CRYPTOCURRENCY MASTER BUNDLE

THE ART OF HODLING
CRYPTO MINING MINDSET
THE ICO APPROACH
CRYPTOCURRENCY 101
BLOCKCHAIN DYNAMICS

Five Books in One!

MARTIN QUEST

The Crypto Master Set

The Art of HODLING

A Beginner's Guide to Cryptocurrency Trading and Investing

+

The Crypto Mining Mindset

+

The ICO Approach

A Beginner's Guide to Understanding Cryptocurrency ICO

+

Cryptocurrency 101:

Your Guide to Understanding How to Trade Bitcoin, Altcoin, and other Online Currencies

+

Blockchain Dynamics

A Quick Beginner's Guide on Understanding the Foundations of Bitcoin and Other Cryptocurrencies

Martin Quest

Bonus!

Wouldn't it be nice to know when Amazon's top Kindle books go on Free Promotion? Want more insider info with Crypto?

CLICK HERE FOR INSTANT ACCESS!

Simply as a "Thank you" for choosing this book, I would like to give you access to an exclusive service that will email you notifications when Amazon's Top Kindle Books go on free promotion, as well as offer you an INSIDER GUIDE to more crypto strategies. If you're someone looking to go to the next level in your crypto success, simply click the link above for FREE access!

permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are the owned by the owners themselves, not affiliated with this document.

Table of Contents – The Art of HODLing

The Crypto Mining Mindset

The ICO Approach

Cryptocurrency 101

Blockchain Dynamics

Introduction

Cryptocurrencies have become all the rage over the last few months, especially after the meteoric rise in the price of Bitcoin back in December 2017. It used to be that cryptocurrency investing was the realm of experts and savvy investors. But because of Bitcoin's massive success and popularity after December 2017, things have changed. It has now expanded to include even the smallest and least experienced of investors. Before going into the details of hodling and cryptocurrencies in general, it would be very beneficial for you to get a glimpse of how cryptocurrencies became what they are now.

Brief History of Cryptocurrencies

It all began in the 1990s when American cryptographer, David Chaum, created what was considered as the first kind of online money in the Netherlands: DigiCash. He created DigiCash as an extension of an encryption algorithm that was considered popular during those times, which was RSA. The technology he created, together with its eCash product, was able to generate a huge amount of attention from the media. It became so popular that Microsoft Corporation tried to buy DigiCash for $180 million with the intention of placing DigiCash on every computer in the world that ran on the Windows operating system. One of the crucial mistakes Chaum and his company made was to reject Microsoft's $180 million offer and earn the ire of De Nederlandsche Bank (Netherland's Central Bank), which was the Netherland's primary monetary authority. All of those crucial mistakes eventually led to the demise of DigiCash in 1998, when the company went bankrupt.

The second generation of Internet money was borne from the learning experiences of DigiCash. Companies from this generation came up with alternative payment solutions and money systems

that were also Internet-based but with small but important changes. Of these companies, the clear winner was PayPal. The reason why PayPal trumped its competition was its ability to give users what they really wanted in the first place, which was money on the web browser platforms they were already familiar with. PayPal - unlike its peers back in the day - was able to give its users the ability to transfer money to and from merchants and buyers, respectively, using a seamless peer-to-peer money transfer system. PayPal's massive success is very obvious by the fact that next only to credit cards, it's the most popular means by which to transact online.

But wait - there's more! PayPal's success led to other companies emulating it. One of the systems that tried to walk on the same path as PayPal was e-Gold. Unlike PayPal, its primary currency was gold, i.e., it received physical gold as deposits from its users and in return, it issued e-Gold or gold credits. E-Gold was able to manage a relatively healthy amount of cross-border transactions using gold. But because of the prevalence of fraudulent investment scams like Ponzi schemes, e-Gold was closed.

The next significant event in the history of cryptocurrencies is the 2008 subprime mortgage crisis that nearly crippled the financial system of the United States and affected many of the world's major financial institutions. This event served as some kind of wakeup call to many of the world's major economies and has led to the emergence of what is now popularly known as the blockchain, which is the foundation of cryptocurrencies today as we know them.

In 2009, an anonymous person (or group) that went by the identity of Satoshi Nakamoto published a white paper that expounded, among other things, the source code, technology and concept of what is now called the blockchain. And together with the blockchain, he launched the granddaddy of all cryptocurrencies as we know it; Bitcoin. The blockchain, while not an earthshattering, disruptive or incremental technology, was considered a foundational one. Why

foundational? It's because it was meant to - and it still does - serve as a bedrock upon other data network storage technologies can be built. The blockchain naturally challenges all the conventional online data management protocols of that time, which included centralization of data.

Today, there are more than 16 million units of Bitcoin that are circulating in the digital financial system and these have a total market capitalization of around $50 billion. More importantly, Bitcoin's already garnering increasing acceptance and support from both the I.T. and business communities alike. As part of its gradual integration into the financial mainstream, some economic powerhouse countries like Australia, Canada and Japan have already begun regulating Bitcoins through tax and legal measures.

Since 2009, the growth in the popularity of the blockchain and Bitcoins has surged. This surge in popularity gave birth to other cryptocurrencies, which are referred to as altcoins or alternative coins to Bitcoin. Today, there are more than 850 cryptocurrencies in the digital financial system being transacted internationally, which include Ethereum (Ether), Ripple, Litecoin, Monero and Stratis. And if you combine the total market capitalization of all altcoins with that of Bitcoin, the result would exceed $100 billion.

Because of the massive expansion of cryptocurrencies, it appears that cryptocurrencies have created an entirely new and global industry. Because of the massive advances in the blockchain technology, as evidenced by the growth in the number of cryptocurrencies on the market today, newly developed apps that will be created upon the blockchain technology will naturally use cryptocurrencies. And as more and more cryptocurrency platforms and exchanges start to emerge, more and more people will be able to use blockchain-based apps, which in turn will make the latter industry grow even more.

Ethereum

When talking about the history of cryptocurrencies, a discussion of the second biggest and most established cryptocurrency - Ethereum - can't be ignored. Ether - as it's more commonly referred to - is an open source blockchain platform that features among others, a collection of programming languages upon which other blockchain apps can be built (Decentralized Apps), the Ethereum Virtual Machine, and smart contracts.

Ether's a relatively young altcoin compared to most other major ones, having been created only in late 2013, by a dude named Vitalik Buterin and publicly launched in July 2015. But considering its relatively young age, Ether has been able to garner unmatched support from the business, consumer and developer communities because of the massive promise it has shown. Its market capitalization has already exceeded $30 billion and because of its open source nature, Ether has made it possible for a lot of startup companies to create their own cryptocurrencies on its platform. And Ether's popularity is expected to increase even more because of its trademark Enterprise Ethereum Alliance (a group of international and cutting-edge businesses that both use and assist the Ethereum platform), its technological advantage over all other blockchain platforms, its relatively huge developer community, and its relatively easy development.

The Future of Cryptocurrencies

One of the main motivations that fuel the development of cryptocurrencies is the breaking down of existing financial and technological barriers and borders, particularly in the realm of trade and finance. More than 1,000 altcoins are vying with each other in terms of early blockchain developmental stages. As a result, we can reasonably expect to see only a couple of successful

cryptocurrencies to stay and change the way we will pay, lend money, borrow money, trade, and do banking in the future. And in the near future, we can reasonably expect several major cryptocurrencies to be accepted in the financial mainstream, which can signal a whole new era of digital finance.

HODLing

The main topic of this book is hodling. But what does hodl mean? The first instance when this term was used was in 2013 at the Bitcoin talk forum. One of its members with the handle GameKyuubi used the term hodl under a thread named "I Am Hodling." It appears from the post that while trying to convey his conviction of holding on to his Bitcoins despite how its prices nosedived at that time, he was drunk. As a result, he seems to have misspelled the world "hold" as "hodl." And it seems to have caught on with a lot of people because the word has become very popular in the cryptocurrency industry to the point that many cryptocurrency traders/investors use it to communicate the idea that they're holding on to their cryptocurrencies regardless of what happens. And what was once considered a typographical error has since evolved into a funny acronym: Holding On for Dear Life.

How to Use This Guide

This book is meant to help or guide you to increase your chances of successfully hodling cryptocurrencies, i.e., making good money out of them. After all, there's only one reason or motivation for holding on to financial assets, and that's to earn significant returns from them. Otherwise, what's the point?

This book is divided into 5 parts; a discussion on the nature of money or fiat currencies, what makes cryptocurrencies work and worth investing in, general principles for safely holding your Bitcoins or other cryptocurrencies, why Bitcoin is here to stay and how to invest in or hodl cryptocurrencies. By the end of the book, you'll be in a very good position to start hodling cryptocurrencies. But the best way to use this guide is to act on the information it gives. Without application, everything you'll learn here is just trivia. This book's value, as well as that of any other non-fiction or self-help book, is in the application of knowledge. So after finishing this book, I strongly encourage you to act on what you've learned.

Chapter 1: What is Money?

To better understand or appreciate cryptocurrencies, it's important to get a good grasp of the nature of money. This is because cryptocurrencies are a form of money and by understanding the true nature of money, especially what important characteristics it should possess, you'll be able to better appreciate and understand the nature of cryptocurrencies. And in turn, you'll be able to better understand the principle of hodling.

What is Money?

At its very core, money is something that is used to represent the value of other things. For example, you gave me money in exchange for receiving a copy of this book, and that sum of money represents the value of this book. The money I received from you and others who have bought this book, I'll use to purchase or acquire something of value from other vendors today or tomorrow. If you study history, you'll see that the values of things have been expressed in different forms and money, the primary way by which values have been expressed has come in different shapes and materials. Case in point, things like gold, shells, wheat and salt have been used in the past to represent value and as a medium of exchange. But for something to be able to continue representing value, the people who are using it must continue trusting that a medium of exchange is indeed valuable and more importantly, its value will persist for a long time so that they will still be able to benefit from it in the future.

How People's Trust in Money Has Evolved

Only until one or two centuries ago, societies had always placed their trust in something when it comes to the value or representation of money. But the way people trust in money has shifted

from trusting something to trusting someone. What do I mean by this?

In the past, people would use - as I mentioned earlier - stuff like gold, wheat, salt and even seashells as a medium of exchange or money. But over time, people caught on to the fact that using such things as a measure of value and medium of exchange can be quite burdensome. Can you imagine buying your groceries with seashells or salt? What if inflation was very high the last several years and you want to buy a month's worth of groceries? Can you imagine bringing that much salt to the supermarket? And if you're the grocery owner, can you imagine having to weigh the salt being paid to you by your customers and needing a very large space and vehicle to store and transport all that salt? And what if it rains? Do you get the picture?

Because of such inconvenience, people were forced to improvise and come up with a more practical value storage and payment solution; paper money! So this was how it worked in the beginning. When you take up a bank or the government's offer to take physical possession of your gold bars for storage, they'd issue you certificates or bills for the amount or value of the gold you deposited with them. Say your gold bars were worth $500, the bank or the government taking possession of your gold bars would issue you a paper certificate or bills worth $500.

Now think about this. Which is easier to carry around - paper bills worth $500 or gold worth $500? Another thing to think about is this. Which is easier to cut in smaller pieces or value, paper bills or a gold bar? If you want to buy a bag of chips for $5, you'd only have to give the cashier five $1 bills, but if you're carrying around $500 worth of gold, you'd have to cut it proportionately to an amount that closely or exactly represents $5.

Another thing worth thinking about back in the day is this. If you wanted your gold bars back, all you'd need to do is give $500 worth of bills or certificates back to the bank or government to

redeem your gold bars. It's that simple. Because of the convenience and practicality it brings, paper money has grown so much in popularity and has become the primary means by which goods and services are bought and sold all over the world today.

Back in the day, the value of the United States dollar was linked or based on gold. The money of the United States of America was valued based on its gold holdings. This was referred to as the Gold Standard. But over time, the macro economy has changed and as a result, the link connecting the value of the United States dollar to the value of gold was cut. As a result, Americans - and the rest of the world, considering the US$ has become the world's primary currency - had been conditioned to shift their trust from gold to the Federal government. In other words, people have been conditioned to shift their trust when it comes to monetary value from something - gold - to someone who assumed responsibility for the value of the dollar, which is the Federal government. And the only reason this system continues to work is trust because let's face it, there's no real underlying asset of worth behind the value of the dollar or other currencies. This was how fiat or paper money was born.

Fiat Money

The word "fiat" is a Latin word that's best interpreted as "by decree." This means that any fiat currency, i.e., paper money, only has value because their respective governments say so. As a result of such legal decrees of value, paper or fiat currencies are also called "legal tender" which means they have to be accepted for payment of goods and services in their respective countries. That being said, you can now see that money as we know it today has value only because of its legal status, which is declared by governments. As I mentioned earlier, the trust in the value of money has shifted from something (gold) to someone (the government).

Now fiat money as we know it now has some pretty serious issues. These are being centralized and are practically unlimited in quantity. Being centralized means that there's a central or lone authority that has the power to issue and control its supply, which in the case of the United States dollar is the Federal Reserve. It's also practically unlimited in quantity because the Federal Reserve has the power and capability to print or mint more units of the US dollar if it chooses to do so. Now, why is this a serious concern?

The reason is one of the most basic principles of economics; supply and demand. To be more specific, this means that when the supply of an object is increased, the value of that object will tend to decrease assuming demand for that thing remains constant. Conversely, when the supply of an item is decreased, assuming constant demand, the value will increase. So if the Federal Reserve or any monetary authority prints more money, it'll flood markets with more of that currency, which can make it worth less, i.e., buy less of goods and services. So when you see the prices of goods and services rising substantially over the long term, it's not necessarily because they became more expensive but because the value of the currency, e.g., the United States dollar, has dropped due to increased supply.

Digitizing Money

The establishment of fiat money has made it easy - even mandatory - to create digital ones. The advent of the Internet and establishment of monetary authorities that control and issue money have made the idea of digitizing money, i.e., making the most of digital or online currencies and letting such authorities keep tabs on who owns how much, a feasible and even necessary one. Proof of this is the evolution of alternative modes of payment to the point that they have become the main methods for transacting today.

For example, credit cards, fund transfers and PayPal have become standard forms of payment these days. And in the United States, in particular, paying in cash is looked upon as unconventional or even suspicious in some cases. The ramifications of this evolution are huge. One of them is the ever shrinking amount of physical money circulating in many of the world's biggest economies and financial systems. As mentioned earlier, it's highly unusual now to pay for stuff in cash in the United States, unless you're talking about mom-and-pop stores and other very small businesses.

Becoming exceedingly digitized, how does money in its digital form work? And a more specific concern with the digitalization of money is this. What systems are in place to prevent double-spending of money, i.e., what's to stop me from digitally reproducing my money so that I'd have so much more than what I actually have? You know, like creating duplicate copies of my favorite songs for listening on my different devices.

