Miners can be individuals or any Bitcoin citizen; however, over time, many large companies have been formed such as Genesis Mining where you, as an individual, can join and rent their mining facilities. There are many other miners that over the years have created a pool, and many of them also offer to join these pools.

The miners are sealing the blocks, which itself can take an enormous amount of computing power, assuring that it cannot be easily replicated. There are multiple methods that each miner may use for the validating processes. Some of the miners may use different software—even creating their in-house made software to speed up the authentication process. However, it doesn't matter what software they use, as all of the work will be checked. The process starts when a miner begins to gather transactions that have been broadcasted on the network, then starts checking those transactions and eventually sealing those collections of transfers and operations into a new block.

A miner receives Bitcoin as an reward for each sealed block that is added to the blockchain. A block is created about every 10 minutes. Therefore, 144 blocks are created each day. As I mentioned before, the miners who have successfully added a new block into a blockchain get awarded a degree of Bitcoin.

The reward for each new block creation used to be 50 bitcoins from 2008 until 2012. The reward for a new block gets halved every four years; therefore, from 2012 until 2016, the award for each new block used to be 25 bitcoins.

Currently, since 2016 until 2020, the award to a miner for a new block that is added to the blockchain is 12.5 Bitcoins; however, from 2020, it will be only

6.25 bitcoins until 2024. This process will be continued until 2140 until the last bitcoin will be created.

Block creation:

1.

Start a new block. Even if the miners are half-way done validating a block, eventually, they will drop everything and concentrate on starting a new block.

2.

Select a new transaction. This is when the miners are choosing from thousands of operations that are broadcasted over the network.

3.

Check priority of the transaction. This time the miners can go back to number one by starting a new block if they find that the transaction they have selected previously is not that significant. However, if the priority is high, the miners may go on and move to the next step.

4.

Check that the transaction is valid. This is a process that every minor must check, there is no exception of avoiding this step for any miner. However, if the transaction is found to be faked, or not valid, the miners have to stop the process, go back to number 1, start a new block, and get another, hopefully, valid transaction.

5.

Accept the transaction. If the previous transaction was tested as a valid transaction, it must be accepted.

6.

Seal the transaction. Again, if the transaction has been found valid and accepted,

now it’s time to seal that transaction.

7.

Add the transaction to the transaction tree inside the block. This process can only be done once all previous steps have been verified.

8.

Check for the size of transactions. The miners need to check if there are enough transactions within the transaction tree, to seal the block. If there are not enough transactions yet, the miner will not be able to seal the block until there are enough transactions. Therefore, the miners must go back to number 2, selecting a new transaction again, and again, until there are sufficient transactions for sealing the block.

9.

Check interruptions. This is the process where the miner must make sure that no other miners have sealed the block in the meantime with the same transactions inside the block.

10.

Seal the block. Once there are enough transactions for sealing the block, the miners will seal the block.

11.

Broadcast the block. The miners must broadcast the new block that has been sealed; however, if the miners have been interrupted within the block sealing process, they might have to start a new block all over again.

12.

Start a new block. This is the next step in the process; however, as you see, we are now back to step number 1. As I mentioned, miners might get interrupted while they are sealing the block, and once they broadcast it, if another block has already been sealed by another miner with the same transaction within a block, the block will not be accepted. Therefore, you must start a new block.

If you tell your friend, who has never heard of blockchain and thinks that he or she is not affected, try to explain that everyone is affected by the blockchain. Although blockchain will not take over the world from one day to another, and it might require a decade or two. However, everyone is affected.

Blockchain is also known as the future of money; even though streaming money sounds weird to some, it not only will happen—but already began nearly a decade ago—and will not stop. Data protection using blockchain will be very secured and always will provide the truth.

Because this high technology enables us to become our own banker, we might not require having banks anymore in future; still, because we have to look out for what we have, certain IT skills will help us to be safer from cyber criminals. Once you understand how easy it is to keep your valuables safe online, you also will realize that it is even easier than opening a bank account.

Therefore, the changes for the young and the next generation will speed up the process of learning about the crypto world. Of course, some people may have to learn the hard way, as many people have been hacked, and only after, begin to invest in learning and implementing security. Still, the time of blockchain has begun, and it will change the world.

Average people with no technical background wouldn’t believe it and probably say that blockchain itself isn’t capable of anything. However, software developers, security experts, large financial institutions, FinTech startups, and Banks already have paid a keen interest, as well as have begun to invest and create their protocols. Intel, Microsoft, Cisco Systems, Dell, and many more large, high-end technology firms are already all over the blockchain and its little intricacies. Therefore, the days are counting to reach the big bang of

transformation, the technology of the future, or I should say, the next internet!

Chapter 2 – Blockchain attributes

In case you have read Volume 1 already you might have skipped chapter 1 of this book altogether. However, I wanted to exhibit a little introduction in case you are completely new to Blockchain, or you just wanted a quick recap on the fundamentals of blockchain.

As I mentioned in Chapter 1, blockchain is a new technology; however, once you take a closer look at it, you realize that the ingredients are pre-existing, and all that was needed was to stack them together.

Some inventors do get offended once a new and better idea takes over their own, especially if it's even cheaper, faster, or often free of charge; but this is part of the innovation that we have always experienced. When it comes to technology and you invent something today, it's almost guaranteed that once it's on the market, there are a significant amount of people already trying to copy or make it better—whatever that service or software is. Therefore, innovation is inevitable. It is just as true when you look at physical storage for keeping data, such as music, video, or software. What happened over the years is this: the less space required the greater the quality became; in fact, most data, movie, and music, are now streamed from multiple sources; therefore, the idea that money will be streamed one day should not be surprising. I still remember when I used to buy VHS and DVDs, also cassettes and CDs.

Also, remember when there were no mobile phones? Then, once they reached the market, I was able to make phone calls, and send text messages pretty much from anywhere, or even play the game called snake.

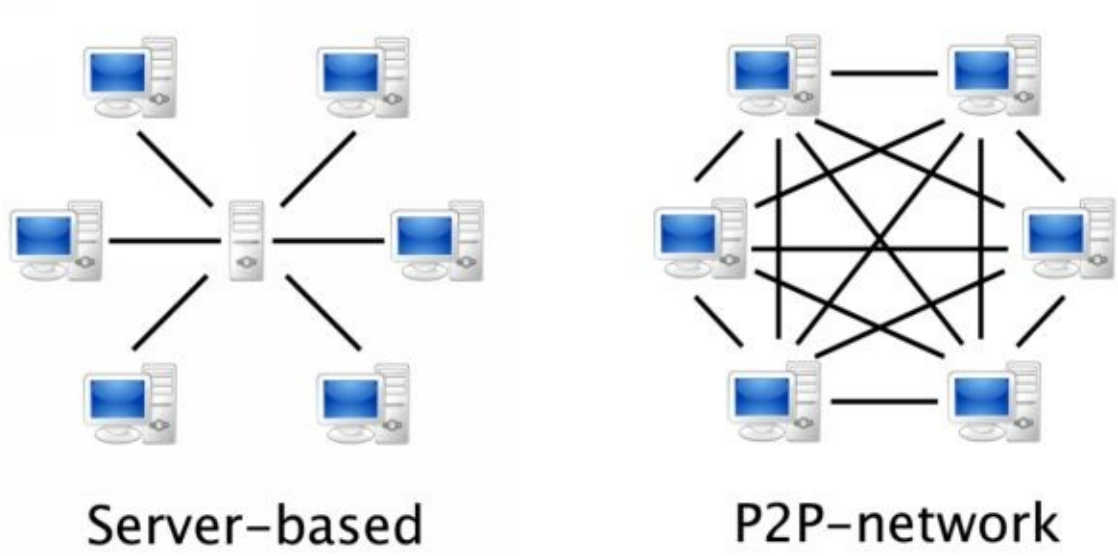
After the introduction of the internet, I was always waiting to get home so I could access the network or I had to call someone to check weather forecast or other useful information for me when I needed it. However, less than two decades later, I can now store hundreds of movies and music albums to my cell phone, as well capable of Skype, video calls, and access any internet page from anywhere in the world.

As you see, no one can predict what happens with technology over time. Believe me, the blockchain is where the internet was back in the middle 90’s. The internet seemed a nerdy idea, and most people thought that it was all about email. Like nowadays, some people believe that blockchain is all about bitcoin. The reality is that e-mails might have been slow and people weren't interested in them; still, in few years, most companies have moved online and of course become even more successful by doing so and the main tool to use for both internal and external communication within the infrastructure is e-mail.

Back to blockchain innovation and its ingredients. Let’s take a look at them and understand a little bit more about them.

Chapter 3 – Peer-to-peer network

To keep the blockchain running, it requires a network that resides on the internet. Furthermore, within the network, there are certain exchanges, for purposes of updates. These updates are required to continuously keep the distributed ledger system up to date with the latest block. If you turn your computer on and start to run blockchain protocol on it, it will become part of the blockchain network. Next, I would do the same with my computer, then my machine would become part of the network too.



Every single device that is connected to the internet, and running blockchain, becomes part of the network. This way all those devices can communicate with each other using the internet, and keep on updating each other. Because there is no master node or a centralized machine that has a different purpose than the rest of them, this network is called peer-peer network. Peer to peer networks have existed for a long time. Therefore, there is nothing new about it. However, because it has no master node of any kind, this is not a centralized network, but a decentralized P2P network. This is very important, as it tells you that there is no boss of any kind; so, it decreases the possibility that one or more nodes on the network might be able to manipulate the rest of the nodes. Manipulation of any kind is simply impossibly, and that, in itself, is proof we can trust the system. This is not all, of course, but the network itself is solely based on a technology that's existed previously; however, this time it has a different purpose. What you

have to understand is that when it comes to a peer-to-peer network, there is no central server or central client. In traditional centralized networks, there is the primary server, or central servers, and multiple clients; and the way they are connected is that the servers are always dictating what the clients can have. Peer-to-peer networks, on the other hand, are completely different, as all nodes on the network serve both purposes, they are all servers as well as clients. Meaning, no one machine can have a bigger decision power than any other on the same network. Therefore, P2P networks are always working together, making decisions together, and equally distributing those to all nodes on the network.

Another problem with centralized networks is that if one node is ready to share the latest news with the rest of the network, first it would have to send the traffic to the master node or server, which then would be able to do many things. The server could manipulate the traffic before forwarding to any other node. Managing the traffic would be easy on the server node, as once the server would receive the traffic from client A, the server would not send the same traffic back to client A (as that was the source in the first place). Instead, the server would send the traffic to the rest of the clients, but if this trade would be manipulated already, neither the remainder of the nodes or client A would never find out about it. Another issue would also be if the server would decide to send the traffic only for a particular group of clients, instead of all of them. Again, this could reduce the power of an extensive peer-to-peer network, and in the case of the blockchain, this would not be an advantage. The worse that could happen in a centralized network is this: once the server would receive traffic for the sake of conversation, data about the latest confirmed block, imagine that the server would decide not to share this data with any other client. This would just put the blockchain out of business. Therefore, the only way that the system would operate is to use a decentralized P2P network. In case you wonder how the server would make such a decision itself, well, it would not. Even though administering a server, or a small group of servers, may be straightforward for a person; when it comes to a P2P network, a person with evil intentions, like hacking purposes, or traffic manipulations, would have a hard time to do so and the reason is straightforward. Administering a large group of machines manually that reside all over the internet is nearly impossible. This is the reason why if you want to open a company, and you want to be the boss, you would create a traditional centralized network by having a master node that you can administer anytime you want. Again, P2P networks have no boss. Therefore, there is no one to blame, and every machine on the network shares the same responsibility.

Timing

In any system, centralized or not, there is always some delay. This is called latency. By the time one device reaches the other, it’s just never the same amount of time. Technically, latency is the time defined while the data travels between its source and final destination. This is something that you may consider understanding as data propagation can take some time, especially when there are thousands of nodes on a decentralized system.

Let’s look at an example for better understanding. Imagine that node A is ready to share its latest block with node B, C, and D. P2P networks are also known as dumb networks, as they have no idea what kind of data they are transferring; all they know is once there is data that needs to get transferred across the network they will do a broadcast making sure that all nodes are receiving the same data. So back to our example of four nodes and their data propagation. Imagine that node A is located in Los Angeles, US; node B is located in Sydney, Australia; node C is in Cape Town, South Africa; and node D is in London, UK.

They will all receive the same data; however, some of the nodes may get the data earlier than the other nodes. Therefore, the order of the transactions might differ on the nodes.

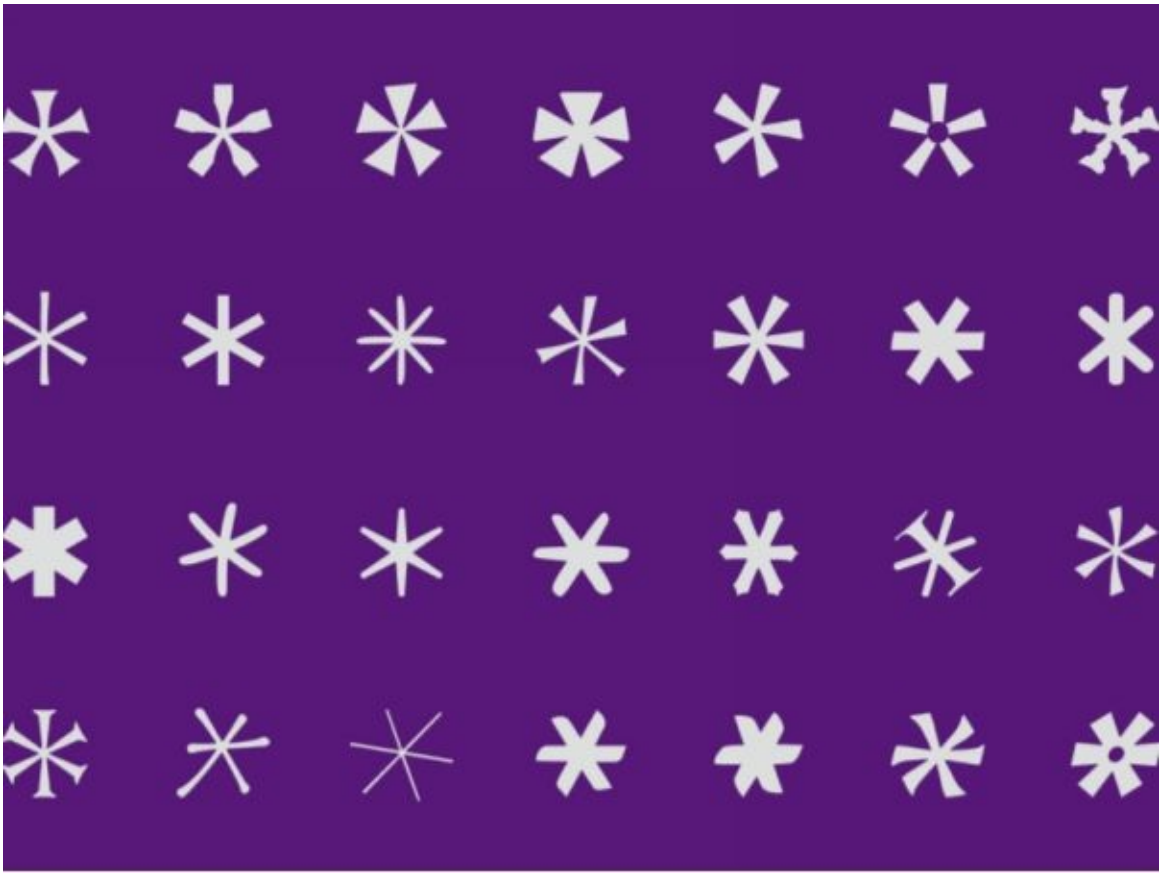
In summary peer to peer networks are helpful for the following reasons: • Reducing overhead by not sharing data over multiple nodes instead of keeping everything in one centralized location.

- Reducing risk of counterfeiting and manipulating data.

- Reducing third party interference, therefore, each transaction of smart contracts have fewer fees as well faster implementation.

Chapter 4 – Hashing

This is another topic that most people just skip if possible, and I can't blame them. Cryptography has complexity that not exactly everyone dreams to learn about. There are many different kinds of cryptography that exist; however, I will try to do my best to keep it simple for you to understand.



There is classic cryptography that has been used since the ancient times by the Greeks and Romans, even in Egypt; however, our focus is modern cryptography, especially the one that is related to computers. Before I drag you into it any deeper, let me elaborate some basic terms that are vital to understand before diving into Cryptography.

Hash

Hashing is referred to a fixed sized string of numbers, for example, 128, 256, 512, 1024, 2048 numbers. Hashing can be performed on various files, such as text, images, audio files, video files, or even software. It produces a unique hash based on that the particular file. An individual file goes through a hash on one end; then comes out scrambled on the other end. It doesn't matter what kind of file you try it out on; the result is always different. For example, you might try to put an md5 hash in the word "blockchain." The hash would be completely different than the word "blockchain1."

Note: MD stands for Message Digest, and the number 5 is its version number. Basically, MD5 has taken over MD4 hashing.

Let me show you how much of a difference there is between two very similar words. As I mentioned the word "blockchain," I will perform and generate an md5 hash on it. Ok, so the md5 hash value for "blockchain" is: 5510a843bc1b7acb9507a5f71de51b98

However, now I will perform the same md5 hashing on the word, "blockchain1." Let's see the result: 1150228f14788047028d774b7c83c5a6

As you see, this is a completely different outcome; this is because the word is different, although very similar, it is still a different md5 hashing value. Let's try to do this now with a number, and for simplicity, I will use very few figures so you will see how powerful hashing can be. This time I will perform md5 hashing on a number string of 123, and then 124, and see if there is any difference. Let's begin, shall we? Ok, so I have performed md5 hashing on the number string: 123, and the hashing value is this: 202cb962ac59075b964b07152d234b70

Now I will do the same md5 hashing on the number string 124:

c8ffe9a587b126f152ed3d89a146b445

As you see, again, it's an entirely different outcome; therefore, hashing itself can provide excellent security. However, I will move on to more in-depth. In case

you think I am some genius, or just making up the md5 values, I would suggest you visit the link for md5hashgenerator and practice for yourself. Perhaps you can start with the same words and number strings I made examples of. The website to visit is: http://www.md5hashgenerator.com/ MD5 is also case sensitive; therefore, using the very same letters, changing only one character to uppercase, the result of MD5 value would also be completely different.

The closest example I can give you is fingerprints or DNS. Those are also unique, and there are no two people who have the same DNS or the same fingerprint. Hashing has been widely implemented, mainly used by software developers. One of the main reasons is making sure that the software is not modified or corrupted while downloading it. Personally, I had an issue before when I upgraded a Cisco Switch with a new code, which has gone into Rommon mode because I was too lazy to check the md5 hash value of the software. Luckily, I was doing it within a test environment, and not in production network; however, it caused great pain and lost hours to recover the switch to its previous configuration. In my case I downloaded the code from the right source; but, it seemed to be that our Proxy server must have corrupted halfway. Still, if I would have checked the md5 hashing value of the new code, I would have been more successful at the task.

MD5 hashing is excellent; however, it is not called cryptography nor encoding. MD5 was implemented first in 1992, and if you think it’s a little old, then you are right. MD5 has been compromised several times due to its vulnerabilities, alone it is not sufficient to provide the best security. That being said, let’s move on to what Cryptography is.

Chapter 5 – Cryptography

Cryptography is a process defined by data being converted into a certain form so that it is only available to those for whom it was originally intended. However, converted data is inaccessible to an unauthorized end user.

Encryption:

What the process of encryption does is simple. It transforms a particular data into a form that is unreadable. The encrypted data has another common name: Cipher text.

Decryption:

The process of decryption is responsible for converting the unreadable data back into its original form so that it can become readable again. For example, a simple decrypted text, after decryption would become a plain text.

Once data has been encrypted, and it has been sent to the destination of the

recipient, there are different ways that can be used for data decryption. There are two prevalent techniques to encrypt and decrypt data, one is using Symmetric keys, and the other is using Asymmetric Keys.

Symmetric Key:

Using symmetric keys is easy. When encrypting, as well decrypting, we only use the same keys. An example here would be a door. When you go out to the store, you lock your door using your key, and once you return from the store, you would use the same key to unlock your door right? Well maybe I am wrong; however, typically the same key is used for those purposes.

The symmetric key algorithm is very fast, in fact, thousand times faster than using asymmetric keys. When we were talking about symmetric keys, same keys, they are also called shared secrets. As you can see the problem here is that both the sender as well the receiver must use the same key for both encryption and decryption too. Of course, this is not an advantage when it comes to security, and the blockchain is certainly not using Symmetric key algorithms. I wanted to introduce some of the basics before we dive into more depth, such as asymmetric key algorithms.

Asymmetric Keys:

Blockchain uses Asymmetric key algorithms as part of other algorithms it uses. Therefore, this topic is what you might have been waiting for.

To implement Asymmetric key algorithm, it requires having two different keys. One of them is called “Public” and the other is called “Private” key. The reason for having two keys is simple. One of the keys will be responsible for encrypting information to become a cypher text, and the other is to decrypt the information to become plain text. The private key would be generated by the originator, the one who would encrypt the information, and this private key must be kept secret at all times. However, the public key would be available to anyone, this is why it’s called the public key.

The asymmetric key algorithm is much slower than a symmetric key algorithm; however, the security is more complex. Therefore, it is harder to be hacked. Both, public and private keys are mathematically interconnected one to another, meaning that each public key has only one corresponding private key. There are

few algorithms like that. However, blockchain is correctly using the one called: Elliptic Curve Digital Signature Algorithm.

This situation is a little different for how Symmetric key algorithm works. Once the private key has been used to encrypt the information to become a cypher text, it is necessary to use the public key to decrypt the information back to plain text. On the other hand, this process can be interchanged and used the opposite way too. For example, I would encrypt the information using the public key; then I would decrypt the scrambled text back to plain text using the private key.

Chapter 6 – Digital Signature

When it comes to a legal contract, the traditional way to do business is that both parties, the buyer as well the seller, has to sign the contract, amongst many other documents for legalization. This traditional way of signing contracts is carried out with handwriting using a pen. However, there are other ways to authenticate certain documents, and one of the most known is using digital signatures.

Digital signatures are very similar to standard traditional handwriting signatures. However, they are much more secure. When it comes to handwriting signatures, there is a long history of them easily being faked by a pro or anyone with a little practice. Digital signatures have overcome the issues of counterfeit signatures by using some simple methods. The digital signature provides the recipient unique information; therefore, it provides authenticity.

Integrity: This is for making sure that while the message was in transit, it had no alteration or any modification.

Authentication: This is to provide the authenticity of the sender.

Non-repudiation: This is, so the sender cannot deny that the message was ever sent.