Most financial institutions today address this issue with centralization. What this means is there's only one party responsible for keeping records of financial transactions under a particular system, i.e., keeping track of who owns what and how much. Everyone who transacts under such systems has an account, which has a specific ledger under which all transactions and balances are recorded and maintained. Everyone - including you and me - trust the systems of financial institutions to keep accurate records of our balances and these institutions, in turn, trust their computer systems. In short, the solution of centralization of records is based on a ledger that's stored in one big-ass computer system or network. Prior to the creation of the blockchain, there have been many attempts to create alternative digital forms of payment that have failed because of one very important issue; preventing double-spending sans a central authority. That's why the centralized records keeping solution has persisted until this day - it generally works.

Challenges Posed By a Centralized Monetary System

Whenever we give someone or a group of people total authority over something, there will be serious challenges that will need to be addressed. When it comes to doing so over the monetary system, there are three specific challenges that need to be addressed and these are corruption, mismanagement, and control.

There's a saying that absolute power corrupts absolutely. Central banks or monetary authorities such as the Federal Reserve, who have the legal mandates to print money and create value in the process, practically have the ability to control how value is created and destroyed in their respective countries and in the case of the Federal Reserve, in the whole world. And such legal mandates are akin to unlimited or absolute financial power. A very good example of this is the fiasco at Wells Fargo where its employees were ordered to clandestinely open fictitious bank and credit card accounts in an attempt to puff up the company's revenues and consequently, its net profits, for several years. And compared to monetary authorities, Wells Fargo isn't even an authority.

Mismanagement is simply when a manager or a steward acts in a way that is not consistent with how his or her boss - the owner - wants him or her to act. Mismanagement - in the case of monetary authorities - can happen when governments act against the interest of the people they govern. A very good example of this is the way the United States monetary authorities allowed major financial institutions to issue credit-linked notes or financial derivatives with mortgages that have very high default risks, which corrupt credit ratings agencies have rated as "investment grade." This has resulted in the near collapse of the United States financial system, which the Federal Reserve rescued by acting against the interest of the public by using public money, which the public has objected to, to save the biggest financial institutions from collapsing in

2008.

Another issue of mismanagement is printing of new money without proper consideration of the deflationary effects of such an action. As mentioned earlier, printing more money floods the financial system with too much money, which in turn can cause a specific currency's value to plunge or drop (law of supply and demand, remember?). A very good case of this is the Venezuelan government, who mismanaged the country's financial system and official currency by printing too much money. The Venezuelan currency has become practically worthless to the point that people started to measure its value by weight instead of amount.

Lastly, a central monetary authority means surrendering all control over the people's money to the government. Because governments have the legal mandate to control the money supply, they also have the authority to control your money in ways that can prove to be very unfavorable or unjust to you, e.g., freezing your bank accounts and keeping you from accessing your money. Keeping physical cash on hand doesn't mean the government can't keep you from beneficially using your money. Governments can still keep you from using your money for your benefit simply by revoking its legal tender status so you won't be able to use it for transactions, such as what India did in the past.

Gold And Silver

Let's talk about gold and silver. Why? Because of its connection to money. To be more specific, gold and silver aren't just investments - they're money! You might say "No, money is the US dollar or the British Pound!" Sorry to burst your bubble but those are merely currencies, as is the case with all fiat currencies in the world. But currency is different from money. First, currency is just a legal tender status, the value of which isn't determined by the people but by

governments. Second, legit money has important characteristics that make it so and the United States dollar doesn't have all of them and as such, money is more than just a medium of exchanging goods and services. Here are the seven characteristics of legit money:

1) Durability, which is the reason why wheat and salt are no longer used as money;
2) Divisibility, which is the reason why paintings and other pieces of art aren't used as money;
3) Convenience of use, which is why copper or lead isn't used as money;
4) Consistency in value, which is why real estate is hardly used - if ever - to pay for goods or services;
5) It must have intrinsic value or value as it is, which is why paper isn't really money;
6) It must be limited in available quantity, which is the reason for not using iron or rocks as money; and
7) And lastly, it should have a long track record of acceptability.

Upon close evaluation, you'll find that only gold and silver actually meet these characteristics. If you look at financial assets like stocks, bonds, or even real estate, they don't pass the consistency test because their prices tend to fluctuate. For others likes stocks, chances are that stocks of companies from 100 years ago - save for a few big and strong ones - have either deteriorated in value or are no longer worth anything because the companies whose ownerships such stocks represent no longer exist. The only items whose purchasing powers have not only been maintained but have also increased over the long-term are gold and silver. If only for this characteristic alone, gold and silver have kicked the butts of many currencies that have failed over the last 5,000 years. And if you factor in the fact that gold and silver are the only items that continue to have high value since the early days of all civilizations on Earth, you'll see why fiat currencies aren't really money.

Gold And Silver: Can Their Values Be Manipulated?

To answer this question, I'll focus the discussion more on gold. Gold price manipulation is defined as any intentional efforts to control the prices of this most precious metal. This supposedly happens in major financial markets when gold traders intentionally attempt to influence gold prices via certain financial instruments, particularly derivatives. These traders may have been able to successfully cause short-term deviations from the real values of gold, but over the long-term, it doesn't appear to be so.

The United States' Securities and Exchange Commission (SEC) defines manipulation in greater detail as any intentional act whose purpose is to trick investors by artificially affecting or controlling the market for a specific asset and includes activities like quote rigging, and voluminous trades or transactions that are meant to paint a deceptive impression of demand for a particular asset and sway market prices in their (traders') favor. And when speaking of gold price manipulation, there's one particular type of manipulation that is believed to be prevalent and that is price suppression, i.e., manipulating gold prices downward.

A really good question to ask then is this. Are the prices of gold - and consequently silver - manipulated? If you ask enough number of gold traders or investors, they'll tell you that it can be. Even more, they'll probably tell you that they are being systematically manipulated right this very moment. Are they right?

There are several iterations of this belief. One is that central bankers control the prices of precious metals. Another iteration of this belief is that greedy private commercial bankers are the ones manipulating gold prices downward through derivative instruments (short-selling and futures contracts) and high-volume trades meant to paint a scenario of low and decreasing

demand for gold and silver. When you look at theories like these, they seem plausible at first glance because of instances where gold prices were controlled in the past, such as when certain governments fixed the prices of gold for decades or when the London Gold Pool suppressed its prices. Add to the fact that very rarely do financial institutions get penalized for gold price manipulation and you have a very prevalent belief that indeed, gold and silver prices can be manipulated.

But if you look at the long-term price histories of gold and silver, it becomes exceedingly clear that the answer to our question is no, prices of these precious metals can't be manipulated. Check out academic papers on the subject and you'll find that no compelling evidence for the case of price suppression or manipulation exists. In fact, you'll find very clear cyclical patterns if you check out the long-term price charts of these two precious metals.

From a long-term view, particularly of the 2000s, you'll probably start to wonder how the heck people believed that price suppression for these two precious metals existed. And when you think about crying wolf, you may start to wonder why manipulation is selective, i.e., manipulation is responsible when prices go down and when prices are going up, it's the market that's pushing it up. And while we can't disprove the belief that the world's biggest players attempt to manipulate prices, their effects - if any - are very short-lived because it's practically impossible to suppress the true market price of gold in the market. Those who want to suppress the price of gold and silver over the long-haul simply don't have enough financial resources to do so. And any attempts to do so will only backfire soon because any significant drops in the prices of gold and silver will only increase demand for it and consequently, lead to an increase in their prices.

Naked Short-Selling

Many investors and traders of these 2 precious metals tend to certain financial institutions, particularly bullion banks, of naked short-selling in order to put downward pressure on prices. But does naked short-selling mean? Short-selling means selling something you don't have. So if you talk about short-selling gold bullions, it means you're selling gold bullions you don't have yet.

Now, why would you sell something you don't have yet and get into a whole lot of trouble for it? After all, isn't selling something you don't have considered fraud? Well, not really. You may not have the gold bullions yet, but you can borrow other people's gold bullion to sell them. And when the price of gold bullions drops, you can buy the same amount of gold bullions you borrowed for short-selling and in the process, make money. This type of short-selling is called "covered" short-selling because you cover yourself by first borrowing enough gold bullions to sell.

Naked short-selling is uncovered short-selling, i.e., you sell the bullions you don't have even when you haven't borrowed any to sell yet. Naked short-selling also happens when you short-sell gold bullions without any guarantee from other people that you can borrow enough bullions for short-selling from them. Naked short-selling can put you or any trader who does it at high risk of not being able to deliver the gold bullions sold to the buyer. Thus, the potential impact of naked shorts can be very serious.

There are "rumors" or "urban legends" that accuse the Federal government of using bullion banks to execute tons of naked gold short sales on the Commodities Exchange on its behalf to suppress the price of gold, maintain the US dollar's value, and gives these bullion banks the opportunity to make huge money by repurchasing the bullions at lower prices. Sounds so evil and believable,

right?

But think about this: if the number of naked short-sellers and there naked-short positions were that significant, the drop in prices of gold would be so huge that it would generate a reciprocal spike in demand for it. And the huge spike in demand would just wipe out the price drop because of the law of supply and demand.

Another thing to consider is the practicality of executing huge amounts of naked short sales just to suppress or manipulate the price of gold or silver. To execute this strategy effectively to drop the price of these 2 precious metals, naked short selling institutions would have to purchase a huge number of futures contracts just to cover their naked short positions. And as the futures contracts mature, they'd either have to buy the actual amounts of huge metals per futures contracts bought or rollover their positions, buy contracts that will be expiring, and flip the next ones out. In either case, the institutions involved in naked short-selling for price suppression will need to eventually unwind their positions, which will ultimately reverse or neutralize any price suppression effects of their attempted naked short sales. And this explains why naked short-selling for price suppression isn't realistic and why you'll see that based on long-term price charts for both gold and silver, their values follow cycles or patterns.

The main point of it all is this is that, despite the many conspiracy theories of price manipulation for gold and silver, proof of such is lacking. As for all financial assets whose values are market-driven, there are bull and bearish markets over the long-term. Bear markets - or when prices are falling - don't equate to price manipulation any more than bull markets - when prices are going up - do. It's all about market demand, cycles, and the ability to time our transactions well.

Chapter 2: Why Cryptocurrencies Work

Now that you've seen why compared to gold, fiat currencies aren't real money; it's time to turn our attention to cryptocurrencies as a solid alternative, why they are much closer to gold than money as we know it today is, and why they'd work better than fiat currencies.

Low Risk of Disruption

According to David John Grundy, the global blockchain head of one of the world's biggest banks, Danske Bank, the only way anyone can stop or shut blockchains down is by shutting down the Internet itself. And by now, I believe you know that is practically impossible. It's like saying somebody can keep the sun from shining or the wind from blowing.

Portability

Unlike fiat currencies, cryptocurrencies can be easily transferred from one account to another using online gadgets such as computers, tablets or even smartphones. With fiat currencies, you'll need to do so physically or through the same bank. Plus, you don't have to bring them with you physically because they're stored in the Internet. So you can go anywhere with a good Internet connection and bring your cryptocurrencies with you regardless of the amount!

Better Value Storage

You can only consider an asset as a good value storage if it's able to keep relatively unchanged levels of utility or satisfaction over time. Applying this to financial assets, it means having the ability to maintain purchasing power over time. A financial asset's ability to keep value can be

estimated through what is called as fundamental analysis, which takes into consideration both the quantitative and qualitative aspects of such an asset.

The ability to keep or store value has become the primary foundation for investing or HODLing cryptocurrencies like Bitcoin, Ethereum, and others. But can cryptocurrencies be really relied on to store value and if they are, can they do it well?

The Gold Comparison

Don't be surprised to find cryptocurrencies being compared or likened to precious metals, i.e., Bitcoin to gold and Litecoin or Ether to silver when justifying cryptocurrencies' ability to store value over the long term. One of the reasons - albeit a shallow one - is the color of cryptocurrencies. Bitcoins are visually represented as color gold while Litecoins are visually represented as silver. But there are more than just visual cues that justify the belief in cryptocurrencies' ability to store values like the two most precious metals on Earth. We mustn't dismiss behavioral economics that underlie both asset classes. When more and more people start believing that cryptocurrencies like Bitcoin, Ether, or Litecoin are able to store value the way precious metals like gold and silver can, it can help push the prices of these cryptocurrencies upward. When their prices do go up over time, then it's highly possible that they'll be able to keep or maintain their values within a specific period of time.

Comparisons to precious metals, e.g., Bitcoins to gold, can be a very strong factor that can influence the perspective of general markets regarding Bitcoin’s and altcoin's abilities to retain or store value in the long term. And this can have a huge impact in terms of the number of investors who'll view cryptocurrencies in general as good investment vehicles.

Limited Quantity, i.e., Deflationary

Just like gold in its physical form, cryptocurrencies like Bitcoin typically have a limited quantity of units, which is defined or set in their respective blockchain protocols. Bitcoin, for example, has a cap of only 21 million units that can ever be created. Litecoin on the other hand has an 84-million unit cap that's also controlled by its operating protocols. This is what makes cryptocurrencies deflationary or disinflationary over the long haul.

Remember our discussion earlier on supply and demand and how asset values are affected by changes in both? Because cryptocurrencies have a fixed number of units that will ever be minted, their supplies relative to the quantities of goods and services it can buy in the future is effectively shrinking. That means its purchasing power can be expected to increase over the long haul and can have deflationary effects on goods and services.

Independence from Other Asset Classes

Compared to all other financial asset classes such as stocks or fiat currencies whose values fluctuate depending on the pronouncements or moves made by central bankers or financial regulators, the real value of gold and silver can't be manipulated by any central monetary authority regardless of their macro-policy decisions. Because of its autonomy from any monetary authority, precious metals like gold and silver are able to withstand price shocks over time, which makes them very good storages of value in the long term.

Cryptocurrencies are like gold in that they're generally decentralized and autonomous by nature. This means just like gold, government decisions or policy changes have little direct impact, if at all, on their long-term values. The amount of decentralization and autonomy can be a hot

discussion topic among cryptocurrency users and investors, where some favor the full autonomy version while others feel more comfortable with some compromise, i.e., hybrid combinations of some form of governance (not from the government) and decentralization. In general, cryptocurrency governance models can vary greatly with some adopting a balanced power structure among its users when it comes to major decision making on one end while others go for the benevolent dictatorship model on the other hand. And in between the two are various other combination or hybrid models. But generally speaking, cryptocurrencies with more decentralized systems may do a better risk in terms of hedging against the risk of their values being influenced or tampered with by regulators.