In case you're wondering how the digital signature is created, as well verified, let me begin by explaining it. Imagine that you want to create a document by adding a digital signature to it so that anyone would know that it belongs to you. What you can do first, is to hash the data. Next, you can use a private key to encrypt your data. That's it, as the encrypted hash is your digital signature. Taking this further to prove that it is indeed your digital signature, you have to send the document to someone who can then decrypt your data. Once you send your text to your friend, you also have to carry the digital signature along with the document. Once your friend has received the document, he or she should decrypt your document by using your public key. This time the result of the hash value of the document would be HASH1.

So, if your friend applied the same hash algorithm on the received document, the result of the hash value on the received information would be HASH2. Next, your friend should compare both hashes: HASH1, and HASH2 and if the values are the same, it would be proof that your document had no alteration in transit, the document is originated from you, and it is indeed yours. Today's digital world demands more flexible and responsive solution, then handwritten signatures. Instead of wasting time by using traditional signatures, digitally, you can handle contracts in a matter of minutes.

Using digital signatures—deals can be closed in minutes—not weeks. Lots of software literally lets you create digital signatures in seconds. All you have to do is select a document on your computer, right click, then choose using digitally, set your password on it and send it off by e-mail.

The process is completely paperless, and the digital signature just as valid as the one made without ink. Furthermore, not only using a computer but a new way of using mobile apps, by having a mobile ID, you can sign documents, make bank transfers using your cell phone only. This also means that you can be anywhere in the world, and in seconds you can authorize bank transactions as well signing any documents. Actually, research has shown that using digital signatures helps an average person save one whole week of free time in every year. You may use this time as a vacation. However, there are other benefits too. Paper. We can save tons of paper around the globe using digital signatures.

Chapter 7 – Logarithm basics

Let me ask you what do you think the difference is between the number:

0.0000000159, and the number:

0.00000000159? Well, if you feel pain in your head already don't worry, it's completely normal. Logarithms are helping us deal with small numbers; however, in some cases, huge numbers. This leads to the concept of logarithms. What logarithms are fundamentally about is to figure out what power you have to raise to, to get another number.

Logarithms are yet another component of blockchain technology that is going back in history to the 17th Century. This discovery has provided a new function that has extended beyond the scope of algebraic methods. Logarithms were publicly announced in 1614, and it began to simplify difficult calculations that contributed to the advance of science, as well, surveying and celestial navigations. Back then they had created different logarithm tables for various calculations; however, nowadays in computer science, logarithms still exist. Let's begin with a simple example for better understanding how logarithms actually work.

To have two to the power of three that means two times two times two.

$2^3 = 2 \times 2 \times 2 = 8$

In this example, we have three numbers to work with.

2 > this is our base number

3 > this is called the exponent, that will determine the number of times that the base number should be multiplied.

8 > this number is known as the product.

Now imagine that the exponent x is unknown, in this case 2x = 8 so we want to find out how much is the x, well we already know that, because of the above example; however, sometimes it can be lot's more complicated than this simple example. If you are only interested in the exponent, the mathematical notation: $x = \log_2(8)$

The pronunciation for the above mentioned is: x = log base 2 of 8

Exponentials $x = 2^3$ and logarithms $x = \log_2(8)$ are each other's opposites

The goal of exponentials is to calculate the product: $x = 2^3$

The purpose of logarithm is to calculate the exponent: $x = \log_2(8) = (8 = 2^x)$

So, we needed a numerical procedure that is easy in one direction, but hard in the other direction. When the generator has raised two different components, the solution distributes uniformly around the clock. If we raise any base number to any exponent x then the solution is equally likely to be any number between zero to 17. However, the reverse procedure is hard. For example, having the product number and you want to find the exponent is hard to do. This is called the discrete logarithm problem. Now we have our one-way function, that is easy to perform, but hard to reverse. It is trial and error really, but if you want to know

how hard it can be, then let me tell you. Well, having small numbers, this is easy to reverse engineer; however, if we use a prime modulus that is hundreds of digits long, it becomes impractical to solve. Even if you have access to all computation power on Earth, it can take thousands of years to run through all possibilities.

Chapter 8 – Diffie-Hellman Key Exchange

For as long as we know, people have always wanted to keep secrets. It has taken a lot of time and effort to accomplish this. As I mentioned before, the use of encrypted data can date back to time immemorial.

In 1976 Whitfield Diffie and Martin Hellman published a paper that explained how to create public key cryptography. They described a way of using open channels to exchange a secret key by using a one-way function called a discrete logarithm.

As you can imagine, one of the biggest problems in cryptography, is to exchange the keys between two parties. We don't just want to establish a common key, but we want to do it in such a way, that anyone who is listening to the communication between the two parties, do not find out the key.

The problem

Imagine that Alice and Bob want to exchange the keys; however, Eve is listening to their communication and intercepts the key that's being sent between Alice and Bob. Unfortunately, if Eve gets the key, she can encrypt the data; therefore, that key would not be secured enough for Alice and Bob to communicate securely.

The solution

First, Alice and Bob would agree publicly on a prime modulus and the generator. Let's take an example using a Generator of 3, and a prime modulus of 17.

Then Alice selects a private random number, say 15, and calculates 3 to the power of 15 mod 17 that would equal to 6. Then Alice would send this result publicly to Bob.

Next Bob selects his private random number, say 13, and calculates 3 to the power of 13, mod 17 that would equal to 12. Then Bob would send this result publicly to Alice.

If you are still with me, you might have realized that Eve might have captured both publicly submitted numbers that are 6, and 12; however, she would not know what to do with those figures so that she could carry on eavesdropping to the conversation between Alice and Bob.

What happens next is Alice takes Bob's public result and raises it to the power of her private number to obtain the shared secret which in this case is 10.

Bob takes Alice's public result, and raises it to the power of his private number, leading to the same shared secret.

They have done the same calculation, even though it does not seem like it at first. Consider the following:

Alice has received the number 12 from Bob, was calculated as 3 to the power of 13 mod 17, so her calculation was the same as 3 to the power of 13, to the power of 15 mod 17.

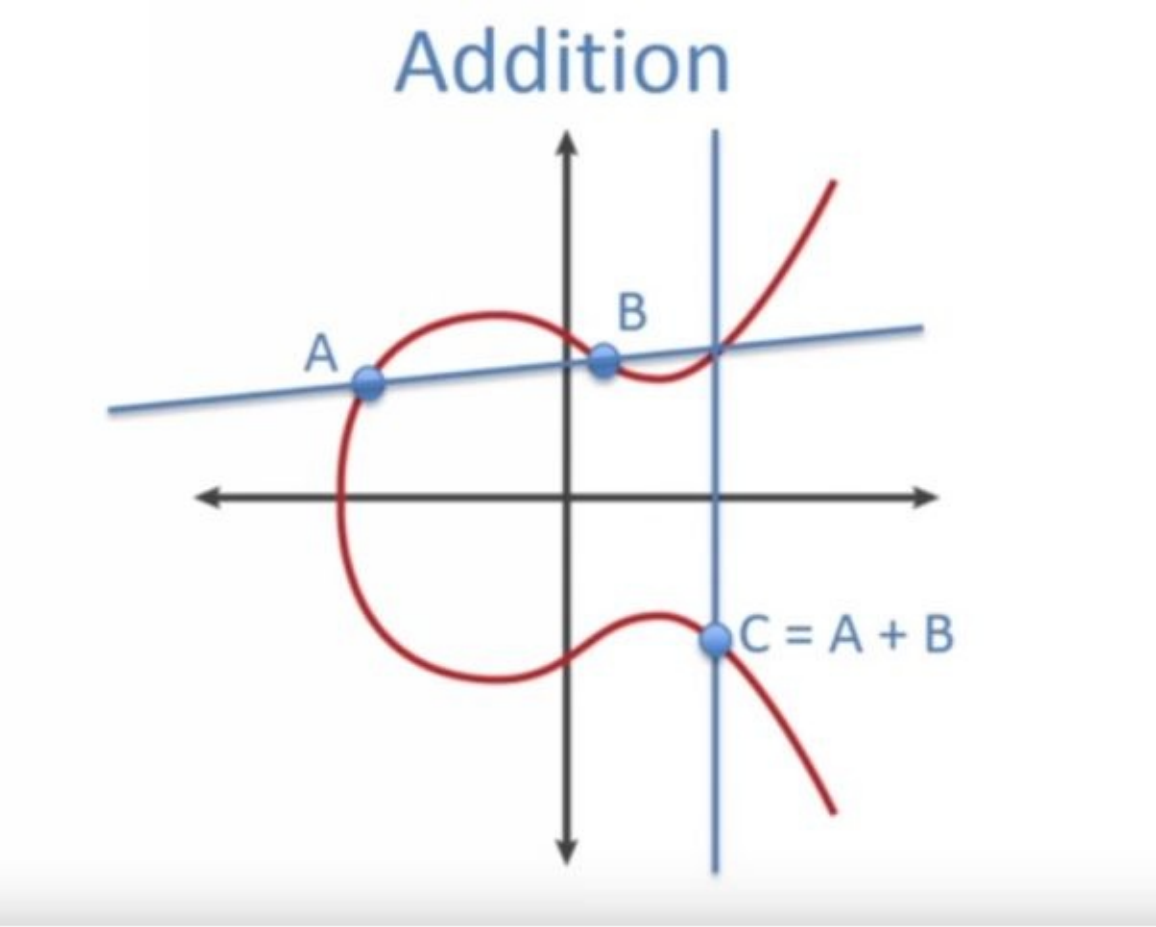
At the same time, what Bob did was this: He received the number 6 from Alice, and he calculated as 3 to the power of 15 mod 17. So basically, Bob's

calculation was the same as Alice's which is 3 to the power of 15, to the power of 13. They have done the same calculation, and the only difference is that they have used the exponents in a different order. They both have calculated 3 to the power of their private numbers. Eve would not be able to find the solution because she would get stuck on a discrete logarithm problem, and with large enough numbers, practically impossible for her to break the encryption in a reasonable enough time. This is how the key exchange problem is solved without any interception whatsoever. Again, thanks to Diffie and Hellman.

Chapter 9 – Elliptic Curve Cryptography

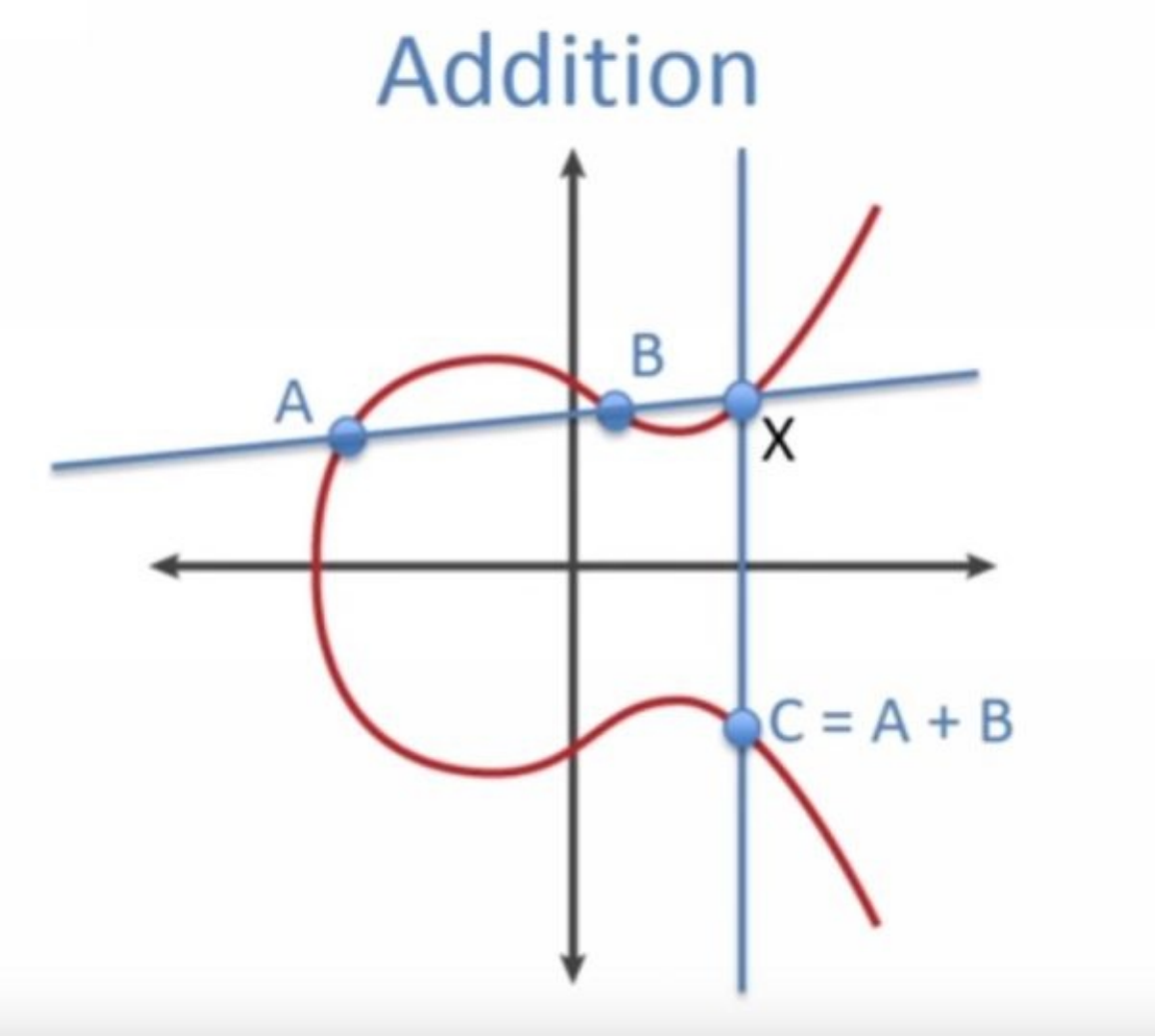
First you have to understand that Elliptic Curve Cryptography is significantly more secured than any other modern day cryptography functions.
Like many cryptographic systems, elliptic curve cryptography gained its power in mathematics. Generally, the elliptic curve's form is the following: $\mathbf{Y^2 = X^3 + AX + B}$
A and B are constant values, they usually can be real numbers or rational numbers. Elliptic curves can be done using standard algebra; but, they actually require their own definitions for thinks like: addition and multiplication. Therefore, in order to understand how Elliptic Curve Cryptography works, you must understand first how Addition and multiplication works.

Addition
Imagine a curve that you are about to add two points to: one called A, another called B. Once you have added those two points, you have to draw a line between them.



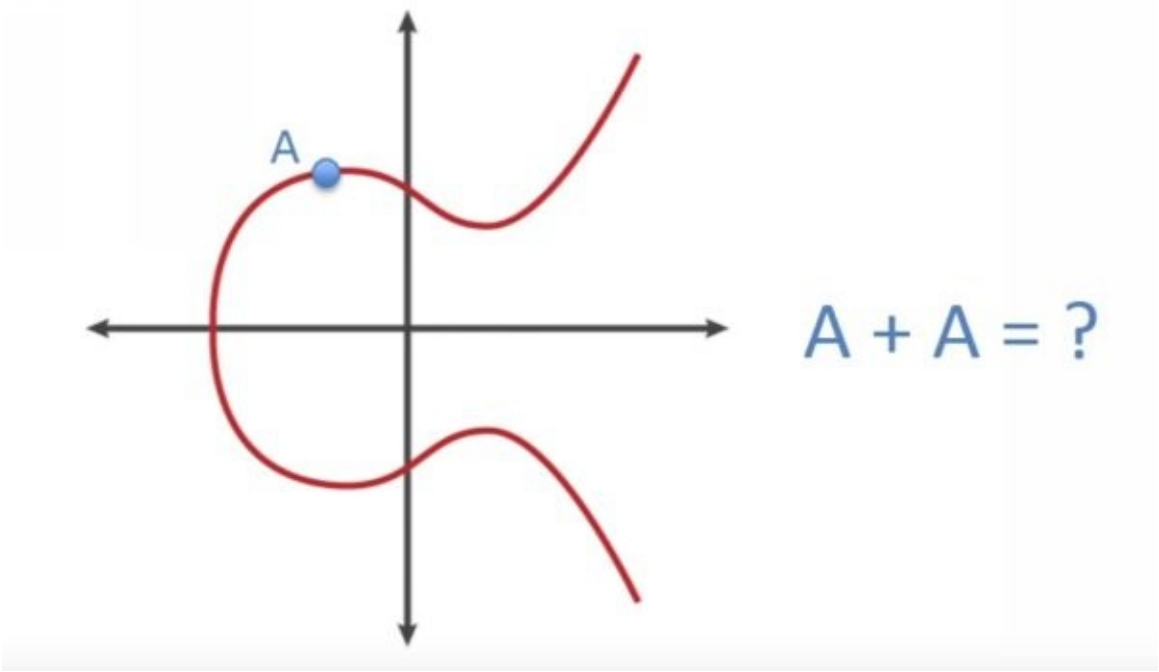
However, once you do that, you may realize that there is a third intersection on the graph. Once you have found the third intersection, you should begin to draw a new line and this new line, where it intercepts the curve again, will become your third point that you should call C.
Please note C is equal to A + B
C = A + B

Next, you can define the intermediate position on the top half of the curve which you can call X

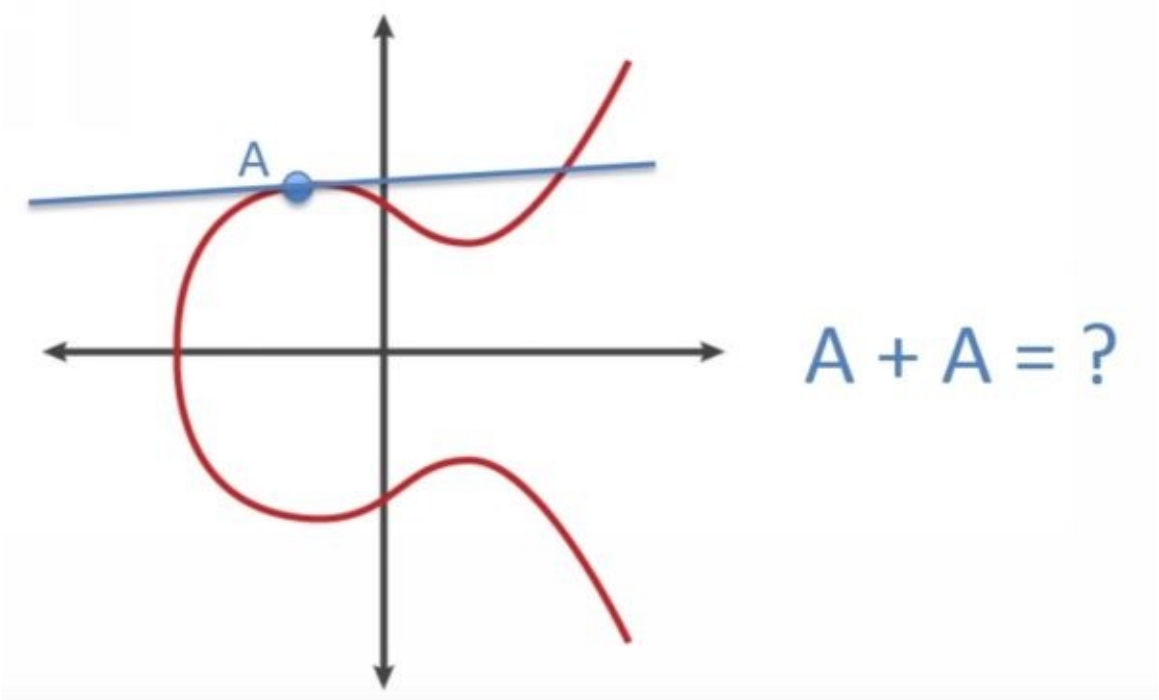


This is very important because the Addition requires a third intercept point; however, adding two vertical points is an undefined procedure. Therefore, this results to what is called the Elliptic Identity, also known as Infinity. The reason for this is when you would try to add two vertical points, there would never be a third interception, and you cannot define that addition.

Next, consider adding a new point to itself:

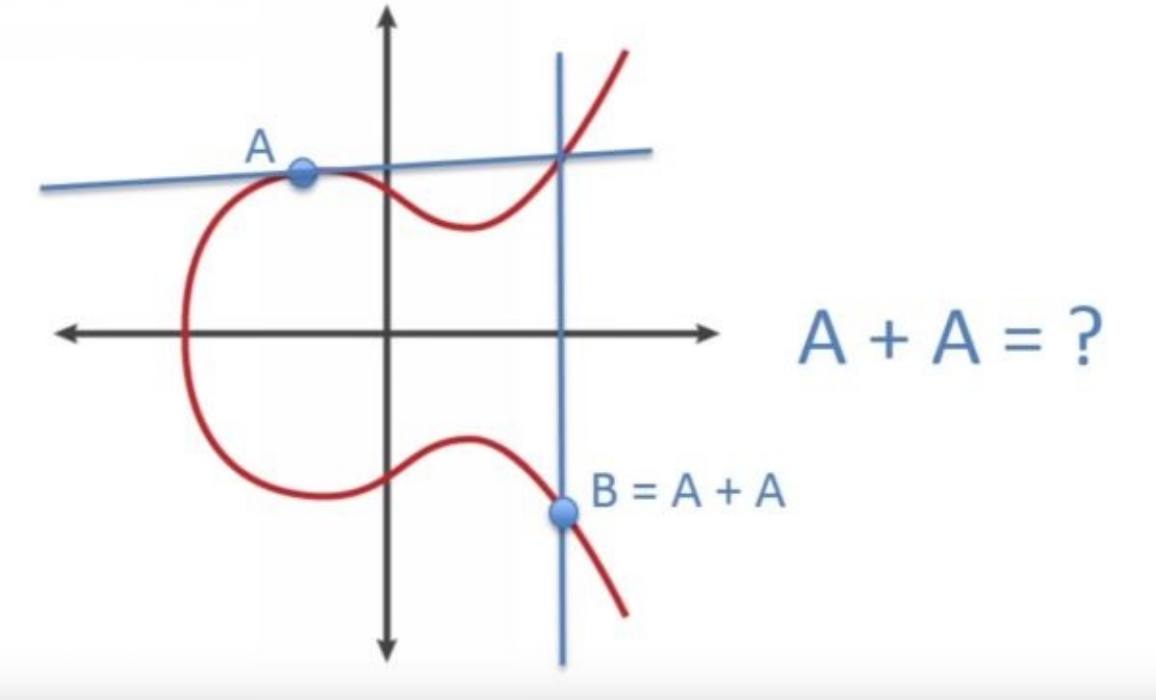


If you are adding a point to itself, of course, there is no second aspect to be considered, and you cannot draw a line between them. Instead, you can draw the line through A, and find the point where that would intercept on the curve.