Underlying or Intrinsic Values

Assets that are considered to be true storages of value have underlying characteristics that serve as foundations for their values. In layman's terms, such assets have intrinsic utility values, i.e., practical uses that give them their values. Gold, for example, is used for manufacturing jewelry and electronic parts such as semi-conductors. Land or real estate's underlying value or utility is their capacity for having structures built upon them and the amount of foot traffic their areas get.

When it comes to underlying utility value, cryptocurrencies have a lot of potential. In particular, cryptocurrencies hold a huge promise in terms of changing the way financial transactions are done online, which include contracts enforcement, records keeping, and payments. As the use of cryptocurrencies like Bitcoin, Litecoin and Ether becomes accepted in more and more markets, their practical utility values increase even more, which can increase their values over the long haul.

Impossible To Fake

The blockchain technology is a revolutionary one in terms of facilitating online transactions and data or record keeping. Being such, it's practically impossible to produce counterfeit versions of it. And as blockchains continue to evolve, it becomes even more impossible - if such a term exists - to produce fake cryptocurrencies that can be used to buy stuff.

Impossible to Control

Particularly for cryptocurrencies whose market capitalizations are already in the billions of dollars such as Bitcoin and Ether, one would need a huge amount of money to transact enough units of such cryptocurrencies just to be able to influence or manipulate their prices. When you take a look at Bitcoin, for example, whose average market capitalization hovers somewhere around US$50 billion, one would need at least US$10 billion to play around just to be able to manipulate demand and supply. Even if you're talking about Ether, whose average market cap is much smaller at "only" around US$25 billion to US$30 billion, one would still need a couple of billion dollar worth of transactions just to sway prices to his or her favor.

The Little Guy Gets In More

Unlike stocks and other financial assets that require relatively high amounts of investment capital, cryptocurrencies have low barriers to entry. That means even people who only have relatively small amounts of money to invest can easily get in. As such, cryptocurrencies, in general, have a higher number of investors participating in them to the point that it becomes

practically impossible to manipulate the market.

Relative Security

Lastly, cryptocurrencies are virtually impossible to rob if you do your homework of using the right kind of storage, which we'll talk about later. But if you just leave them in your cryptocurrency exchange account, that's the only time when it's at high risk of being hacked and stolen. So if you follow my advice later on regarding storage of your Bitcoins or other cryptocurrencies, you can make your cryptocurrencies so safe that they'll be practically impossible to steal.

Chapter 3: How to Store Your Bitcoins or Altcoins Safely

In Chapter 2, I mentioned that if you do your homework and follow my advice, your cryptocurrencies can be practically impossible to steal or hack. In this chapter, I'll spill the beans on how you can do that, which can be summarized in 3 words - a cryptocurrency wallet.

A cryptocurrency wallet is where you store your cryptocurrencies. This may be considered a cryptocurrency investing because the financial assets you're dealing with have no physical counterparts, i.e., they're digital. And because they're digital, you can only store them via a digital storage facility, i.e., a cryptocurrency wallet. The only question is what type of wallet will you use?

There are two general types of wallets: hot storage and cold storage. Hot storage wallets are those that are online or Internet based. Cold storage wallets, on the other hand, are those that are offline or aren't connected to the Internet. So which of the two is best for safely HODLing your cryptocurrencies? If the only way to steal or rob your cryptocurrencies is via hacking, then the obvious answer is cold storage or offline wallets, which come in two general variants: paper and hardware. And I suggest using both.

But before I explain how these two cold storage wallets work, allow me to explain how cryptocurrency storage, particularly the blockchains, works. When you buy cryptocurrencies from any particular exchange, your transaction is assigned a public key that is linked to the number of units of a cryptocurrency that you bought. Your cryptocurrency exchange, on the other hand, assigns private keys that corresponds to your public keys. Therefore, your private keys are your lifeline to your cryptocurrencies, and if you lose or forget them, you can say goodbye to your cryptocurrencies.

For others to successfully "steal" your cryptocurrencies, they must get hold of your private keys. It's like your ATM card's personal identification number, which will allow other people to withdraw from your account without your permission. When you leave your cryptocurrencies in your hot wallet, i.e., your cryptocurrency exchange account, you put them at risk of being hacked and stolen. That's why as soon as you're done buying your cryptocurrencies, you must transfer them, including your private keys, to your cold storage or offline wallet.

Ok, now that we've got that covered, I can explain how the paper and hardware wallets work. The paper wallet isn't really a wallet but more of a backup. Write your private keys on a piece of paper and put that paper in a place where it's virtually impossible to steal or destroy them. A very good place to do so is a fire-proof vault or safe. Another's a safety deposit box.

Hardware wallets are USB-type devices that you can store your cryptocurrencies and its private keys in. These are devices whose sole purpose is to hold your cryptocurrencies and as such, they're offline most of the time. To use them to receive or transfer your cryptocurrencies from and to your cryptocurrency exchange account for executing transactions, you only need to plug it into the USB port of your Internet-connected desktop or laptop computer and follow instructions.

Cold storage hardware wallets are much safer compared to software wallets, i.e., apps installed on gadgets for two reasons. One is if it's installed on a device that's mostly online, then the risk for getting hacked is still fairly high. Second, even if you install it on a device that you only connect to the Internet for transacting in cryptocurrencies, there's still a risk of loss if that computer is damaged beyond repair or even if it can still be repaired, the computer technician to whom you'll have it repaired can possibly hack the drive and consequently, your wallet. With a

hardware cold storage wallet, the risk of losing your private keys due to hardware damage is much, much lower. Further, using a paper wallet as a backup can help mitigate such a risk. Some of the most popular hardware wallets include Trezor, KeepKey, and Ledger Nano. They may cost a bit, but they're worth the investment.

Chapter 4: Is Bitcoin dead?

Because of the rapid rise in value of Bitcoin, especially in December 2017 when its market price quadrupled in just a couple of weeks, and its subsequent price retreat in January 2018, many people were led to believe that Bitcoin's just an asset bubble that has already popped. In other words, they believe that Bitcoin's as good as dead.

But while the huge returns Bitcoin and other major cryptocurrencies have generated in a relatively short period of time is reminiscent of the Internet and Holland Tulip bubbles in the past, it's fundamentally different than those two assets. As such, Bitcoin and other noteworthy altcoins have a much brighter future compared to the two aforementioned assets.

The following are indicators that Bitcoin isn't dead yet and more importantly, it's going to be around for a long, long while.

More and More Legal

Not to say that Bitcoin's an illegal endeavor but what I'm saying is that it's becoming more and more accepted as legal tender. You see, one of the most serious challenges facing Bitcoin with regards to being accepted in the financial services mainstream is acceptance by government monetary authorities (lawmakers and regulators alike), which is hampered by its decentralized and autonomous nature. Governments hate what they can't control so Bitcoin's not exactly in their good graces - at least not yet. But recent developments in major economies indicate that government acceptance, in general, is becoming more and more likely.

Japan announced back in April 2017 that it would officially start treating Bitcoin as a valid or

legal alternative payment method and as of 2018, it already is. This has made Bitcoin practically part of the Japanese mainstream financial system as more and more merchants in the Land of the Rising Sun have officially started accepting Bitcoin payments.

Other major world economies like Russia and Australia have also released similar statements indicative of Bitcoin being accepted as a form of legal tender in their respective economies soon. As more and more major world economies accept Bitcoin as a legit payment method, the rest of the world is highly likely to follow suit.

More Stores

More than just government pronouncements, Bitcoin's acceptance among merchants continues to rise because of the confidence shown by some of the world's biggest companies in accepting payments using the granddaddy of all cryptocurrencies. These companies include Microsoft, Overstock, and Rakuten.

But more than just riding on the bandwagon of these big companies, there are fundamentally sound reasons for the rising number of merchant acceptance of Bitcoin. One of them is transaction fees, which are much less than what credit cards charge to its merchants. Other practical advantages Bitcoin as payment has are the ability to reach new customers from regions in the world that are not yet reached by mainstream banking institutions and elimination of chargeback fraud. With the expected rise in mainstream acceptance by merchants, demand for Bitcoin is expected to rise and of course, its price can be reasonably expected to rise over the long term as well.

Wealth Storage

Remember our discussion in a previous chapter concerning cryptocurrencies' ability to store value and its relationship with functional value? The increasing acceptance of Bitcoin in many of the world's financial markets, particularly in countries that are experiencing economic distress, gives the granddaddy of all cryptocurrencies increasing functional value. In such distressed economies as Bolivia and Venezuela, local currencies' values continue to deteriorate to the point of becoming worthless. In such economies, Bitcoin is becoming more and more accepted as a mode of payment, which means its functional or utilitarian value is increasing. So as their local currencies are becoming less and less valuable, Bitcoin is becoming more and more precious and as a result, is becoming an even better storage of value for citizens of such countries.

Walking Dead...No!

As you can see, Bitcoin's very much alive and kicking and based on the indicators I've just enumerated, you can expect it to continue staying alive. Bitcoin, being the granddaddy of all cryptocurrencies, has the highest market capitalization and best performance track record, both of which will continue to make Bitcoin more and more accepted in the international financial mainstream. And as that happens, the likelihood of Bitcoin dropping dead will become even more statistically impossible.

Chapter 5: Cryptocurrency Pre-Hodling Strategies

Before we discuss how to hodl in more detail, I want to make a distinction between two investment methods: the long-term approach and the short-term approach. The short-term approach is more popularly known as trading, i.e., buying and selling of financial assets within a relatively short turnaround time like within a few hours, or at most, a couple of weeks. The long-term approach, also known by the names buy-and-hold and buy-it-forget-it, is an approach where the investment time horizon is - you probably guessed it right - long. By long, I mean at least 1 year.

Hodling falls under the long-term, buy-and-hold approach. Hodling has its share of advantages over the short-term approach. One of them is time. With the short-term approach, you have to be on top of your positions most of the time so you can time your transactions well. This is especially true for financial assets whose prices are very volatile, like cryptocurrencies. With the long-term approach, the bulk of the work you'll need to do will be prior to buying your financial assets, i.e., research. After doing your homework, you buy the financial asset you believe is your best bet and forget about it. All you'll need to do is update yourself on the price of your investment once a week or even once a month. Because your investment view is long-term, you won't be affected by the price fluctuations in between and hence, only need minimal management or monitoring.

Another advantage is cost. In a perfect world, every transaction shouldn't cost a dime. But our world ain't perfect so you'll need to pay transactions fees for every financial investment transaction. With trading, you'll trade more often, which means more transactions fees. With a long-term approach, a.k.a. hodling, the number of transactions you'll have to make are few and far in between, which means less transactions fees.

Now that I've gotten the distinction out of the way let's jump into how to significantly increase your chances of hodling successfully. For better appreciation and understanding, I'll divide this topic into two main sections: Before and during hodling. We'll focus on before HODLing in this chapter.

Ask Yourself Why

Remember what I wrote earlier about how bulk of your hodling work will be in the beginning, i.e., prior to your actually hodling your cryptocurrency investments? Good. Now let's buckle down to work! The very first thing you'll need to do is know your reason for hodling.

When you examine the lives of people who have achieved so much in their lives, one common thread that runs through them is awareness of their life purpose. In other words, they know why they're doing what they're doing. And more importantly, I guarantee you that if you examine each of their reasons, you'll find those reasons to be very meaningful or compelling ones. Therefore, you'll need to have a compelling reason for hodling any financial asset, which in this case is cryptocurrencies.

Why is this crucial? Hodling successfully will require self-control and perseverance, especially during times that prices are down, i.e., bear markets. It is during such moments when your emotions can become so strong that they override all logic and make you do things you'll probably regret later on.

But while anybody's reason for hodling's very obvious, i.e., make money, it's not a very compelling one. In fact, it's a very generic and shallow one. I'm talking about a deep,

compelling, and personal reason. To better help, you figure this out, ask yourself deeper questions such as why do you want to make money of this investment? Is it so you can have enough money for your child's college education 15 years from now? Is it so you can retire early? Or is it so you can travel around the world by the time you turn 60 years old? The more personal and bigger your reasons are, the more compelling they can be.

When you're tempted to switch to a riskier cryptocurrency that's been increasing in value at a faster rate than the relatively less risky but consistently performing cryptocurrency you're hodling, knowing that you're doing this to minimize the risk of your child not being able to go to college can help you exercise self-control and avoid taking excessive risks and gambling away your child's future. When you're tempted to unload your cryptocurrencies simply because they've dropped in value even though all indicators may point to a bright future ahead, knowing that you're doing this so you can retire early can help you resist the temptation knowing that unless you actually sell your cryptocurrencies at a loss, your market loss is just a theoretical one and can still be recovered.

Minimum Rate of Return

When you know how much your investments need to earn at the minimum, it'll be easier for you to choose your investments wisely. And by wisely, I mean choosing investments that are neither too safe but unprofitable nor potentially very profitable but also excessively risky. When you know how much return you need to accomplish your hodling goals, you put yourself in a good position to take on investments that will help you accomplish your goals for the least possible risk.

So how do you know you minimum rate of return? First thing you'll need to know is how much

money you need to have by the end of a certain period, e.g., after 5, 10, or 15 years. Then, determine how much money you can afford to set aside for investing. Finally, determine the rate of return based on your expected future value (the amount you need to have in the future) and present value (your available funds for investing or hodling). And when you've determined that, make it your minimum expected rate of return and choose only those cryptocurrencies whose average annual rate of return is equal to or more than your minimum required.

Risk Appetite

This refers to how much loss you are willing to take in the event your investments turn sour. Why is this an important consideration? It's because there's no such thing as risk-free investments and the higher the expected returns on investments are, the higher the financial risks you must be willing to take. So there is a possibility that your investments won't be able to give you the returns you're after. And the worst thing that can happen is you lose money on your investments, which can be as much as all of it. By knowing how much you're able to comfortably lose, you'll be able to determine whether or not to invest in a specific financial asset such as cryptocurrencies. And if you decide you want to invest in a specific financial asset despite the risk, knowing your risk appetite or tolerance can help you determine how much money to invest.

When figuring out how much cryptocurrencies to hodl, there are two ways you can estimate your risk appetite. One way is to think about how much money you can comfortably lose. There are two benefits to this approach. The first is this: your finances won't be seriously affected if the worst case scenario happens. Investing your entire savings in cryptocurrencies is a foolish idea because if the price goes down by a significant amount, you might not have enough money for

your personal needs when something unexpected happens like getting hospitalized or if you accidentally wreck your car. But if you invest an amount beyond what you really need to live a comfortable life, you can live with worst case investing or hodling scenarios.

The second benefit to this approach is you won't be pressured when prices of your cryptocurrencies go down or fluctuate wildly. When that happens, your emotions won't get the better of you and because you can be more objective when it comes to your cryptocurrency holdings, your chances of successfully riding out temporary investment "storms" are much higher.