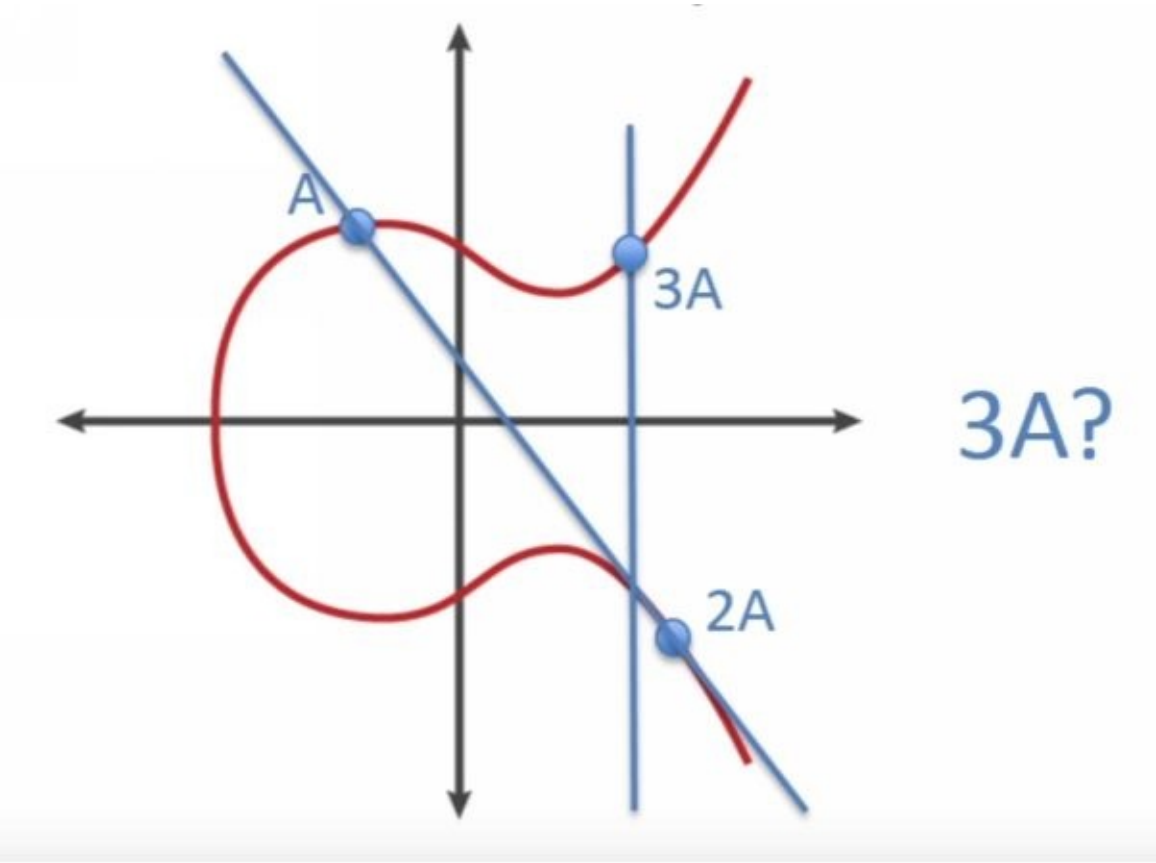
Once you have done that, it is the same procedure as before by drawing a vertical line, based on where the line intercepted the curve, and the crosses will

find point B. Note, B now equals to A + A



This is also known as Point Doubling. This is indeed a common way to achieve multiple occasion. This is also very similar to another algorithm called square to various algorithms, and if you repeatedly point double, you are doing what's considered multiplication regarding elliptic curves.

Let's call this 2A and move on to think about what if we want to calculate 3A. To perform some multiplication with three times A, you have to perform point doubling three times, meaning you have to add A to itself three times.
First, you have to draw the line between 2A and A, and wherever that line intercepts the curve, you flip across the x as you have done previously. As you can see, there is lots of jumping around on the graph, even just to perform a few multiplications. This computation is very similar to the square multiply algorithm, and this is where Elliptic Curve Cryptography gets it straight. As it's infeasible to divide the multiplications and find a particular point that you multiplied, unlike in regular algebra.



For example, if you've been given the number 10, and someone says he multiplied 5 to give you the number 10, you would know that the other number from the multiplication would be 2. However, it doesn't work like that in Elliptic curves. This is also known as the elliptic curve discrete logarithm problem. To compute the multiplier point, you would need to calculate all the multiples of the given point until you would find the one that matches. Of course, this is not possible, especially when you use larger values; due to the computation complexity of this problem.

Please understand that explaining fully what Elliptic Curve Algorithm is, could take a full book itself, in fact, books. However, I have tried to explain a general overview about this type of cryptography as it’s used by Bitcoin, as well Blockchain technology. Briefly, Elliptic Curve Cryptography is one of the most secured cryptographic systems used today. It’s computationally infeasible to calculate the private keys when using Elliptic curve key exchange.

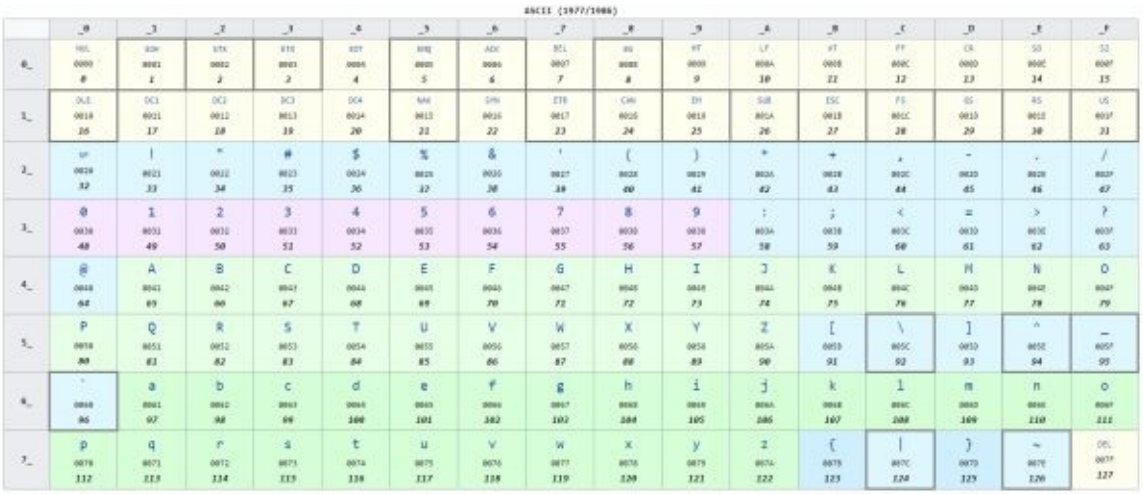
Chapter 10 – Encoding arbitrary data

In this chapter, I will explain some basics on different encoding mechanisms that blockchain uses for encoding arbitrary binary data into ASCII text; however, first let's begin with what ASCII text is.

ASCII
This is a character encoding standard, that represents text file to PC's, computers, and other telecommunication systems.
ASCII stands for American Standard Code for Information Interchange. It has been standardized by IANA – Internet Assigned Numbers Authority.
IANA is mostly known for controlling IP Address allocations around the world; however, that's an entirely other topic for a different day.

ASCII has been used to represent English characters in the form of numbers as each letter assigned a number from 0 to 127, therefore, providing 128 possibilities. Computers are converting text into figures because it makes it possible to transfer data from one computer to another.

The standard ASCII character set uses 7 bits, which is 27 = 128 possibilities for each character for English letters. However, there are many other character sets, such as SIO8859 or Unicode, using 8 or more bits to convert non-English characters and other symbols into numbers.



To understand further how ASCII encoding and decoding work, it is advisable to see an ASCII table, so you can see what numbers represent each letter

I will provide an example for your reference, so you can further understand how ASCII encoding works.

Let’s take an example of a word: Hello

If you began to encode the word Hello to ASCII text, the following number would be converted to:

Hello -> ASCII Encoding -> 72, 101, 108, 108, 111

At the same time, if you would want to decode the numbers back to its original letters, you would have to convert it as follows:

72, 101, 108, 108, 111 -> ASCII Decoding -> Hello

Please note, if you use the same word: hello. But this time the h letter wouldn’t be written as capitalized, the ASCII encoding would give you a different outcome. In this case the word hello would be a number of:

hello - > encoding -> 104, 101, 108, 108, 111

BASE-64

This is a way of encoding arbitrary binary data into ASCII text. Base-64 encoding systems are commonly used when there is a need to encode binary data; for example, images or audio, that needs to be stored and transferred over media that are designed to deal with textual data. This is to ensure that the data remains intact without modification and any alteration during transport. Base-64 encoding schemes use both capital A-Z, lower case a-z letters as well 0-9 numbers for the first 62 values, and the symbols of + (plus), / (slash).

The = (equal) symbol is used as a padding character. Base-64 maps are 3 bytes. (8 x 3 = 24bits) in 4 characters that span 6 bits (6 x 4 = 24bits). When the number of bytes to encode is not divisible by 3, and there are only 1 or 2 bytes of input for the last 24-bit block then extra bytes with value zero are added, so there are always three bytes.

BASE-58

Base-58 encoding schemes are also converting binary to base-64 encoding without using 0 (zero), O (capital O), I (capital I), l (lower case l), + (plus), and / (slash) because they look the same in some fonts.

Base-58 is used in Bitcoin and is unique to the Bitcoin project. To apply the Base-58 encoding, you have to implement the same process like with the Base-64 encoding; however, instead of using the Base-64 symbol chart, you have to use the Base-58 symbol table.

Chapter 11 – Checksum

Some identification numbers have digits embedded inside their numbers. Some of these are well known to the public, such as bank account numbers. These digits can be numbers of characters that are called Checksum Digits, and are used for error detection if you mistype the identification numbers.

Let's look at a British bank account number as an example:

GB29 NWBK 6016 1331 9268 19

In this example, the two-digit checksum values are 29. There is a special algorithm applied to this bank account number to calculate this checksum value. For example, if you would mistype this account number by typing:

GB29 NWBK 6016 1331 2968 19

Any British bank application will notice that this is an error because the checksum value of this number does not correspond to the expected checksum digit of 92, instead, 29.

Most cryptocurrencies, such as Bitcoin, are also using checksum digits. To be fair, there are so many blockchain implementations that it’s hard to say if all crypto currencies are using checksum digits; however, when it comes to Bitcoin, it is certain. What you have to understand is that checksum and hashing are not the same, in fact, there are some significant differences between them, so let me explain them now:

The checksum is designed to detect accidental errors in small blocks of data, such as: social security numbers, bank account numbers, cryptocurrency addresses, and so on, but they are most often very fast to compute.

While a hash reduces large data to a smaller number, in a way that is minimizing the chance of accidents.

Social security numbers or even bank account numbers are only identification numbers and have no other functions, but to identify individuals for Social Security or banking. However, the public key has a corresponding private key that is mathematically linked to each other. These keys are used to create a transaction between two or more parties, by using encryption, as well decryption, of data using these keys. The randomly generated private key and the calculated public key are converted into private addresses and public addresses. There are multiple reasons why the public and private key pair are turned into different looking public and private addresses, so let's look at some of those examples:

- Implement checksum digits in addresses to detect mistyping of the addresses.
- Perform version number in addresses to differentiate between similar blockchain implementations or the environment.
- Apply Base-58 encoding to addresses to avoid mistyping of the addresses.
- Use the hash algorithm to addresses to reduce the address sizes.

Chapter 12 – Vanity addresses

A vanity address is a public address where the part of the address is chosen by the address holder. Basically, Bitcoin addresses that have a custom prefix within. To better understand let's take a look at a bitcoin address.

1555JSudJlo9HYPLMbbriwoYdFQawszx6SBgIndkshhe

Here the vanity numbers are 555; however, you cannot start your Bitcoin address with the same numbers as every single Bitcoin address always starts with the number 1 as the first prefix. However, you might choose to have your vanity letters at the end of your address, like the example below:

1JSudJlo9HYPLMbbriwoYdFQawszx6SBgIndkshheCAR

To generate vanity addresses yourself, there are many platforms that you can do

so; however, there are few things to note here.

If you want to have vanity letters or numbers that are between one or three characters long, those addresses can be generated quickly. However, if you choose to have a vanity address that is four or more character long, the procedure could take as long as hours or even days to generate. It is not necessary to create a vanity address; however, I will provide some reasons why you might choose to use a vanity address.

- Branding: Vanity addresses can be ideal for organizations, as well improving brand recognition for businesses.

- Business model: You might choose to use some part of the address as services that you offer to your clients, for example using the word: CarHire within your address would stand out, making clients recognize your business as more professional than an average car hire service.

- Donation purposes: Again, same as using for business name or services. If you want to use a Bitcoin address for donation purposes, you may choose to reflect that within your address, so that it would be visible to those who transfer to it.

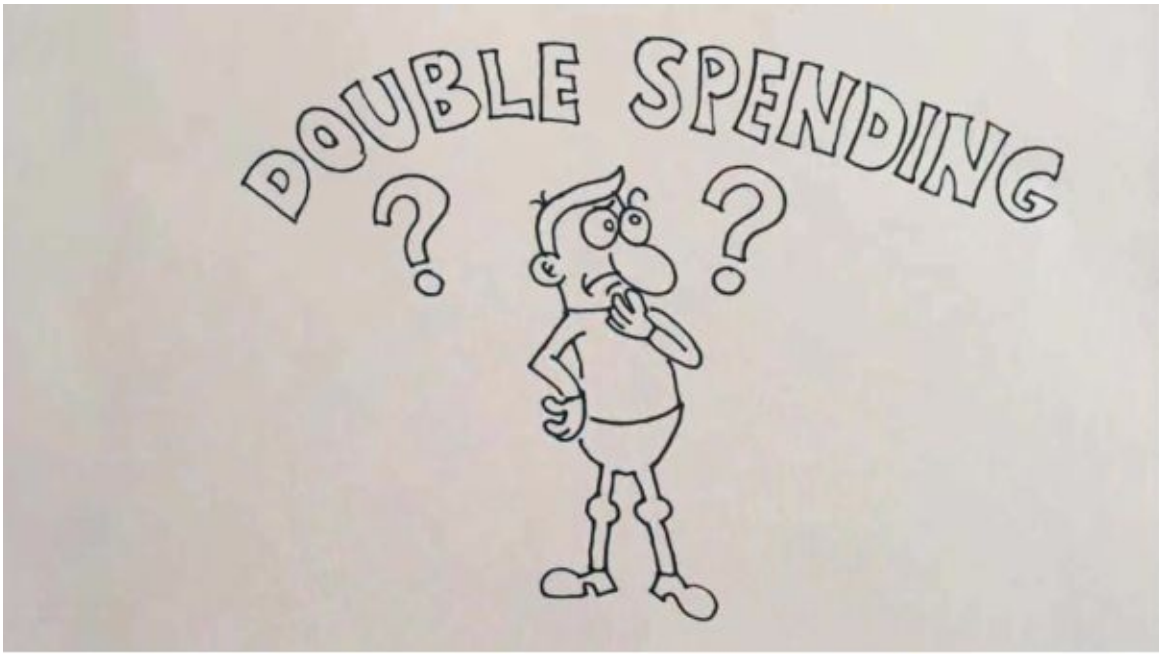
When the vanity address is generated, only the public key (also known as a bitcoin address) is custom. The private key would remain random. In theory, the entire address can be custom; however, it is infeasible to generate an address with the prefix of over 6 or 7 characters.

Some websites will create vanity addresses for you; however, do not use any of them unless they use split-key generation incorporated. This function is where they would generate a public and private key pair, and you would give them the public key. Next, they would create a vanity address with your public key, as well another key pair. Using this technique, the service that would create a new vanity address would only know some of the private key needed to use Bitcoin. In case they do not use this technique, then it is possible that those services would be able to steal any Bitcoin stored on that address.

Some issues regarding vanity addresses that are good to know. For example, as I mentioned, anyone can create a vanity address, that is nice. However, hackers—or anyone with bad intentions—might also know that fact and would try to use it to their advantage. What a black hat hacker would do is simple really: they could use your legit company or donation name within their Bitcoin address and try to receive funds by impersonating you or any business that has good intentions. Another downside, again, is that longer prefixes could take a long time to generate.

Chapter 13 - Blockchain is a money

Well, blockchain is not exactly money; however, when you think about what money is really, I am sure that you have to think carefully to answer. Sure, there are simple answers too, and having to define what money is, using one word, what comes to mind is this: payment.



That's right; money is a sort of payment in exchange for a service or an individual product. Now that you know that money is some kind of payment, let's think about the value. Certain products have different values in different countries; and to separate boundaries and measure the values of each product to different countries, some regulations can be purchased and what not all over the world. Blockchain has no limits: as it's running on top of the internet, which is accessible from anywhere in the world.

However, when it comes to electronic payments, there are issues and a big one is double spending. Back in the early 80's e-cash was conceived as an anonymous cryptographic electronic money. The way it worked, in a simplified explanation, is this:

Banks created an electronic money, that was cryptographically signed. The digital money contained a unique ID, also known as a token. Users were able to purchase these funds, then begin to spend it in shops. What happened was that e-cash was relying on a third party to get authorization, or some kind of proof, that the e-cash was valid, and it had not been spent previously. It sounds like it doesn't make any sense; however, because electronic files are easily duplicated, banks were required to check on all e-cash to make sure they hadn't been spent yet.

Double Spending problem

The double spending problem is the main issue that needed to be solved to introduce a new electronic money system. The problem could have been solved by using a central trusted third party online, who could verify that the electronic cash has not been spent yet.

Back in the day, the idea was that this trusted third party could be anyone like: a bank, broker, or any entity that can facilitate interactions between two sides who both trust the third party. Of course, there are plenty of disadvantages for trusting in third parties; in fact, in any financial services.

In the 2008 financial crisis when several banks failed, it taught us there is no such thing as a trusted third party. They failed mainly because of mismanagement, or greed—or even many because of involvement with illegal bank activities. Additionally, half of the adults around the world have no access to financial services because financial institutions are too far away or too expensive to use. Third parties are commercial entities; therefore, they will charge fees for their services.

If you think about inventing a new electronic money, one of your goals should be to make it accessible to anyone around the world. Third parties have the power to suspend customers' accounts. For example, a few years ago PayPal suspended WikiLeaks donation account and froze its assets. PayPal claimed WikiLeaks encourages others to engage in illegal activity. This was not a result of legal process, but rather the result of fear of falling out of favor with Washington. Third parties can also deny or limit access to your assets. For example, in 2015 in Greece, the banks had limited access for cash withdrawal because of the rush on the banks.

Double spending solution

The solution for double spending without third parties now exists; and that is what blockchain allowed for Bitcoin. Bitcoin was the first application to solve the double spending problem without the use of third parties, or any involvement with any centralized system. Satoshi Nakamoto came up with the idea of Bitcoin and created its original reference implementation. Therefore, Satoshi has solved the double spending problem using a technology that is called today Blockchain Technology. The system is based on cryptographic proof instead of trust. Blockchain technology was originally used as a cryptocurrency for the payment transaction between two parties, but nowadays it can be used for many other services such as:

- Notary Services,
- Identity services,
- Voting services, and so on

Chapter 14 – The great Ledger

The ledger is a sort of database where confirmed transactions are recorded. Traditional centralized ledger systems work in a very similar way as the Blockchain ledger system; however, there are few differences.

Centralized ledger:

An old way of doing a ledger system that is centralized by a bank. For example, it works like this: if you purchase from me, you pay me; really, you would only initiate a transfer from your bank account to my bank account. Then both of those banks, if they are not the same, would have all the details of the transaction registered. However, only those two banks would be able to access those transaction details, therefore, no other banks, nor anyone else, would have access to those details.

If someone wants to have access to see the details, they need to ask the bank for authorization first. Of course, it all depends on what is the reason for the access. But the point here is that this traditional ledger system is still working in the same way. There are several different kinds of ledger systems; however, when it comes to Blockchain's great ledger system, it's not centralized. It resides on the

peer-to-peer network; therefore, it’s a decentralized ledger system.

Distributed Ledger:

Blockchain platforms do not use a centralized database; instead, each node has a copy of the ledger that resides on the peer-to-peer network. Cryptocurrencies, such as Bitcoin ledger, only store balance information in the distributed ledger. However, other platforms can, in fact, are already storing other information. Blockchain platforms, such as Ethereum can store any information in the distributed ledger. Some examples are:

- Identity information
- Patient information
- Real estate information, *etc.*

This method is also known as a public ledger, or permissionless ledger. When there is no central authority managing access to the ledger, this ledger is called a public ledger or, again, a permissionless ledger. So basically, you, or anyone, could join to the existing peer-to-peer network (for free of course) and receive a copy of the ledger of all existing transactions that have ever been recorded on the blockchain. This would date back to January of 2009 when the great ledger began to work for the first time. As you can see, this is completely the opposite of what the current banking systems are providing.

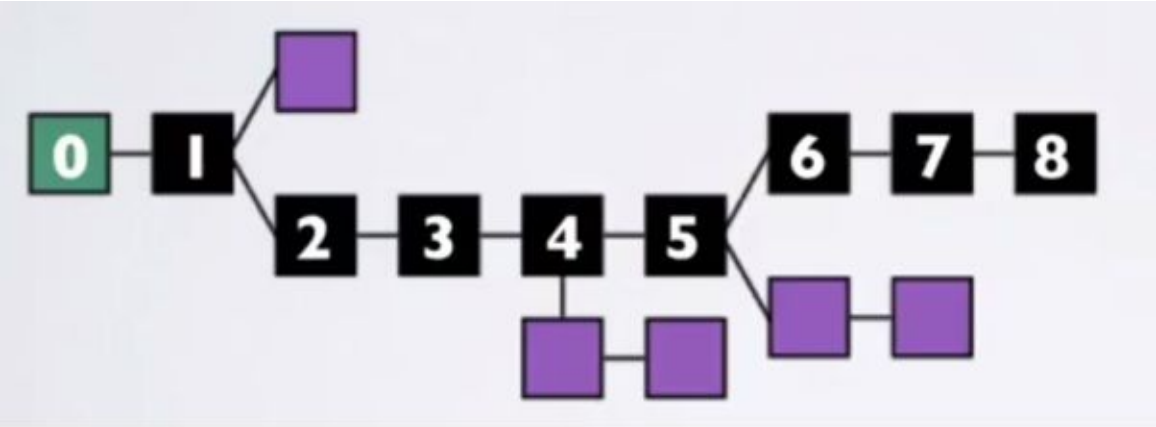
Private Ledger

When there is a central authority managing access to the ledger, it’s then called a private ledger, also known as a permissioned ledger. This is of course not a peer-to-peer network, and you would have to ask for permission from the central server to have access to a copy of the ledger.