The other way you can estimate your risk appetite is by determining an amount of money you strongly believe you won't need to use within the next 1 or 2 years and beyond. How's this a good basis for determining how much to invest in cryptocurrencies or other financial assets? Hodling is a long-term endeavor. As such, you need to be able to keep your investments intact so it can ride out temporary dips in prices if any. For you to be able to do this, you'll need to make sure that the money you're going to invest is an amount that has a high probability of not being needed in the near future.

Read the Damn White Papers

Especially if you plan to invest in an initial coin offering or an ICO, which is the cryptocurrency equivalent of initial public offerings or IPOs of stocks and bonds, you'll need to read the white papers of the cryptocurrencies you're interested to hodl. But what are white papers?

Before we get to that, we need to talk about ICOs first. An ICO is a way by which creators of a cryptocurrency raise enough funds to launch a new one. These fundraising activities are

unregulated, considering the autonomous and decentralized nature of cryptocurrencies. Compared to the usual fundraising activities of mainstream investment banks and other financial institutions, ICOs are way less rigorous and regulated, which makes them easier to do.

ICOs worth their salt will always give out white papers, which is the ICO equivalent of an IPO's prospectus. A white paper is a document that elaborates on the details of the fundraising activity, i.e., ICO. These details include among others the purpose for the fundraising activity. As a prospective investor, it's crucial that you know as much as you can about the ICO you plan to get into so you can have a very solid idea of whether or not it's legitimate and whether or not it has very good investment potential. White papers are written by people from a wide range of backgrounds who are knowledgeable about the coin or token to be issued as well as the financing of such like lawyers, PR practitioners, experienced business men, and information technology experts, among others.

White papers are created and distributed to the investing public to give them a clear idea what the ICO is really about and in the process, foster a good level of trust from them. White papers - just like prospectuses - can help establish the legitimacy of an upcoming ICO and thus, is crucial for its success. And for you, as an investor, the white paper is the primary means by which you can learn all there is to learn about a soon-to-be-issued cryptocurrency. Through white papers, you can make the most informed decision possible about whether or not to invest in an ICO. So when you see an ICO already being sold without a white paper, that should be a red flag already concerning its legitimacy or if not, the quality of that ICO.

So what are the things a good white paper should contain? These include:

- The ICO's vision;
- The underlying technology for the token;

- The token or the project's unique selling proposition (USP), i.e., what current problems or challenges it can effectively address, why being able to effectively address such challenges is important, and the token's unique characteristics;
- How the token will be distributed among its ICO subscribers as well as among the team behind it;
- Timeline of activities that need to be completed for the ICO;
- Language and focus of the white paper; and
- The people behind the token's development and their credentials.

Details such as these are crucial for your hodling success because these are the things that can affect the long-term viability of the token in question.

Reading the white papers is very crucial for spotting a potential scam. Of all the details white papers contain, there are three that can give you a good indication of whether or not the ICOs they're backing up are legit. These are the vision, the people behind the ICO, and the language and focus of the paper.

The vision part of white papers gives you an idea if the people behind the ICOs believe that they'll be around for the long haul or for the short term only. Legit ICOs are in it for the long haul so if their vision is either short-term or is vague as to the timeline, better think twice.

The people behind ICOs should give you a very good idea of the quality of their quality and their chances of being able to successfully accomplish their vision. Conduct a background check on the people identified in the white papers as being part of the core team, particularly their accomplishments, credentials, and where available, any scandals or issues involving them. Because they are the people who are responsible for creating and managing the tokens up for sale

in ICOs, they should be the single biggest factors to consider when weighing the chances of success for ICOs. Or whether or not they're legitimate.

Lastly, the way that white papers are written is another indicator of whether or not they're legit. In particular, pay close attention to the focus and language of the paper. What's the paper focusing on? Is it focusing on the benefits with very little or no discussion on risks? If this is the case, then chances are it's either a very low quality ICO or worse, it may be a scam. Scams tend to focus on the potential benefits, making them seem almost sure or guaranteed, in order to make you feel so good about them enough to be duped. Legitimate ICOs disclose relevant investment risks so their prospective investors can make the most informed decision possible.

What about the language? White papers that are written very poorly, i.e., using inappropriate language or terms can be indicative of a scam. For example, try watching the TV show Designated Survivor and one thing you'll probably notice is how realistic the show seems, which makes it a legit high quality program. And one of the reasons why you'll probably think that way is because they use terminologies that are actually used in the White House or in politics. In the same manner, legit white papers will use terms and sentences that you just know is consistent with the industry. White papers that appear to be written by amateurs is a red flag.

However, white papers that meet these three criterions isn't a guarantee of legitimacy and high quality, as it's possible for scammers to hire professionals to write very good white papers for them. But what it does is tell you that there's a very high probability that the ICOs such white papers back up are legitimate and of good quality. That's why it's also important to research information outside of white papers. That way, you can validate the information you'll obtain from them.

Chapter 6: Cryptocurrency Hodling Strategies

Now that you've done your pre-hodling homework, it's time to discuss hodling strategies that can help you achieve your investment goals.

Use the Minimum Expected Return to Choose Your Cryptocurrencies

After determining your minimum required rate of return, it's time to do a bit more research for hodling cryptocurrencies that have the highest chances for success. In particular, you must research on the average rates of return on your prospective cryptocurrencies, particularly if you plan to buy those that are already being publicly traded. Why? It's because tokens being sold through ICOs don't have past prices to compute average returns with.

For illustrative purposes, let's say that after doing your research, you find that the average annual returns on Bitcoin, Ethereum, and Litecoin were 30%, 20% and 25%, respectively. If your minimum required rate of return is 18%, which of the three would you choose? Chances are, you'd go for Bitcoin without batting an eyelash because it has the highest average annual return at 30%. I wouldn't say it's wrong but what I can say is that it's incomplete. Why?

When comparing actual returns to average returns, they're rarely the same. Actual returns aren't equal to the average, but they tend to be within the range of the computed average in most cases. This means that actual returns can be higher or lower than the computed average by up to a certain amount. To optimize your chances of being able to achieve your minimum required rate of return, you'll need to choose investments whose most conservative estimated or forecasted future returns equal or exceed your minimum. And for this, you'll need to compute for the standard deviation, which measures the volatility of returns or how far can you reasonably expect

returns for a specific investment to be from the mean or average return computed. Allow me to illustrate this in a way that you can easily understand.

Let's say that the computed standard deviation for Bitcoin, Ethereum, and Litecoin were 15%, 3%, and 7%, respectively. What do these figures mean? It means that you can reasonably (not perfectly) expect the return for Bitcoin this year to range from 15% (30% -15%) to 45% (30% + 15%), where 15% is the lowest expected return for Bitcoin for next year. For Ethereum, the annual return for this year to range from 17% (20% - 3%) to 23% (20% + 3%) and for Litecoin from 18% (25% - 7%) to 32% (25% + 7%).

Now, compare the lowest expected returns for each of the three cryptocurrencies. Bitcoin's is 15%, Ethereum's is 17%, and Litecoin's is 18%. Given your minimum required rate of return, the wise choice would be Litecoin because its lowest expected annual return for this year is the only one that satisfies your 18% minimum requirement. Without the benefit of standard deviation, you could've gone for Bitcoin, which has a reasonable chance of registering a lower annual return than your required minimum. And even though its mean or average annual return's the highest, it's also the most volatile with the highest standard deviation, which resulted in the lowest among the low end of the expected return spectrums.

Diversify

A very crucial hodling strategy that you can apply to practically any financial investments, it means to spread your investment eggs in different baskets so that if one investment basket drops, your other investment eggs won't crack. And more than just investing in at least 2 cryptocurrencies, you must also make sure that you don't put all your investible funds in cryptocurrencies only. Why?

Because Bitcoin, Ether, Litecoin, and other altcoins belong to the same class of financial assets, which is cryptocurrency. There's a good chance that when something happens that concerns or can affect the whole cryptocurrency industry, the prices of all your cryptocurrencies may simultaneously take serious hits. For example, if the Federal Reserve makes a pronouncement that will make it more difficult to transfer funds from banks to cryptocurrency exchanges, it won't just be the price of your Bitcoin that will go down. But if you also diversify your investments to other financial assets, you reduce the potential impact of negative events on your total portfolio.

Cost Averaging

This is a very useful hodling strategy that can help you earn good returns despite substantial price drops in the cryptocurrencies in your portfolio. So how does cost-averaging work?

Cost averaging refers to a method of investing by which you buy more units of a financial asset (cryptocurrencies, bonds, stocks, etc.) when prices go down. You may be thinking: "Why the heck would I buy more units of a financial asset whose prices are going down?" That's a good question, one that I'm inclined to answer.

The principle behind cost averaging is this: by buying more units of a financial asset when its price goes down, you bring down your average initial cost per unit of that financial asset. So what's the significance of this? If your average cost goes down, your breakeven price for that financial asset goes down as well. That means you don't have to wait for the price of that

financial asset to fully recover just to break even. And if the price eventually goes back to the same one at which you originally bought it, you won't just break-even but make a profit already!

Allow me to illustrate with a practical example. If you bought 1 Bitcoin at $10,000 and its price plunges to $6,000 afterwards, you would've suffered a $4,000 or 40% loss on your investment. For you to break-even, the price of Bitcoin has to fully recover back to $10,000. And for you to make a profit, you'll have to wait until Bitcoin goes above $10,000 per unit.

Now let's see what can happen if you employ the cost averaging strategy. Say you bought another unit of Bitcoin when its price dropped to $6,000. Now, you have 2 Bitcoins for a total investment of $16,000 ($10,000 + $6,000). By using simple averaging, your average cost of buying per unit of Bitcoin is $8,000 ($16,000 ÷ 2 Bitcoins). Now, you only need to wait until the price of Bitcoin goes up to $8,000 to breakeven, compared to waiting for the price to go back up to $10,000 to break-even when you only owned 1 unit of Bitcoin. And when it goes back up to $10,000 per Bitcoin, you would've made a profit of $2,000 per Bitcoin or a total of $4,000 for your total investment. If you didn't cost average, you'd have to wait until the price of Bitcoin had gone up to $14,000 per Bitcoin just to register a $4,000 profit.

Conclusion

There's no denying that the next frontier in the evolution of the world's financial systems is Bitcoin and other major altcoins like Ethereum, Litecoin, Ripple and Monero. As such, good quality ICOs also have a bright future in the world of digital finance. But being able to successfully hodl and take advantage of the opportunities that cryptocurrencies - both existing and those that'll be issued in the future - require smart work and a whole lot of self-discipline. To the extent you can work smart and control yourself, especially your emotions is the extent you can successfully make money by HODLing Bitcoin and other cryptocurrencies.

To recap, HODLing refers to holding or keeping cryptocurrencies and that this word is a mistyped version of the word "hold" which has grown to be an accepted term in the cryptocurrency community. HODL is also a long-term approach to investing, which is can also be called as a buy-and-hold approach. To successfully HODL, there are two phases you need to get right: the pre-HODL phase and the actual HODLing phase.

The pre-HODL phase is when you prepare for taking positions in cryptocurrencies by knowing your investment goals or purposes, establishing your minimum acceptable rate of return, estimating the amount of risk you can take, and reading the damn white papers of ICOs, if you're looking to buy new tokens or coins. The actual HODLing phase involves choosing the optimal cryptocurrency based on the minimum expected range of returns, diversification, and cost averaging.

Before we proceed with the basic concepts of cryptocurrency mining, I would like to thank you all for showing an interest in downloading my book. I have always been fascinated with this modern-day financial system. I believe that anyone who has invested his/her time and money in

this book is one part interested in this new form of encrypted exchange, one part skeptic, uncertain and dubious about this concept.

There is nothing wrong with showing doubt and being a little negative about something that we do not know. I know I was negative once. Terms like Bitcoins, ICOs, blockchains, cryptocurrencies, whatnot – they are all new for us, and we have every right to know about their history, workability, advantages, and anything in between.

Thus, in this book, I am going to get you acquainted with cryptocurrency terminology, as well as give you a brief explanation of how it operates and pays an investor. Does it have any potential? Yes, it does, but certain aspects make it follow a discreet environment.

Firstly, let us understand how we can define Cryptocurrency.

A cryptocurrency is defined as an asset fabricated to operate as a way of exchange carried out digitally. It implements a protective technology known as cryptography, which regulates the generation of more credit units and monitors their transfer between parties.

Simply put, cryptocurrencies are a form of currency in the digital world that do not follow the rules and regulations of a centralized banking system. Transactions work through a decentralized database called blockchain, which we will examine in detail in later chapters.

Bitcoin, which emerged as the first cryptocurrency in 2009, has gained worldwide fame over the years. It was Satoshi Nakamoto, a pseudonym used by an individual or a group, who developed Bitcoin as the first cryptocurrency. Also, they were the ones to fabricate the beginning of a blockchain database.

Since then, numerous decentralized cryptocurrencies have revamped the operations of the traditional financial system. Bitcoins and alternate cryptocurrencies (also known as altcoins) are already witnessing tremendous growth, making them a part of new technology in the financial world.

With the digital era evolving to new levels, Bitcoins and other cryptocurrencies are likely to grow exponentially in the future. With benefits that offer multi-operational utility in the financial sectors, cryptocurrencies are developing an open system that will allow us to exchange credits in ways that no one thought possible.

Thus, it is even more significant that you learn about this digital phenomenon and familiarize yourself with how it works to secure your financial assets.

Chapter 1: History Of Bitcoin Mining

In simple terms, Bitcoin mining is a method of calculating the value of cryptocurrency assets through a cryptographic process. These processes mine Bitcoins in blocks, which are simply ledger files that permanently record all recent cryptocurrency transactions.

You should know that the size of the block decreases as the number of coins increase. Any block starts with 50 BTC (Bitcoin currency symbol), and as the number of blocks reaches 210,000, it halves. This results in a recurrent halving of the rewards for an individual block. This process is performed so that the inflation rate is regulated. Otherwise, there would be an uncontrollable number of paper currencies printing every second.

This concept in itself is proof that mining is not a simple process. It needs investments in the form of power, time, and computations. Also, with an increase in the time of mining these coins, its comprehensive power also increases.

Another fact to note is that the speed of emerging Bitcoins is inversely proportional and drops exponentially. Satoshi calculated the number to be approximately 21,000,000, which can never be exceeded. Let us explain this mathematically:

A block takes around 10 minutes to be mined. And a complete mining cycle halves every four years. So, it results in:

Six blocks per hour. Multiply it further by 24 (hours per day), 365 (days per year), and 4 (number of years in a blockchain cycle).

So, we get -> 6 x 24 x 365 x 4 = 210,240 ~ 210,000.

After every 210,000 the block size is halved, and each block has 50 Bitcoins.