The blockchain ledger is visualized as a series of blocks which are connected with each other. Each block is made of a header, containing metadata, such as its previous block hash, Merkle root hash, and nonce. Followed by a list of transactions. The blocks are connected with each other, by referencing each of its parents' block hash.

Chapter 15 – The Blocks

All blocks in the main chain are numbered, starting with the number 0, then 1, 2, 3, 4, 5, and so on. The green block is the first block that was created, and it's also known as a genesis block, and it has a block number zero.

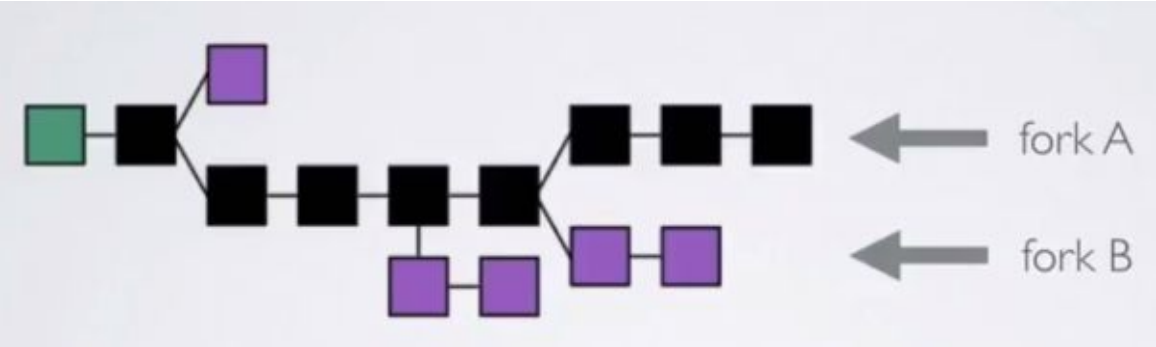


The purple blocks are the ones that are forming short and invalid chains, they are called blockchain forks. Blockchain forks do occur very often, additionally these side forks, also known as orphaned forks.

A Bitcoin block is created every ten minutes on average; however, Ethereum blocks are set up in every 17 seconds on average. The block height is the sum of the blocks in a chain between it and the genesis block minus 1. Blocks on side forks can have the same block height as blocks on the main chain. Particular nodes on the peer-to-peer network are creating these blocks. These nodes are called miners. All the miners are collecting every transaction that people are sending to each other over the network, and only valid transactions are relayed to the other nodes. Each miner takes a number of these collected operations and puts them in a newly formed block. These lists of transactions are numbered tx0, tx1, tx2, … and so on. Tx stands for transaction, followed by the number. The first transaction (tx0) is also known as the coinbase transaction. This is the transaction where the miner assigns a block reward to his address. This is how Bitcoins are created. For Bitcoin miners, as of now in 2017, the block reward is 12.5 Bitcoins; however, back in the day of the genesis block, the reward was 50 bitcoins for each block creation. For Bitcoin, the block reward is halved after every 210,000 blocks. Once there have been 64 halvings, the block reward will be zero. There will be a maximum number of 21 million Bitcoin in circulation in

the year of 2140. Other Bitcoin transactions, such as tx1 or tx2, are the ordinary transaction where the bitcoins are transferred from the owner address to a recipient address. Each transaction requires a small transaction fee. This fee will continue to increase as an incentive for the miners to create new blocks because the block reward will continue to be lowered.

When the miner has constructed the block, he must solve a hash puzzle that is applied on his list of transactions. The miner who first solves the hash puzzle is allowed to broadcast his block on the peer-to-peer network. The block also includes the solution to the puzzle, also called the nonce, in the block header. This is, of course, available to anyone who wants to see it and the details for each block can be found at www.blockchain.info Other miners on the network will receive this block, and they validate the block before they append it to their chain of blocks. It happens regularly that another valid block is broadcasted on the network because another miner has solved the puzzle nearly at the same time.



When this happens, temporary forks are created. For example, fork A and fork B. Let’s assume that 70 % of the miners on the network are working on fork A, and the rest of the miners are working on fork B. In this example, fork A becomes the main chain because it consists of the longest series of blocks from the genesis block. Miners should always work on the longest chain. In this example, blocks on fork B will become orphaned blocks.

The miner who solves the hash puzzle, and his block is on the main chain, will receive the block reward and also all the transactions fees (tx1 and tx2) in this block. The miner who has solved the hash puzzle, and his block is an orphan fork, cannot spend the block reward and transaction fees, because his block is not on the main chain.

Chapter 16 – Platform testing

Due to the scaling transactions, the original blockchain that was created back in 2009 requires certain maintenance. Back then, there were only a few transactions; however, as of mid-2017, there are close to 150,000 transactions every day. That means more than 6,250 transactions within an hour, which comes down to 105 transactions in every minute, meaning nearly 2 transactions are happening every second.

I hope you can understand that the system does require updates to make sure all those transactions can be handled by the network. There are already plenty of blockchain jobs on the market, and if you have good programming skills, you could become a great blockchain engineer.

Blockchain developers are highly paid; here in the UK, a permanent blockchain developer pay rate starts from 80K to 150K, even 300K per year, and I am talking about pounds, not dollars. The problem is that only a few people understand blockchain, as the knowledge of technicality required can be overwhelming and certainly not for everyone. Having a bit of knowledge on C++, SQL, or Python could be very advantageous, and if you are into learning

these programming languages, it will pay off. Two decades before, everyone was on about that IT is the future, and learning such skills will be needed for most future jobs. It is certainly good to have some IT background, especially if you are planning to become your own bank; however, let's be specific for a moment. Learning IT skills can mean many things; so, you should be specific, and specialize.

I can easily say that the future jobs that will pay off big time are software developers, or to be more accurate, Blockchain developers. Where to start? Get an online course on Python programming for beginners, along with a reference book. But before I start a whole new topic on programming skills, let me explain a little bit about what environments current blockchain developers are using for testing purposes.

Testnet:

A testnet is an alternative blockchain used by developers for testing purposes. The crypto coins mined on the testnet, also known as testnet coins, have no real value. A testnet offers developers a sandbox environment to experiment without having to use the actual crypto coins or worrying about breaking the main chain. The main chain is also called, the mainnet. In case you we're wondering about mining bitcoin, this is it. You can quickly mine your own Bitcoin or Ethereum testnet coins by setting up your own Bitcoin or Ethereum node.

There are fewer miners on the testnet, and the hash difficulty is also low enough to find solutions easier for solving hash puzzles—as well—getting a block reward. The mainnet and testnet are two individual networks, and there is no availability to send coins from one platform to another neither vice versa. To work on the Bitcoin testnet, you need to generate a differently formatted testnet Bitcoin address. A Bitcoin testnet address always begins with the letter m or n. The Bitcoin testnet address does not work on the mainnet.

However, when it comes to Ethereum, there are no differences between testnet and mainnet. The same address will work on both networks: testnet as well mainnet. Therefore, you must be very careful not to mix them up.

Faucets:

There is another way to get testnet coins, and that is to search for a Bitcoin faucet or an Ethereum faucet. A faucet is a website that dispenses small amounts of testnet coins on your address in exchange for completing a task described by the site. You can easily google search both: Bitcoin faucet, or Ethereum faucet.

Chapter 17 – SegWit

As I just explained some testing tools for developers, let's see what else is out there that requires maintenance when it comes to the real blockchain network. SegWit stands for Segregated Witness. SegWit can be explained in many ways, and its technical details can be very confusing for some; therefore, I will try to explain simplistically before really diving into it.

SegWit is a change on the blockchain network, more specifically it's a change within the blocks. I am a network engineer, and it's easy to say, that when it comes to a decision of making a change, especially within the production environment, it is because there is an issue that needs to be addressed. The problem currently with the blocks is simple. Each block can handle 1MB of data, meaning all transaction details.

Once there is enough data within a block, the block gets sealed, and miners start to create another new block. The issue that needs to be addressed is that each block gets filled with some data, but indeed it has been identified that there should be more data within each block. I have explained previously that each block contains lots of data, in fact, every transaction details are recorded on the blockchain, specifically, within the blocks. Data such recorded are the block

number, destination address, source address, transaction value, hashing algorithms, and so on; however, one of the most important data recorded, is the actual script that contains the digital signatures as well the public keys. To have a block validated on the blockchain peer-to-peer network, these parts of the blockchain rules had to be within the script. However, it has been identified that the current situation is slowing down the system, and an upgrade is required. This scaling issue needed to be addressed; therefore, blockchain developers came up with an idea.

Solution:

The solution is called SegWit. However, the real plan to implement SegWit is to remove the script from the blocks, making the blocks lighter; therefore, leaving more space for additional transactions, as well, speed up the system. However, the proposal has a possible side effect. The reality is that the script is still going to be required as the rules of the blockchain cannot be changed, therefore, part of the proposal is that there will also be an extended block that will have the script. This is of course very confusing for many, especially for those who have no technical background. The other problem is that developers are not sure if it's going to work out ok or not: even though they believe it is needed, hence the change proposal in the first place. Still, we only can find out once implemented. This solution is a solution for many other issues too. One is that each transaction fee is very cheap; however, it could be even less expensive. What you have to understand is that bitcoin is an excellent digital currency when it comes to values such as $100 worth or more. However, in order to implement it worldwide in every store, it requires some upgrades.

For example, if you make a payment using Bitcoin that’s worth $100, the transaction fees could cost you around $0.30 cents. However, when you want to buy an espresso from your local coffee shop that costs a dollar, a $0.30 cent transaction fee could be just too expensive. So, what has been identified is this: If we could add more transactions to each block, like twice as much, that could mean that each transaction would cost half of what it is now. However, in order to fit more transactions to a block, something has to be removed. What has been discovered, is that the script can be re-written and added to an extended block on the original block, and this would be called Segregated Witness aka SegWit.

Why is it called SegWit?

The witness is also known as Cryptographic proofs, and the signatures that are used are also witnessing the proofs. Separating the signatures from both the transaction data structure and the block data structure into their data structure. Taking the signatures out of the transaction data structure is the main reason; however, there are some side effects, so let’s take a look at them. First, side effects are not always bad, in fact, regards to SegWit, there are some very positive outcomes possible.

The original goal was to clean up some of the functions of Bitcoin. One thing that is not static within the transaction data is the digital signature. To be fair, everything else is covered by the signature, therefore, cannot be changed effectively, unless invalidating the signature; however, the signature itself can be malleated. So, once the signature would be taken out of the transaction data, the transaction ID would not be based on the signature anymore.

The transaction ID’s hash is not based on the signature, which means that the transaction ID cannot be malleated. This, in itself, is a massive development, and it helps with chaining transactions, additionally helps with lightning networks, as well payment channels and it will resolve lots of problems that we currently have with transaction malleability.

Transaction malleability:

In simple terms, transaction malleability, is a cork in Bitcoin, and other cryptographic systems, where you can make unauthorized changes to transactions and re-broadcast with a different transaction ID. You cannot change where the funds are coming from, neither where the funds are going, because the signature covers that; however, you can make small modifications to the signature.