So, sum of all the sizes of block rewards becomes:

$50 + 25 + 12.5 + 6.25 + 3.125 + \ldots = 100$

So, total number of coins that can be mined:

210,000 x 100 = 21,000,000.

If we talk about it in economic terms, the currency is divisible infinitely. Thus, the accurate value of cryptocurrency coins can be ignored as long as we fix a limit, which is 21 million. No doubt there can be a time when the number of mined coins reaches 21 million, and there is no more profit left unless there is a way to redefine the computations and new regulations are determined. But, that can take a while. Let us learn why.

The annual consumption of energy for mining Bitcoins has been estimated at 30TWh, which is equal to the stable energy of 114 megawatts for a whole year. Also, an individual transaction of a Bitcoin can take up power used for providing energy to about 10 U.S. houses in one day. Indeed, we can see that the energy consumption expenses for mining Bitcoins are high.

Also, if the expenses of the mined coins surpass the costs of equipment and electricity used for mining, the cost-effective and less competent equipment will no longer be needed for this industry. This activity is economically reasonable, as increasing in the mining activities will increase investment in challenging computations, which in itself becomes expensive. In fact, the difficulty in computations has escalated to some 210,000,000,000 times. Also, the overall mining capacity for computations has reached 1,500,000,000 hashes per second.

How It All Got Started

Cpu Mining

Bitcoin mining started with earlier servers that let users utilize personal CPUs for mining. The first block header hash (a secure linkage between previous and current block) was computed using a conventional CPU of a computer, the Intel Core i7 990x to be precise, which was efficient enough to calculate at 33 MH/s.

Gpu Mining And The Starting Of Mining Farms

As time went by, the cryptographic mining industry upgraded its processing system to graphics processing units (GPUs). These adapters were able to perform cryptographic computations at a much faster rate than CPUs. The higher models of GPUs were able to calculate at 675 MH/s. Moreover, it was deduced that the calculative abilities could be even faster if one combined the power of more than one GPU. This linking of GPUs to mine cryptocurrency is termed as a Mini Farm, which contained a RAM unit, a CPU, 5-6 potent GPU accelerators, and a motherboard.

Gate Arrays

No doubt the disadvantage in initial mining was the requirement of a very powerful system. To tackle this weak link in the mining farms, a technology called Field-programmable gate array, or FPGA, was introduced. An FPGA is an IC (integrated circuit) that is configurable by the designer or customer once it is manufactured.

FPGA miners were evaluated to be five times more efficient compared to GPU miners. Regarding hash period, an FPGA computation displayed efficiency levels of 25.2 GH/s.

However, there was still the overwhelming costs incurred while using FPGA mining processes. GPU units were still less expensive and had a better resale value once exhausted.

ASIC Mining

After the advent of the mining farms, it was found that the previous methods became economically impractical, as they were not specifically designed to run mining computations. This is where application-specific circuit miners or ASIC miners came into existence, which only served the purpose of cryptographic mining. These miners are almost ten times more efficient in mining.

One of the leading designers of ASIC miners was Butterfly Labs, which started developing miners in 2012 on pre-orders for potential customers. One of their masterpieces is the SC Mini Rig, which has the computation energy of 1,500 GH/s.

As mining became more and more difficult, it was almost impossible to manage computations using mini-farms. Lack of resources ultimately led to the migration of the mining technology to data centers, which were highly efficient in their calculative power. True Bitcoin mining farms are justified using such setups with massive data centers to support the activity.

Cloud Mining

While ASIC mining using data centers is running currently, there is a new method of mining, thanks to the emergence of cloud computing technology. We call it cloud mining, which implements cloud-driven services for mining cryptocurrency. The cloud was able to save costs on expensive tools and equipment, and electricity, so the technology was favorably included in the mining process. This solved many problems that data centers usually involve, yet it is not 100% financially efficient. Almost 80% of cloud mining services present today are frauds, and many mining services do not pay the revenue after investment. So, this type of mining service needs to be approached very cautiously.

Hack Mining

Another emerging mining concept is hack mining. This is carried out using smart devices owned by other users. This mining activity is carried out using a special malware software which hacks into a device without the user being aware of it. After penetrating the device, they discreetly mine using the hacked system. Many users purchase such shady services, which do not cost much.

As a lot of power is needed to mine a cryptocurrency coin, a hacker hacks multiple smart devices, and combines the power of the activity. This way, the owner of the smart device does not even notice any changes. A case in 2014 emerged, where an anonymous attacker exploited a limitation in the cloud servers of Synology to mine around $200,000 worth of Dogecoins. More cases emerged, targeting mobile devices in their millions to mine cryptocurrency since the existence of this concept.

Hack mining activities are usually successful as hackers can read the software codes better than the security teams of the manufacturers. They tend to locate the vulnerabilities in their systems and exploit them for their advantages. Therefore, beware, as you may never know that your computer system is also helping a miner get rich.

Chapter 2: How It Works

By now, you know that in approximately every 10 minutes, new batches of cryptocurrency coins are made, with an individual coin worth $8000+ at current value.

Before I proceed with explaining how it works, let me first make you understand how it does not work. Firstly, do not get the wrong idea that cryptocurrency mining involves using equipment to search through the depths of the internet to locate a digital ore that can be mined into Bitcoins. There is no actual ore, and Bitcoins are not about smelting or extracting that ore from the virtual world.

It has been called mining because the individuals who get new Bitcoins earn it in small and finite quantities periodically, similar to gold. Thus, the process has been termed as mining, and you are already aware of the halving system of the Bitcoin batch in an interval of every four years.

Now, to learn how it works, you should know that all Bitcoin miners are doing is comprehensive bookkeeping. A huge public ledger contains all the records of the transactions carried out in the world of cryptocurrency until the present. Any transaction of Bitcoins between two parties has to be recorded and accredited by the miners in the virtual ledger.

It is the miner’s responsibility to monitor that the sender is transacting actual money for mining the Bitcoin. Once the transfer of money is approved, the miners validate it in the ledger. Moreover, to make sure that potential attackers do not hack the ledger, the ledger is encrypted with very complex computations that are almost impossible to hack. This service of mining offers them Bitcoins.

There is always a competition going on amongst miners, who look forward to approving their batch of transactions to complete the computations needed to encrypt the transactions in the public ledger. Every new batch results in a rewarding activity for the miners who completed the

transaction.

However, the computation process is quite daunting. Specialized equipment with hi-tech processing units are responsible for computing and solving cryptographic problems.

It all does seem exhilarating, doesn’t it? After all, the process of mining has generated a robust solution to a tough problem that every digital currency faces, which is double spending.

The Concept Of Double Spending

What Is Double Spending?

Double spending can be defined as an activity when an individual transacts more money than the required amount. Most currencies online face this issue. Traditional currencies keep check on such problems by paying real cash or acquiring the help of reputed third-party organizations like banks, credit card services, PayPal, etc., which all transact the amount and record the changes in the account balances based on the transactions.

However, Bitcoin functions in an open digital world, where third-party organizations do not influence or monitor it. Its philosophy counters the traditional approach we witness in the financial world. Thus, if I say to you that I have 20 Bitcoins with me, how will you come to know that I am not lying about it?

Thus, to keep everything in check, a public ledger was fabricated that records all the transactions. This public ledger is referred to as Block Chain. I will discuss it in detail in later chapters. This public ledger lets you trace all the Bitcoin transactions right from the very first time they were recorded.

But Bitcoin is a digital currency, and is not monitored by any intermediaries. This technology's philosophy counters the monitoring activities practiced by third party enterprises. So, if you say that you own 25 Bitcoins, how will I trust that you are being honest or not? The solution is that public ledger with records of all transactions, known as the blockchain. (We will learn about it later.) There is no way you can lie about the number of coins in your possession, when this technology fabricates a way to trace every transaction right from the start.

Thus, for every Bitcoin transaction, miners go through the ledger and check for malicious practices of double spending. If everything is found perfect, the transaction is validated and

recorded in the public ledger. It sounds simple, but it is not.

A public ledger accompanies a few problems:

Privacy is the first issue. How can one make sure that the exchange of Bitcoins retains transparency while not disclosing their identity?

The other problem is security. If we talk about a public ledger that is open for all, how is it possible to prevent people from using it for their capital exploitations?

Well, to answer these issues, first you should know that a Bitcoin miner does not own an account in which to keep his/her Bitcoins.

Now coming to privacy, the cryptocurrency ledger manages to overcome the issue of privacy by using a deceptive technique. This ledger functions as a record keeper for the transactions only. It does not keep a record of the Bitcoin balance or account. This way, all user information remains discreet.

Let me explain how it works with an example:

Let us assume that Rick needs to transfer a Bitcoin to Morty. To accomplish this, Morty will generate an address virtually so that Rick can transact money, including an encryption key, to that address. The process is similar to an account with a password. The only difference is that Morty (the receiver) will open a new virtual address and a key for every new transaction. It is not necessary to do so, but to keep everything secure it is recommended that the transaction is done like this.

Now, when Rick clicks the send button to transact the money to Morty, the transaction chances into an encrypted code containing the amount and Morty's virtual address. This transaction is also transferred to all Bitcoin miners on the internet, which includes all computers running the software for mining. Once the miners figure out that the transaction is authentic, it gets validated and recorded to the ledger. Let us conclude that the ledger authenticated and recorded the

transaction.

Now, let us assume that Morty wants to send one Bitcoin to Jeremy. So, Jeremy validates a virtual address and an encryption key. Morty eventually transacts the Bitcoin by using the key and address that Rick gave him, and sends it to Jeremy.

Just like before, the transaction is sent to all the miners for validation. The miners evaluate the transaction via a reference number that points to the previous transaction from Rick to Morty. This is to ensure that Morty did not make any other transactions after that, which we call Double Spending. After the transaction is authenticated, every miner sends and receives a message of validation from every other miner. Similarly, the transactions for Morty and Jeremy are also validated for track keeping in the ledger.

This is how transactions in the Bitcoin world work. People transferring Bitcoins (or Bitcoin fractions) to one another. The ledger keeping track of the Bitcoins, but not the people or their balances. As a user creates a new key and address every time, the ledger will not be able to identify him/her, his/her addresses, or the number of coins he/she possesses. Thus, we define it as a transaction record that moves from one anonymous user to another.

Now, moving towards a solution for security:

The primary step that Bitcoin currency takes for securing the public ledger is decentralizing it. There is no sign of a master document or a large spreadsheet secured on a server. Instead, the public ledger is divided into chunks of blocks, which are hidden logs of transaction that contain Bitcoins in batches. Plus, every new block accompanies a reference to its previous block. This way, a user can follow the reference links and locate the very first one, when Satoshi Nakamoto designed this whole concept and Bitcoins were born.

We refer to this long chain of blocks as blockchain, which incorporates the public ledger for Bitcoins. As mentioned in previous chapters, each new block takes 10 minutes to mine, expanding it into a long chain over time.

You should know that every miner of Bitcoins possesses a copy of the complete blockchain on his/her computer. If the user/miner switches off his/her computer for some time and then powers it on once again, his/her computer sends a message to all other miners requesting they share all the blocks that were created during this period of inactivity. Therefore, there are no special privileges given to any particular miner or computer. Also, no specific miner keeps a record of all the updates related to the blockchain. The information is held in check by the numerous miners, publicly.

Factors That Influence Mining

As the activity of mining is intricate, it is prudent that you choose the right hardware. One has to keep in mind specific factors that affect the overall performance of a Bitcoin mining process. Let us discuss each factor.

Hash Rate:

Hash rate can be defined as the number of calculations performed by the hardware in one second. This rate is of high significance, as the higher the hash rate number, the faster the calculations, which will close the block and reward you much quicker.

Miners keep a look-out for a particular output from the hash function. For the hash functions, the same output is generated for the same input, yet they have been fabricated to show erratic behavior. Thus, miners try several random inputs to find a particular output for the hash function. You should understand that the competition in mining is robust, so to obtain a reward, a miner needs to search through all the random inputs as fast as possible. Thus, a higher hash rate facilitates faster search output – thus increasing the probability of being rewarded.

To measure hash rates, we use the unit MH/s (megahashes per second), GH/s (gigahashes per second), and TH/s (terahashes per second). You may have already seen these units displayed above, but now you understand their importance. Furthermore, a hardware's hash rate is particularly fabricated for Bitcoin mining, which can range from 336 MH/s to 14 million MH/s.

Consumption Of Energy:

The next factor of importance in Bitcoin mining is the investment in power input. Powerful hardware that you are planning to use for computations is going to need a convenient supply of electricity (energy). Before proceeding, you will need to understand the energy consumption of the hardware in watts. Plus, you will have to calculate your electricity bill as per the predicted number of watts. This calculation will help you to anticipate whether your investment in mining Bitcoins is less than the rewards you are going to earn or not.

Utilizing the consumption of energy and hash rate in numbers will help you figure out the number of hashes that you receive for each watt expended by your hardware. For achieving the numbers, you can divide the hash rate by the watts.

Here is an example:

Assume that the hash rate of your hardware is 4,000 MH/s with a requirement of 30 watts, so the consumption of energy will be 133,333 MH/s per watt. You can even use an electricity rate calculator online, or simply check your electricity bill to know the actual cost of your investment in the power supply for your hardware.

Hardware:

At one time, the concept of Bitcoin was too good to be true. People from a multitude of regions and cultures were attracted to this financial technology that offered freedom. There was no role of a centralized network, which relaxed users. Now, they had the power to check their transactions through an autonomous system that did not function through corporations, tax authorities, banks, and other third-party organizations. There is no one to keep an eye on how one spent his/her own money.

Moreover, in the past few years, the value of Bitcoin was not motivated by mere profit, but was admired due to the unique concept and philosophy it followed. Back then, computers were all that were needed to transact and calculate the exchange of Bitcoins.

As technology advanced, miners found that better GPU processors were able to calculate and mine Bitcoins at a faster rate. In fact, the results were almost 100 times more efficient than previously. Thus, mining hardware manufacturers came into existence, and they started designing hardware specifically for this purpose. This conclusively gave birth to the concept of cryptocurrency mining.

Nowadays, mining Bitcoins has become quite profitable. Many are even paying their regular bills through the rewards generated using mining of Bitcoins. The mining farms consist of graphic card processors and cooling units to keep the computation running continuously.

Apparently, a mining farm will require a vast supply of power, which is not usually available to individual miners. Thus, the big corporations invest in the energy utilization and virtually gather limitless resources to create mining farms. However, there is still a way for individual miners to make a profit. And that is by joining with other miners and combining their power. This is known as a mining pool.

Proof Of Work

You should also be familiar with the phenomenon ‘proof of work’ in the mining industry. A Proof of Work is a part of data that is quite time-consuming, costly and difficult to produce. It is needed for acknowledging particular needs. However, it has to be more streamlined to check whether it satisfies the specific requirements or not.

Production of a POW can be formulated randomly with reduced probability. Lowering the probability results in more chances of trial and error, which is essential to validate before generating a proof of work. Bitcoin uses a hash cash proof of work system, in particular.

The hash cash method used in Bitcoin mining helps reduce spam emails, as the sender will have to provide a valid proof of work in the contents of the email, including the To address.

Any legit email can show the proof without any difficulties. On the contrary, spam emails will not be able to do so, as there is a need for computations for generating the proof.

In Bitcoin system, the hash cash proof of work generates blocks. This proof of work is attached to an individual block’s data so that it can be validated. Its difficulty is also regulated so that there is a limit on the generation of new blocks. Thus, each block generation takes roughly 10 minutes.

Moreover, as the probability is set at a low value, the success of a generation of proof of work becomes unpredictable, as there is little information about the particular computer that will be generating the successive block.

Also, there is a requirement for validating a block, which is based on a lower hash value than the present target. In other words, every block that generates consists of the hash value from the previous block. This results in the chain of blocks that together incorporate a lot of computational work to produce Proof of Work.

Furthermore, altering a block will require reworking on all the following blocks. This way the blockchain remains safe from being tampered with.

The Difficulty Of Bitcoin/Crypto Mining

What Is Mining Difficulty?

Mining difficulty is defined as the measure of how hard it is to locate a hash under a given target value during the POW (proof of work).

Why Is Mining A Bitcoin Block Difficult?

Mining a Bitcoin block is difficult as accepting a block is only possible if its target is greater or equal in value to the SHA-256 hash of a block header.

In simple terms: Every block hash initiates with a specific cluster of zeros. With so many zeros, there is a very low probability of computation of a block hash. This results in many trials before generating a hash. For generating a new hash, the hash cash function used in Bitcoin mining increases.

The Metrics Of Bitcoin Network Difficulty

This network difficulty in Bitcoin mining is a comparison between the instance it takes to identify a difficult block and the easiest block. After every 2016 blocks, this measure is recalibrated to such a value that the 2016 blocks from the previous cycle would have emerged in two weeks' time if all miners were generating at the same difficulty. This way, each block generates every 10 minutes.

With more miners adding up, the block generation rate also increases. This will also raise the difficulty of a generation so that it can balance the increasing rate of block generation and push it back down. Furthermore, attempts to add fraud blocks by exploiters are straightaway declined by all miners in the Bitcoin network, so it is futile.

The Reward For Block Discovery

On discovery of a block, the user gets a particular number of Bitcoins as a reward. This reward is given to him/her after consent from all other miners in the network. At present, the reward compensation is set to 25 Bitcoins, whose value will be halved after the generation of 210,000 blocks.

Also, the users who carried out the transaction also compensate the Bitcoin miner with a certain amount. This compensation is given so that the miner can add the transaction to the block. Thus, as more Bitcoin miners join, the value of Bitcoin is likely to decay. Then, the compensation fees for adding a transaction is likely to be of high significance for generating an income through mining.

Chapter 3: What Is A Block Chain?

A blockchain functions as an open-source ledger where users record, control, and amend transactions. The blockchain is no different from other platforms, say for instance Wikipedia. Just as Wikipedia is an open source platform where a single publisher is not responsible for fabricating content, blockchain too does not give full power to just one miner.

However, as we move towards a deeper level, we find that Wikipedia is running on the internet through a client-server model of a network. Here, users are first provided with permissions to amend content in the website's pages that are all stored on an integrated server.

So, a user accessing the page on the website will be provided with an updated version of the original copy for any particular entry on Wikipedia. Also, the regulation of the whole database system stays with the administrators, who are granted permissions and access through the main authority at the center.

Wikipedia's system operates similarly to the databases of other centralized and secured systems like insurance companies, government, or banks. So, in such cases, there is a primary owner who has the authority to manage, protect, and access any update to the system against malicious activities.

However, the distribution system and the database involved with the blockchain technology are quite distinct. While Wikipedia's original copy is amended on the server, which is not visible to the users (clients), the blockchain offers updates independently. Every update to the system is done on the master copy, which is visible to all users.

This difference makes it very useful, as this method eliminates the requirement of third-party organizations for digital affiliation. However, we cannot consider blockchain technology as new.

On the contrary, it can be termed as a modern combination of innovation and proven methods. In

other words, it came into existence because of three technologies: a protocol to incentivize, cryptography with an encrypted key, and the internet. And Satoshi figured out this concept and changed it into a billion-dollar industry.

Thus, the blockchain technology prevented centralizing the system as building and securing digital relationships is absolute. Here all digital transactions are supplied using a robust, elegant and straightforward network framework that works as a peer-to-peer system.

Building Digital Trust

Maintaining trust in the digital world is often linked to authorization and identification. In simple terms, people online would like to know whether the person on the other end identifies himself honestly and if he can complete the job he claims.

The blockchain system offers a secure tool of ownership that completes all necessary authentication criteria. The encryption key is enough to identify the authenticity of the owner. Thus, there is no need to share detailed personal information that would otherwise have created the opportunity for hackers to attack.

Nevertheless, the relationship cannot be only based on authentication. There is also a need for enough money, authorization, correct address, transaction type, etc., which all requires distribution to balance it out in the overall network. This distribution strategy decreases the chances of forming a centralized body that would otherwise promote failure and corruption.

Furthermore, the distributed network should commit to security and recordkeeping. So, any authorization of a transaction will result in permission from the entire spread-out network.

Authorization and authentication, when carried out like this, allows the relationships to generate without the need for expensive investments. In fact, modern-world entrepreneurs have risen to indications of this technology, which is influential, innovative, and inconceivable. The blockchain technology has evolved as the base for all transactions carried out in the digital world, where it is building stronger digital relationships.

Chapter 4: How To Get Started

Now, I hope that you understand the basic terms related to the cryptocurrency mining industry. It is time to learn the actual steps for starting with the process.

Firstly, one should know that mining Bitcoins in the current climate would be too expensive. If you had initiated mining Bitcoins in the year 2009, when it started, you could easily generate tons of dollars. But, it is also true that you could have lost plenty of money. I would not recommend beginners who are planning on starting small to invest in Bitcoins. The level of maintenance expenses and investment needed, accompanied by the computational difficulty in the process, is not lucrative at standard-level hardware. Bitcoins are not more appealing to large-scale industries who have hundreds and thousands of dollars to spare in the process.

However, we do have alternative cryptocurrencies, like Feathercoins, Dogecoins, and Litecoins, that provide benefits at a much-budgeted level for beginners. Anyone interested in mining any of these altcoins can generate up to 10 dollars every day using the usual consumer-level mining hardware.

Here is how you set up a mining process for any of these coins.

Steps To Start Mining Altcoins

1. Set up a coin wallet, which is a private database, free to use. It is like a digital Piggy bank that is protected with a password to keep your earnings secure. It also stores the open network ledger used for recording the transactions.
2. A software package (usually free), which is usually made of open sources and pool mining regulatory platforms, like stratum and cgminer.
3. Online mining pool membership, where miners have built a community to combine their computers and increase their power, hence profits.
4. Authorization at some currency exchange online, where you can trade your earned coins for traditional cash.
5. Continuous and fast internet connection. At least 2 Mbps is needed.
6. An air-conditioned part of your home where the hardware will be set up.
7. A customized desktop created explicitly for mining. Your standard computer may not be used, as you will need to keep running the system for mining. Also, your laptop, handheld device, or gaming console will not be of any use as these units are not able to generate enough computations for earning profits.
8. A GPU unit or an ASIC chip, which is a processing device used for mining. It can cost from $90-$3000 for either of these two units.
9. A cooling fan to keep the mining system cool at all times. A lot of heat generates while mining, which is why a cooling device is needed for a successful mining process.
10. Staying updated with the technological changes in the mining industry is also a requirement. New techniques and amendments are continually happening in this industry, so you will have to be aware of them to be a successful miner.

Now, if you still want to dedicate your time to stepping into the big leagues and mine Bitcoins, then the following method will be of use to you.

Steps To Mining Bitcoins In Particular

Step 1: Buying Hardware

Currently, the best Bitcoin mining hardware for miners is the ASIC mining hardware. These machines work at solid computational speeds while keeping the consumption of power lower than GPU or FPGA mining systems. Many reputed companies have already manufactured great ASIC rigs for users worldwide.

ASIC systems serve the sole purpose of solving Bitcoin blocks. With the increase in the popularity of Bitcoins, their price also inflates. This triggers the rise in price of the ASIC mining hardware. For maintaining balance of cryptocurrency generation, its difficulty in mining inflates. Thus, it becomes almost impossible to beat the system without a decent ASIC machine to support the process.

Also, the ASIC technology used for Bitcoin mining is improving its productivity, efficiency, and speed with time, so that it can be considered the best hardware for mining.

Some popular mining hardware is AntMiner S5, AntMiner S7, AntMiner S9, Antminer U3, USB miners, VMC Platinum 6, BTC Garden AM-V1, Avalon 3, Avalon 6, Avalon 2, Asic Miner BE Prisma, and ASICMiner BE Tube.

Do note that current prices may vary, so have a look at each set of hardware before deciding which one to choose.

Step 2: Choosing A Bitcoin Mining Software

Now that you are aware of decent hardware for mining Bitcoins, let us move on to the software.

What Is Mining Software?

Even though the mining hardware for Bitcoins takes care of the real process for mining, mining software is also of high significance.

- For individual miners, the software does the work of linking the blockchain network to the miner.
- For pool miners, the software tends to link the individual miner to the pool of miners.
- However, for cloud miners, there is no need for software to mine.

The Significance Of Mining Software For Bitcoin

The primary work of mining software is to transfer the computed work of the mining hardware to the distributed network on the blockchain. It also receives back all the completed and validated work from the rest of the miners present on the blockchain network.

With Bitcoin mining software, the input and output operations of the miner are all monitored. Also, the crypto-mining software displays the temperature, fan speed, hash rate, miner speed, and similar statistical values.

Bitcoin Wallet

I mentioned a cryptocurrency wallet in the previous sections of the chapter. Well, a Bitcoin wallet also plays a significant role in keeping a check on transactions, etc. Moreover, a miner

will need to have a legit Bitcoin wallet before moving on to the software part. It happens because the software will request a valid Bitcoin address to send and receive payouts and rewards. Once you download or generate a wallet, you will be able to create a Bitcoin address.

You can find many Bitcoin wallets available online. Here are a few wallets, if you are confused about which to choose.

- **BreadWallet**: A popular Bitcoin wallet for iOS users.
- **Mycelium**: Android users love this Bitcoin wallet.
- **Electrum**: This Bitcoin wallet is suitable for Linux, Windows, and Mac.
- **Ledger Nano S**: Simple and secure hardware wallet suitable for all platforms.

You may have noticed that the Ledge Nano S is specified as a hardware wallet. This particular wallet is the most secure type of Bitcoin wallet, and is suitable for miners who earn a considerable amount of money through the process of mining. We will learn about it later in this guide. Now, let us move on to more about the Bitcoin software.

Some Recommendations To Get You Started

Mining Software For Windows

1. Bitcoin Miner

This mining software is excellent for using on Windows 8.1 and Windows 10. It provides a user-friendly interface with quick-sharing, mining pool, and power saving features. It also offers a feature called profit reports, which will predict whether your mining process is going to be lucrative or not.

2. BTCMiner

This open source miner for Bitcoins is popularly used for ZTEX USB-FPGA modules. Looking at its features, the BTCMiner boasts a frequency scaling mode that autonomously selects the most dynamic frequency for the hashes with the highest rate. Furthermore, it is a ready-to-use software where there is no need for a license. It also accompanies FPGA boards that support it through a USB interface for programming and communication.

3. CGMiner

Any miner comes across this software in the mining activity, as it is arguably the most common of all among miners. It has been designed using the original programming algorithms of CPU Miner. A few of its many features are:

- Support for CPU mining
- Support for multiple GPUs
- Self-detection protocol for finding new blocks, including a mini database
- Interface capabilities that are located remotely
- Regulated fan speed

4. BFGMiner

It resembles CGMiner in operations. However, unlike CGMiner, it has been built specially for ASIC rigs and not for GPUs. A few other features of this software are:

- Fan regulation
- Combined overclocking power
- ADL reordering device by PCI-based bus ID
- Free mining with LLVM Open Cl/ mesa

5. EasyMiner

This is a graphics user interface-based software that encases other software like BFGMiner and CGMiner to make it more efficient. It supports both stratum protocol for mining as well as getwork protocol for mining. Plus, it is efficient for both individual and pool-based mining. Its main features comprise of delivering excellent graphs for monitoring performance through simple visualizations, and it provides with miner configuration.

Mining Software For Linux OS

1. CGMiner

Just like for the Windows platform, CGMiner is a popular and standard mining software that most miners prefer to mine Bitcoins. CGMiner reflects the standards of the original programming algos used in CPU Miner. The features for this software are the same as the ones mentioned in the Windows platform section.

2. BFGMiner

See information about it in the Windows OS section.

3. EasyMiner

See features in the Windows mining software section.

Mining Software For The Mac OSX Platform

1. RPC Miner

RPC Miner shows feasible compatibility with Mac OS of versions 10.6 or higher. It offers combination features with systems and APIs based on MAC OS.

2. Cash Out your Coins

This particular software will require a miner to cash out some Bitcoins to pay for the energy consumption, such as electricity.

Besides these, the Mac OS platform can run any of the software discussed in the previous platforms. So, you can read about them from previous sections. You can choose the software for beginning your mining activity by comparing their features and other requirements.

Step 3: Joining A “Mining Pool”

In previous chapters, I mentioned the term mining pools but never got the chance to elaborate upon them appropriately. Thus, let me explain the concept briefly.

Mining pools are parties created by miners to work and mine Bitcoins and other cryptocurrencies together. Thus, their combined power results in sharing the rewards based on the hash rate contributed by all miners. For an individual miner, it will be tough to find blocks, unless that particular miner is filthy rich to set up a super powerful mining farm. So, to increase the probability of finding blocks, miners mine together to achieve results at a much faster rate.

So, your most feasible step to mine Bitcoins is by joining a mining pool.

How Are You Rewarded In A Mining Pool?

It depends on the speed of generating hash rates. Hash rates are directly proportional to the chances of finding a new block, which in turn will bring out better rewards. Do note that each mining pool website that you are planning to join will ask for a particular pooling fee. So, expect to pay that as well.

Which Countries Are Mining The Most Coins?

Bitcoin mining gives more weight to countries with cheap energy consumption, such as electricity. Apparently, this has led to the centralization of the mining industries to only 10 to 15 major mining companies, which have taken over a considerable amount of hash power present in the blockchain network.