Let’s think of this in simple terms. Let's say that the signature contained the number 5. The analysis of the algorithm 5, and 05 are the same, but if you pad a number in a certain way, it will change the fingerprint of that transaction, even if that signature is interpreted the same way. Therefore, you can modify part of the signature because they are not covered by the signature and they would produce a transaction with an entirely different ID. By doing that, you can jam it into the

network and cause confusion. Transaction malleability has been blamed for some thefts and Bitcoin exchanges, where people mostly are getting a form of double withdraw, using transaction malleability. It also allows you to carry out a DOS – Denial of Service Attack, against the network; as well, against the people who are using payment channels or chaining many transactions together.

How does SegWit allow more transactions on the network?

One of the interesting side effects of SegWit is that you can start counting block sizes differently and give some capacity to increase directly through the SegWit. Transactions are the key to opening the door to get into the blockchain; therefore, you need a signature on the transaction to be validated to the blockchain. However, once the transaction is in the blockchain, nobody checks those signatures ever again; typically we do not go back to see old transactions that happened a long time ago. They're only buried within the blockchain. They have been validated: therefore, old transactions are already trusted. The signature is only used once for validation. For example, when you write a paper check, you have the option to go to your online banking system and look at the image of the check after it has been submitted and cashed. It's not part of the bank statement, and you don't need it for anything other than to check it once to see that it was validated; after, it's only hanging around, no need for it anymore. Same thing applies to signatures. What you have to understand is that digital signatures take 75% of the total space of some transactions. Additionally, the more transactions there are, the bigger the signature gets. Large complex scripts and multi signatures have huge signatures, and they take up a lot of space on the blockchain, and, again, nobody ever cares about them once they have been validated.

The other part of the SegWit wasn't considered until recently because fixing malleability and removing transaction signatures from the transaction data is something that requires considering the whole network, and it's been assumed that it needs a hard fork. However, there is a way to proceed using soft fork instead of hard fork. Indeed, it's a fascinating trick. This method allows you to put a version number in front of the Bitcoin script. What that does, is allows you to upgrade the version number of the script, while old clients cannot see the difference, but still able to validate transactions entirely. Former customers can

continue to operate without upgrading, and all that is different is that they are endorsing a little less they used to do before. Additionally, new clients can upgrade scripts. Once you have a new version of a script (this is awesome) as you can introduce endless amounts of soft forks parallel to change all kinds of scripting mechanisms. This trick is not only good to use for SegWit, but all other kinds of new developments. This is accelerating the innovation in the scripting language. Altogether these aspects: Segregated witness, Transaction malleability, increasing the capacity of the block by removing lots of information that's not used after validation, and the same time upgrading version scripts—make a truly compelling feature and resolve lots of problems.

Chapter 18 – Soft fork VS Hard fork

First of all, let me explain a little about soft fork activation. It is usually done by a voting process, yet there is another innovation that is called Version Bits, also known as BIP 9, that was introduced in parallel and allows you to have multiple soft forks.

What it allows you to do is say if a certain bit in the version of the block set, meaning you want to implement this soft fork, the miners then set that bit. Once 75% of the blocks have that bits set, you are activating the feature, then once 95% of the blocks have the bits set than that feature is forced for validation. It's a two-step voting process.

It has been done on multiple occasions, such as Check Lock Time Verify. These incremental features can be voted on parallel. Previously, they had been implemented by increasing the blocks and by upgrading block version. For

example, updating block version 3 to block version 4, and so on.

However, now you can turn the block version into a block field; therefore, you can do all these in parallel. Previously, it was that only one soft fork could have been implemented at the time, and the vote had to be completed by the way. It is hard to accept one, dismiss another, and move to the next. However, with the new proposal, you can implement multiple soft forks simultaneously.

The important feature of the soft fork is that it’s forward compatible. In simple terms, let me provide an example for better understanding. Imagine that you want to open an old Microsoft word document. Word 1998 documents can be opened with the current version of Microsoft Word. This is what backward compatibility is, meaning it recognizes old formats.

On the other hand, forward compatibility is when the version of Microsoft Word from 1998 that has not been upgraded would still open a document that we use today, or at least in a certain way. It may not be able to see all original details correctly, and may not be able to understand some of the features; however, it still would be able to open the document. Therefore, soft forks have forward compatibility, meaning that clients who have not yet upgraded to the new code will not break and won’t stop validating so they can still maintain validating on the current consensus chain. All there is, is that they are validating less information because they may not be able to see the new features; however, they can ignore them while validating.

Hard fork, by comparison, means that if you do not upgrade, you can no longer approve blocks, and you are no longer part of the consensus chain, therefore, if you don’t upgrade, you are not on the network.

Overcoming risks:

There are always risks, especially when looking at compatibility. As I mentioned before, any change to the system apparently will cause effects. Soft forks, hard forks, they all have bugs, even though all these features are always tested on Testnet. For example, segregated witness testnet had been running for months before implementation, and that allows to have more faith before any change. Miners have become very concerned about any change and making sure there are multiple tests before any implementation takes place. The general belief is that soft forks are less dangerous than hard forks, but the problem that some people identify is that they do not force the network to upgrade, meaning you can end up with lots of old clients that validate less transactions. However, some other developers prefer to have more of a strict approach, and just believe that if you don’t upgrade, you should be off the network. Therefore, it’s more like a philosophical issue rather than technical.

Chapter 19 – Lightning Network

Lightning network is a Layer 2 network, also known as Data Layer network. It aims to scale peer-to-peer networks from millions to billions of transactions per second, simultaneously using smart contracts. For example, getting paid not monthly nor weekly, but every second. Exciting, right? I'm sure you would love that too! Imagine checking your online pay slip and seeing it always changing, showing you a different amount every second. But first, let's look at why the idea was born in the first place.

Transactions are slow

Receiving payments monthly is obviously ridiculous. I used to get paid weekly before and that's a lot better; however, I've also had many jobs before where I used to get paid daily. Getting paid daily is what I most liked; however, I was on a cash to hand basis, and it was not recorded anywhere; therefore, I cannot account for those days. Using blockchain, especially lighting network, can allow you to receive validated payment simultaneously, which is registered in the great ledger forever.

As an employee, I believe it's a nice way to get paid; however, think from an employer point of view. Imagine that you have a company that employs

thousands of people. Each month people are working on pay slips, making sure everyone will get paid correctly, and still before any validation, it has to go through the bank, in fact, many banks, to get everyone paid. Therefore, lightning networks will be the favorite of every employer.

Now that you have a good knowledge of how blockchain and Bitcoin works, when it comes to lightning networks, it's actually bending the rules a little bit. Let me explain why: we know that when we send a Bitcoin, we broadcast the transaction, then we have to wait for confirmation, and confirmations are only arriving every 10 minutes in the form of a block.

Once the block has been created, it groups many transactions, and it will get registered on the ledger. However, if you are waiting for the next confirmation, you have to wait for the next block to be validated, that might take another 10 minutes. Because a lightning network works on top of the existing system, only using a different layer, it has its own layer for instant payment.

Transactions are expensive

The Lightning network promises no fees on the transactions. Again, this is new, simply because each transaction has fees that sometimes are even larger than the previous transactions were. Fees are for making your transactions a priority within the list of other transactions. The more fees you would pay, the faster you would get the confirmations. Paying no fees sounds like you are possibly never going to get confirmed by the network.

Solution

You must think of it in simple terms. Imagine when you go to a Pub where the waiter tells you that you have to pay cash, or if you choose to pay with a card the minimum order has to reach $5. This is because for each transaction the pub needs to pay a certain fee to the provider. However, if you open a tab, and you pay only once, in the end, there will be only one transaction fee that requires payment.

When you create a payment channel on the lightning network, you have to deposit a certain amount of bitcoin. Now you are proving ownerships for those

bitcoins by handing them over to the network. It also works with multi-signatures. The system has a way of enforcing these sets of rules; therefore, you don’t even have to wait for the block to be confirmed. Once the transaction has been announced, it’s is immediate; hence, you don’t have to wait until these funds are approved.

As we do not force the miners to write these transactions on the blockchain, as normally, you would have to pay the miners for transaction fees. This system allows you to make many payments; however, you only have to broadcast it when it’s necessary. At the current stage of August, 2017, we already know that the concept works; however, this software is still under development. It is highly complicated to implement, therefore, it is still going to take some time. Any bug in the code can cause a catastrophic outcome; thus, there is not a fully working resolution yet.

Conclusion

I hope that you have grasped a little of what the blockchain attributes are, and how complex the system is. I will write another book shortly and explain Bitcoin in more depth, and how to invest securely and safely.

Overall, what you have to understand is that blockchain and Bitcoin are not the same things. Blockchain is a technology, and its first application was on the platform named Bitcoin. Bitcoin is blockchain. However, Bitcoin itself is only a cryptocurrency that is capable of replacing fiat currencies. Nevertheless, not that many people will like the idea at first. Blockchain has solved the problem that we have always faced, that is trust, using Elliptic Curve Cryptography and a huge amount of computation power. Using blockchain technology enables us to avoid trusting third party services, by replacing them with digital signatures, and mathematical algorithms. Therefore, any payment or exchange over the internet will be between 2 parties only. This is revolutionary as we can expand the trust gap, and the market of the future not only will be faster and cheaper, but will have no limitations, such as age, race, sex, occupation, nationality, or anything like that.

If you tell your friend, who has never heard of blockchain and thinks that he or she is not affected, try to explain that everyone is affected by the blockchain: • Person to Person

- Business to Business - B2B
- Machine to Machine - M2M

Although blockchain will not take over the world from one day to another, and it might require a decade, or two. However, everyone is affected.

Blockchain is also known as the future of money; even though streaming money sounds weird to some, it not only will happen—but has already begun for nearly a decade, and will not stop, especially using a new protocol called Lightning Network. Data protection using blockchain will be very secure and always will provide the truth, using a fully decentralized peer-to-peer network, data will always be available.

Because this high technology enables us to become our own banker, we might

not require having banks anymore in the future; still, because we have to look out for what we have, certain IT skills will help us to be safer from cyber criminals. Once you understand how easy is to keep your valuables safe online, you also will realize that it is even easier than opening a bank account.

Therefore, the changes for the young and the next generation will speed up the process of learning about the crypto world. Of course, some people may have to learn the hard way, as many people have been hacked and only after begin to invest in learning and implementing security. Still, the time of Blockchain has begun, and it will change the world.

Average people, with no technical background, wouldn't believe it, and probably say that blockchain itself isn't capable of anything. However, software developers, security experts, large financial institutions, FinTech start-ups, and banks, already have paid a keen interest, as well as have begun to invest and create their protocols. Intel, Microsoft, Cisco Systems, Dell, and many more large, high-end technology firms, are already all over the blockchain and its little intricacies. Therefore, the days are counting to reach the big bang of the transformation, the technology of the future, or, I should say, the next internet!

Thank you for purchasing this book. I hope this title has provided some insights into what is really behind the curtains when it comes to the future of money and doing Business either with people or machines. I have tried to favor every reader by avoiding as many technical terms as possible on how the Blockchain works; however, this is an advanced guide, and some instances were just impossible to do so. My upcoming book on Bitcoin will provide more details on how to invest in digital gold safely and securely.

Additionally, I will touch on Cryptocurrency trading, and how to recognize the right time when to invest in Bitcoin, or any other Cryptocurrency. I will also provide guidance on how you can become a miner by renting equipment, as well, how you can start mining digital money using your laptop, or even your Android phone.

Lastly, if you enjoyed the book, please take some time to share your thoughts and post a review. It would be highly appreciated!

[A1]I assuming you meant won’t from the context