As most of the companies are concentrated in a few countries, only these few countries mine and export Bitcoins. Here is an insight into the major ones:

China

China is the leading miner of most of the Bitcoins, and hence acts as the major exporter of cryptocurrency coins as well. China owns many major pool-mining communities, which have been estimated to own around 60% of the hash power. This also means that 60% of newly mined Bitcoins come from China.

Georgia

Georgia is the residence of the famous Bitcoin mining company, BitFury, which not only controls 15% of the mining activities but is also one of the biggest manufacturers of Bitcoin chips and mining hardware.

Sweden

Sweden's Stockholm is where KnCMiner, one of the significant Bitcoin mining players, has spread its roots. It contributes to 7.5% of the mining of Bitcoins.

U.S.

21 Inc., located in the U.S., is a BTC mining company situated in California. The firm not only executes a considerable amount of mining activities but also produces and sells low-powered miners for Bitcoin, which is a product of their 21 Bitcoin computer line. The majority of hash power generated from the 21 Bitcoin systems targets the mining pool owned by the company. Their mining power can contribute 3% of the total mining activities.

Rest Of The World

The companies mentioned above take care of 80% of the Bitcoin mining processes. The remaining 20% is spread out around the rest of the countries.

China's Mining Pool Concentration

In later sections, I will discuss the best pool mining communities to join. But, before we proceed, you should know that China is the leading region for major pool mining activities. Also, most pool websites are in Chinese only. This may be a big issue, as the major part of centralization for mining is in this country.

This is possible because of the low electricity costs in its region, which has attracted more mining activity than any other country. Not to mention, China is the major manufacturing hub and can produce the hardware units needed for computations at a much lower price than other countries.

It’s rumored that some Chinese power companies point their excess energy towards Bitcoin mining facilities so that no energy goes to waste. Currently, 20 mining pools stand out as the most famous ones. Out of these almost 81% of the hash rates from the mining pools are controlled by Chinese regions.

Top 10 Mining Pool Communities Active At Present

Now let me introduce you to the ten major mining pool communities.

1. Antpool

Located in China, Antpool is the most active pool mining platform, and is currently functioning under BitMain. Antpool mines around 25% of the blocks.

2. BTC.top

BTC.top is a mining pool community owned privately by its members. It is not accessible to common miners.

3. BTC.Com

BTC.com is publicly accessible to join for pool mining.

4. Bixin

Bixin is another Chinese pool-mining platform that is publicly available. However, you will need to speak Chinese here to interact with other miners.

5. BTCC

BTCC boasts itself as China's third-biggest exchange platform for Bitcoins. Its pool mining community currently handles about 7% of all available blocks.

6. F2pool

DiscusFish, also referred as F2Pool, is another Chinese platform for pool miners that has succeeded in finding around 5 to 6% of the blocks in just six months.

7. ViaBTC

ViaBTC is a new mining pool platform, which is focusing more on Chinese miners.

8. BW Pool

BW emerged in China in 2014. It has almost a 5% share of the block mining under its name.

9. Bitclub.Network

Bitclub Network is another platform that has shown results and is quite large. But, there have been rumors about it being malicious.

10. Slush

Slush Pool has been there since the beginning. It is a trusted platform for beginner miners. Despite being the first pool mining community, it only racks about 3% of the blocks.

Recommended Pool Mining Community For Beginners

While it feels natural to choose a mining pool platform that has a major share in the activity, it is not always best practice to do so. I recommend going to Slush Pool mining community, which has been present since the very start of the pool-mining project. Slush Pool is operated by

Satoshi Labs

The Process Of Joining Slush Pool

Anyone can easily join Slush Pool. All you need to do is:

1. Sign up for an account.
2. Setup configuration for your preferred mining software so that it points the hash power produced by your hardware to the Slush Pool's mining platform.
3. Share the address details of your Bitcoin wallet, which will be provided with rewards and payouts.

List Of Urls Offered By Slush Pool

To be a member of the mining community at Slush, you will have to show your software the way to the regional URLs offered by the website. This way, you can enhance your mining profits.

Mainland China

stratum+tcp://cn.stratum.slushpool.com:3333stratum+tcp://cn.stratum.slushpool.com:443

Usa (East):

stratum+tcp://us-east.stratum.slushpool.com:3333

Europe

stratum+tcp://eu.stratum.slushpool.com:3333

Singapore/Asia-Pacific:

stratum+tcp://sg.stratum.slushpool.com:3333

How Much Pooling Fees Does Slush Charge Its Miners?

Slush asks for pooling charge fees of 2% on all rewards and payouts. Slush Pool transparently organizes its mining pool community with its users. That is why it shares the transaction fees with individual miners on receipt of rewards.

Slush Pool’s activities are executed under Satoshi Labs. The firm is also responsible for the creation of a hardware wallet for Bitcoins named Trezor.io, and also owns coinmap.org.

Step 4: Setting Up Your Bitcoin Wallet

By now you know that wallets are your encrypted storehouses that contain all the payouts and rewards. Now, we are going to look a little deeper into their types.

There are two types of cryptocurrency wallet, which are: Cold or offline wallets and Hot or online wallets. Let us learn how the two types vary from each other.

The most fundamental difference between the two is that the hot wallets are linked to the online world, while the cold wallets restrict that connection. Most miners use both types of wallet, which provide them with varying purposes.

Hot wallets are more like checking accounts that you use more often. On the other hand, a cold account is like a savings account for keeping all your digital assets safe. Miners usually keep a small amount of currency in the hot wallets for trading. And a significant amount of their digital money is stored safely in the cold wallets.

Now, you must be wondering about the security aspects of the two. Let us explore a little more deeply.

Why Do Miners Keep A Large Sum Of Their Bitcoins In Cold Wallets?

The answer to this is simple. This way the attackers will not be able to steal their digital assets, as there is no online connection to exploit the wallet.

Does That Mean Hot Wallets Are Not Safe?

For determining how secure a hot wallet is, one will have to study the reputation and behavior of the third parties and individuals who are connected to the hot wallet. Anything that is linked

online is prone to hacking and attacks. So, miners usually prefer keeping a small amount in their hot wallets, as an attacker will not waste his/her resources just to get hold of a small amount.

Types Of Hot Wallets

Account-Based Hot Wallets

Accounts that are stored in the online asset exchange companies, such as Bittrex and Poloniex, are deemed as hot wallets as they record all the funds of a user in their servers and infrastructure. If an attacker hacks the Poloniex system and drains all the assets stored there, then your account is most likely to be affected by the attack as well, as Poloniex is holding your funds for you directly.

A Coinbase account is also a type of hot wallet. So, if Coinbase is attacked, you could lose your funds too. This is why many practices keeping a small number of their digital assets in Coinbase and similar hot wallets.

Using Coinbase to trade and exchange Bitcoins is secure, as long as you immediately move the money out of the wallet once the trade is completed. Many have found Coinbase to be a secure platform for business. However, it still questions the ethics whether it is fully secure and worth risking storing huge sums of money in it. I would suggest using Coinbase if you are a beginner miner, as the firm offers a user-friendly app and website for users, especially in the U.S.

Software-Based Hot Wallets

There is another type of hot wallet, such as Exodus.io, which is software downloadable and installable on a computer. Another name in the software types of hot wallet is Dash QT wallet. In this wallet, Exodus does not practice storing the private keys of the miners on the servers. Thus, the miners control their own money. However, there is still a risk of getting phished, as your

wallet is connected to the internet, which can be a medium for a potential hacker to attack your computer and gain access to it. Exodus wallets are fabricated to communicate with the various blockchains directly. It also acknowledges many digital cryptocurrencies, except Bitcoins.

You can consider several factors when choosing a software wallet. Exodus has been a popular choice among many users because it is user-friendly and has been combined with Shapeshift. This combined feature lets users avoid migrating to an asset exchange division externally, such as Poloniex or Bittrex to facilitate trading. With Exodus, miners have the benefit of not leaving the unsecure system. It surely is a great wallet, but it still needs to update its features to make the hot wallet more secure for users.

Types Of Cold Wallets

Hardware Wallets

While there are many types of cold wallet, the main one that we will focus on is the hardware wallet. This wallet has a physical body that is not connected to the internet. However, it does have a plug-in feature that lets it connect to the internet when required.

These wallets are very secure, as whenever a transaction is made, the wallet asks for confirmation from the user by instructing him/her to press the button present on it. You can consider them hack-proof. These encrypted devices are great for storing large sums of assets.

Three popular hardware wallet brands that miners usually choose are: KeepKey, Ledger Nano S, and Trezor.io.

Each one of these hardware/cold wallets has its unique features. For instance, Trezor.io has an outstanding reputation, and it was designed at Satoshi Labs. Trezor provides exceptional customers service and supports a multitude of currencies, namely – Testnet, Dogecoin, Namecoin, Litecoin, ZCash, Ethereum Classic, Ethereum, Dash, and Bitcoin.

Step 5: Start Mining

By now, we have learned all the beginner-level stuff about Bitcoins and their terminology. Do note that there is much more to learn in this network of cryptocurrencies, but all the above information is enough to get you started.

Now that we know which devices, software, and other equipment are needed for mining, it is time to start the actual mining. This last step is where you will learn about ways to improve your knowledge and stay updated about Bitcoin mining and news. This currency and all the rules surrounding it are quite volatile. They tend to change often. Therefore, you will have to try your best to stay as updated about new techniques, latest news, etc., as you can.

Even though Bitcoin has been considered a risky investment, you cannot deny that the interest in this digital currency is increasing every day. You read this book until now because you want to learn about it. You have probably already set up all the accounts and hardware to start with the mining procedure, but before you continue, you should know that keeping yourself updated with any new developments in the mining space is of high significance.

Staying Updated

So, as stated earlier, the last step is all about staying updated and mining according to what you learn from such updates. This is not as simple as it may seem. You will have to dig deep into the layers of the cryptocurrency world to find information of importance to you in your mining activity. This can be very time consuming, especially when you do not know where to start.

Fortunately, this book gives you tips on how to proceed with the research work. So, let us continue.

Learning Through Widgets

My Bitcoins Gadget (For Windows)

With this widget's aid, you will get to know the number of coins you possess, their current worth, and it also lets you link to your pool mining community to reveal data and rewards, if any. Domchi, a member of BitcoinTalk, developed this widget. A new update has also been released for this widget after the previous update Mt.Gox collapsed. At first glance, the website may look malicious, but many BitcoinTalk administrators have already tested it and found that it is clean, simple, and safe to use.

Bitcoin Ticker (For Mac)

For MacBook users, the Bitcoin Ticker performs quite efficiently. This widget stays at the top of the screen on your Mac OSX and displays the prices of up to seven types of cryptocurrency exchange.

Learning From Internet Browsing Websites

Here are some popular news websites, which offer Bitcoin news and updates regularly.

Coindesk

This cryptocurrency-related news website stays up-to-date about anything related to Bitcoins and the cryptocurrency industry. A number of articles are published every day which talk about more than just recent updates. Many long-form pieces present on this website are worth reading, as they teach a lot about the world of cryptocurrency, its future, tips to improve mining, etc. Coindesk is also a great place for beginner miners to start. Their Blockchain 101 has been listed

as a great article for newbies. Here, the most commonly asked questions related to the Bitcoin world are answered. Besides the cryptocurrency section, readers can also go through their other sections, which are Data, Research, Business, Markets, and Technology.

Cointelegraph

This site is an independent news platform targetting applications related to decentralization, the blockchain network, and cryptocurrency. It started in 2013 but has since garnered a massive audience, making it stand out as the second most visited Bitcoin news website. Cointelegraph publishes a mixture of cryptocurrency-based commentary, market data & analysis, expert opinion, and breaking news. Cointelegraph also provides a user-friendly ICO calendar that gives all updates related to the launch of potential new coins.

Bitcoin Magazine

This magazine is more focused on Bitcoin in particular. The other cryptocurrency coins are occasionally covered, but a significant part of the website focuses on news updates related to the first cryptocurrency. This website consists of articles that are divided into five broader classes, which are: Technical, Opinion, Price & Data, Guides, and News. Each class further divides into subclasses that provide various topics of interest. So, there is plenty of information on this website, despite its coverage limited to just Bitcoin. It started in the year 2012 and publishes four articles every day, currently.

TheMerkle

This website is considered to be the youngest of all the websites on this list, as it was launched in

2014. The site covers the whole cryptocurrency sector, but there is an occasional turn towards news and reports related to other markets as well. Besides the usual categories of news, you may also find its review section educational. TheMerkle studies the finest cryptocurrency wallets and exchanges and reviews them. The site also provides comparisons on various virtual currencies and other financial equipment of importance. For instance, one of their comparison articles talked about the difference between stock-driven IPO and crypto-driven ICO. This site updates with up to 15 articles every day.

CryptoCoinsNews

CCN is a sister website of Hacked, but while the latter targets advice on trading and analyzing coins, the former is all about providing news coverage. The significant currencies covered in the news on the website are Ethereum, Litecoin, and Bitcoin. However, there are also updates related to other alternate coins from time to time as well. The site is more focused on a professional approach compared to the others on this list. For any reader who wants to study offerings of new products, changes in price, and mergers, then CCN is the place for you. CCN also offers an educational portal, just like CoinDesk. Though it may not be as detailed as CoinDesk's, it still provides vital information on the crypto sector.

Official Bitcoin Blog

This may be the official Bitcoin blog, but it only updates when there is a major announcement or news update regarding this currency. The Bitcoin team hardly updates a single post every couple of months, but when it releases, it gets aggregated coverage from all other news websites instantly. Nevertheless, if you are into Bitcoins, then you should definitely bookmark this website for updates. In addition, this is the only official platform that will offer you genuine

updates about these digital coins. You can just add it to your current RSS feed and stay updated.

Bitcoin Talk

Bitcoin Talk is not really a conventional news website, but a forum, and a reputed one, at that. Over 1.5 million forum members actively operate on this website to cover and share the slightest update related to the cryptocurrency world. There is also a subclass for every possible section related to Bitcoins, such as trading updates, mining news, technical discussion, etc. A unique and helpful section that this website possesses is the Press Hits page, which offers one of the most broad-scale cluster of news articles for your knowledge. When you scroll down further on the website, you can also find a little section that dedicates itself to other cryptographic currencies and coins. Members share and discuss all major updates in that section.

Reddit

Anyone familiar with Reddit already understands the vast cluster of data available on it for educational, entertainment, and other significant purposes. Subreddits related to Bitcoins and the cryptocurrency industry are no different. You can find plenty of them available on the website, which you can join and stay informed. A few of them that will update all major and minor news related to the crypto sector are /r/CryptoCurrency, /r/Bitcoin, /r/CryptoMarkets, and /r/BitcoinMarkets. Do visit /r/Bitcoin if Bitcoins are your number one mode of interest in this industry. Nevertheless, try subscribing to as many subreddits as you desire. You may never know when you get vital information from any of them.

Learn From Your Mobile Phones And Smart Devices

These mobile applications, which I am going to share below, are great at providing you with news updates and information on the run. Websites are most suitable when you are at your home

computer or laptop. But apps provide you with a user-friendly layout that can be viewed whenever you get time. That said, here are a few popular mobile apps to get you updated with Bitcoin information.

Bitcoin Checker (For Android)

With over 50,000 users and a rating of 4.7 by 3,400+ downloaders, Bitcoin Checkers offers you information related to the latest cryptocurrency prices. In addition, you can set alarms on this app that notify you about any major or trivial change in the cryptocurrency market, for which you can set up specific prerequisites. For instance, the app can notify you with an alarm when there is a rise or fall in the coin price by a certain amount.

Zeroblock (For Both iPhone And Android)

The ZeroBlock app not only keeps you updated on the real-time market prices, but also the latest news related to the world of digital currency. In addition, you also get a Bitcoin calculator incorporated in this application. This app has seen more user following among iPhone owners, who also use it for staying updated about current prices.

My Recommendations

No doubt, there are many portals from where you can gather Bitcoin information at your convenience, but let us look at the ones that I recommend you to try out above all the rest.

WeUseCoins

WeUseCoins was one of the first portals I found very useful to polish my Bitcoin knowledge. You are able to acquire news updates, starting guides, FAQs, Mining tips, and buying guides for Bitcoins as well as altcoins. Some of the most influential Bitcoin experts and miners share their experiences and tips on this website. In addition, you can certainly learn a lot from them. To get you started, you can read their posts about some of my favorite and 100%-noteworthy topics:

1. Decentralized Bitcoin
2. Tips on Securing Your Online Mining Presence
3. Why Wont Bitfinex/Tether Publish Already Existing Reports
4. Should You Buy Bitcoin with a Credit Card
5. How Latin American Growth Will Advance Through Bitcoin
6. The Process of Accepting Bitcoin Payments for your Business
7. BCash Hard Fork
8. A Guide to Claiming and Selling Bitcoin Forks
9. Top Cryptocurrencies Besides Bitcoin
10. Purchasing Litecoin

The Subreddit: /R/Bitcoin

I already mentioned it, but now I highly recommend that you follow this portal for all the latest updates regarding Bitcoins in specific. It is one of the highest-ranking platforms on Reddit, and this reputation makes it worth subscribing. You should note that other Redditors share external links here that will give you an idea of the most fascinating news leaks related to cryptocurrencies.

Coindesk

With an estimated visitor count of a few million every month, Coindesk is the largest and the leading source of Bitcoin information. A great thing I like about Coindesk is that there is no sponsored submission on this platform. This makes the posts more trustworthy to read. It may sometimes be hard for you to keep track of the number of posts updating on this website. A way to cope with that is by subscribing to their newsletter and reading the posts you find useful, while briefly glancing over the trivial ones.

DCMagnates

This website platform offered me not only the latest news about Bitcoins and altcoins, but also advice and guides on trading in these coins. It has a great collection of articles comprising of news updates, trading assessments for Bitcoin, and other currencies, such as Litecoin. You should sign up to their newsletter to stay updated about any new posts.

Recommended Bitcoin Calculators

Some of the above websites and apps offer Bitcoin calculators, but I found more useful information related to Bitcoin trading analysis and calculations at the following portals.

BitcoinX

BitcoinX's profitability calculator provides the most extensive information based on the information you enter. The fields that it calculates and covers for your information are:

- Difficulty
- Mining Factor
- Average generation time for a block (solo)

- Hardware break even
- Net profit first time frame
- Coins per 24h at these conditions
- Power cost per 24h
- Revenue per day
- Less power costs
- System efficiency
- Mining Factor
- Average Mining Factor 100
- Power cost per time frame
- Revenue per time frame
- Less power costs

These fields are enough to give you an idea of whether you will make any profit from your status in the Bitcoin world or not.

The Bitcoin Wisdom Calculator

This calculator offered by Bitcoin Wisdom not only updates the usual profitability information, but also targets the latest prices of interesting hardware related to Bitcoins and other cryptocurrencies. It is worth visiting if you are planning on upgrading your equipment and want to find all competitive prices in one place.

Conclusion

Bitcoins have been helpful in reaping benefits that were never imaginable before. In fact, many major-scale industries are actually making millions by mining and exporting cryptocurrencies. Many people find these useful, because they have an international currency status. A person with Bitcoins can use them in any part of the world by converting them into the conventional currency of that region. In addition, the security of the blockchain network is top-notch, which ensures that your money is sent to or received from the right person, and that too without the need of disclosing either one's identity online.

Many have seen the numerous benefits Bitcoins provide. A major one is that there is third-party influence, which would have charged a fee for a transaction otherwise. This is why Bitcoins are supported by many small and large-scale industries who do not have to rely on intermediaries any more. Support from users strengthens the existence of Bitcoins, and if all people in the world start using it, then the day is not far off when Bitcoin replaces all currencies as the official one.

But, there are still disadvantages due to skeptics at the moment. Many hesitate to learn and become involved in it because it is an innovative and self-governing technology. But, with time, this issue can be resolved as more and more people embrace it.

Long Learning Curve, But Surely Worth It!

The concept of Bitcoin has a long learning curve that makes sure that the competitors are out of the picture. In addition, the rising value of Bitcoins has been possible because there was very little saturation involved in this crypto currency exchange. With such a rising value, there is no doubt that many investment companies are promoting this cryptocurrency among the people to their fullest. Long-term investment in this currency will certainly garner enough assets.

The long learning curve may be complicated to grasp. But, this digital asset's performance is not influenced by individual companies, bonds/stocks, or the economy. No physical place is present that stocks these currencies in one place. And there is certainly no chance of hacking or exploiting anyone's assets (not that I know of), as the chain is spread throughout the internet. Here, everyone is an owner without any centralized banking system to control it.

Keeping the five steps you learnt above in mind will ensure that you reap maximum rewards by mining your favorite cryptocurrency. But, you need to invest in this field smartly. Being emotional will not mean that you earn more. Invest with a mindset that you may occasionally lose as well.

The Crypto world is like the Wild West, where you are free to explore, invest and earn as much as you like. You chose this book to learn about this independent world and found useful tips to get you started. My book will help you on the way, if you choose it to, but remember that the final decision to choose the right path is yours.

In the end, I would like to appreciate all my fellow readers that chose this book to learn about the concepts of Bitcoin and cryptocurrency mining. It may not have the advanced-level stuff, as it was meant to stay simple so that beginners can learn about it and move on to the next step.

I am glad you showed your interest in joining the new digital currency frontier, which has great

potential in the future. Staying put before the calm will offer you a head-start, so that you know how to trade in the world of Bitcoins and other cryptocurrencies.

The ICO Approach

A Beginner’s Guide to Understanding Cryptocurrency ICO

Chapter one: Introduction

Definition Of Initial Coin Offering

Initial coin offering, commonly known as ICO, is the mechanism used to raise funds for financingcryptocurrency-related ventures and it is mostly used by startups as a way of evading the regulated capital-raising mechanisms used by banks or venture capitalists. For example, the Ethereum cryptocurrency project has already raised a lot of money in ICO. This investment model is closely related to Initial Public Offering (IPO) whereby interested investors purchase shares of a certain company. In ICO, the resulting coins are called tokens and they can be equated with the shares of a company that are sold to the investors. ICO has dominated the blockchain community, and many view ICO projects as securities that are unregulated. This can enable the founders to raise the capital required to undertake a certain crypto venture. To make it simple, crowdsourcing eliminates the hustle that is very common in the capital venture process. In every ICO campaign, a given cryptocurrency percentage is sold to the initial funders of the project as an exchange for a legal tender or another cryptocurrency like Bitcoin.

Every cryptocurrency startup must create an elaborate plan in its white paper explaining what the project is about, the problems that the project will solve after its completion, the amount of money needed to fund the venture, and the percentage of the coin that the pioneers will keep for themselves if the project succeeds. However, if the venture fails, the funds are returned to the financers and the ICO is said to have been unsuccessful. If the funds are enough, the project is initiated or the funds can be used to complete the project.

Generally, ICOs can be easily structured with the aid of technologies like ERC20 Token Standards, which ease the process of developing any cryptographic assets. Investors contributeto the ICO development by sending their funds in the form of Ether or Bitcoin to a set smart contract that can store their funds and, later, distribute the equivalent value of the new token.

Anyone can participate in an ICO because this venture has few restrictions, if any, assuming the fact that the token is not a security. Compared to the global pool that many investors find themselves in, with ICOs one can easily raise astronomical profits if things go well. However, there is a large margin of risk because they are extremely speculative since most of them raise pre-product money. But before discussing ICOs in detail, let us look at the historical context of how the entire trend started.

History of ICOs

The year 2014 turned to be one of the most dramatic points in crypto history because this was the time the ICO projects begun. Earlier on, many projects employed the crowd-sale model to fund their projects. A good example is Ripple, which pre-mined about one billion XRP tokens which were sold to potential investors in exchange for Bitcoin or flat currencies. Early in 2014, Ethereum raised about 18 million dollars and this turned out to be the largest ICO completed at that time. The DAO was the initial attempt at raising funds for an upcoming token on the Ethereum system and it aimed at creating a decentralized and elaborate organization that would also fund other blockchain projects. However, the decisions and governance of the coin would be executed by the pioneers themselves.

DAO became a great success and managed to raise more than $150 million. However, due to much technical vulnerability, an unknown hacker broke into the system and drained millions from the DAO organization. The foundation opted to still focus forward despite this drawback. After the failure of the attempt to raise money to fund tokens using the Ethereum platform, the blockchain community realized that it was easier to raise the tokens compared to following the venture capital funding model. The ERC20 standards make the process of developing ICO tokens easy in the Ethereum platform which is blockchain based. When Ethereum opened the door for smart contracts, it unveiled a great potential for a generation of ICOs. With the ease of use of this system on top of a few regulations that have been set, startups have raised a large amount of funds within a short period and Aragon, as a perfect example, managed to raise about $25 million within 15 minutes. Out of the simplicity of creating tokens on the Ethereum blockchain platform, a wide variety of tokens have been created to serve different purposes.

Chapter 2: ICOs in Detail

We always encounter many news about ICO ventures, but due to insufficient explanations in these news publications, it becomes difficult for many people to understand everything about ICO in detail. This eBook sets out to explain how ICOs work and why they are opted for as a fundraising model.

How ICOs Work

An initial coin offering can be viewed as a refined form of crowdfunding that has emerged outside the common financial system. This technique has enabled companies to undertake some great projects and, through crowdfunding, they have secured the funding required to fund their projects.

ICO can be said to be the cryptocurrency version of crowdfunding that has been well incorporated into the crypto world, and this model is here to stay. An ICO event extends up to one or more weeks whereby everyone is always allowed to buy new tokens in exchange for Bitcoin or any other established cryptocurrency. Every ICO has a specific limit or goal for the project funding and this means that every single token always has a pre-determined price that does not change throughout the initial coin offering periods; this is what makes the supply of the token static.

There can also be a static supply with a dynamic funding objective, whereby the distribution of the token will depend on the amount of funds received and this results ina higher token price if the project receives more funding.

What is an ICO presale period?

As implied by the name, pre-ICO sales give the investors a chance to buy the tokens before the onset of the official sales. A pre-ICO sale is based on a smart contract to keep the funds separate from the official sale to avoid confusion. Generally, few funds are gathered at the presale stage because, during this period, the ICO tokens are sold at a lower price on top of certain bonuses to the investors. Different organizations initiate the presale for different reasons. Just to give you a glimpse, these are some of the common reasons why companies initiate presales prior to the official opening of the crowdfunding.

- It is used as a promotional tool by most of the companies. An ICO is always an easy way of distributing capital and ensuring that the investors will stand for the upcoming project. An ICO presale is more of “buy one, get one for free” kind of approach. The presale thus ends up raising awareness about the ICO. This is always the best period to invest in an ICO because the tokens are sold at a lower price because the companies give offers that will attract the attention of the investors. After the implementation of the project, the companies increase their profits after getting enough long-term investors.
- Some of the companies may opt to initiate a presale as a way of testing the potential that the ICO has. Simply, they aim to understand whether people are interested in their ICO and whether they are willing to invest in it.
- This undertaking is also a tool that attracts and keeps long-term investors’ whole belief in the idea, products, or services offered by the company.

Generally, the main aim of a presale in an ICO is to attract angel investors who fund the operational costs of the company when the white papers and roadmaps are being worked out.

While an ICO presale is a great way that the company can raise some funds to jumpstart its

operations, the company can also be hurt, especially if many tokens are sold at a low price during the offer period. Most of the companies begin their presale period about a month before the official release of the ICO, but such an opportunity cannot be available to every person because the presale may be accompanied by some limitations. To participate in this, one needs a KYC (know your customer) approval and secondly, to meet the minimum amount needed. For instance, the lowest set amount could be $10,000 and the maximum amount cap per person could be about $1,000,000.

Pros of an ICO presale

- Liquidity. As an investor, one can trade tokens in secondary markets instead of fixing up a given value in equity of a certain company.
- Ensures there is a good distribution of capital. When an ICO presale is well organized, it opens a great door that facilitates allocation of capital in a rational manner. With ICOs, there is no any demographic or geographic barrier and anyone can be involved in this investment, regardless of their nationality.
- A crowd-funded ICO startup has many supporters. In ICOs, many people are involved and incentivized to be participants of the project and the company ends up getting many supporters who are committed and engaged with the happenings of the company.

Cons of an ICO presale

- Many scams and frauds. Scammers sometimes take advantage of such opportunities to illegally raise money which ends up in the pockets of certain people and not in the project that was initially presented to the vibrant investors.
- Restrictions and risks. Economists always argue that the greater the margin of risk, the greater the reward. In simple terms, very risky projects always have a high potential for producing great returns. Based on this risk, it is advisable for one to be cautious when investing in ICOs because some projects may end up failing and the presale investors' end up losing large sums of money, especially when the companies fail to refund the investors.
- Loyalty related issues. In the presale phase, most investors buy large amounts of tokens at a cheaper price because of the favorable offers that are used to attract investors at the beginning. When the prices rise, most investors immediately sell all their tokens, thus defaulting the company.

For any ICO to succeed and bring awesome profits, some key parameters need to be accounted for. These are some of the key things that one must pay attention to when deciding which a good is or a bad presale and whether it is worthwhile to invest in or not:

- Reviews. When considering whether to buy a certain product or undertake a certain investment, reviews act as a guide to whether the product is worth it or not. Presale ICOs are not an exception to this determinant. As an investor, make sure that you check all the critiques and opinions given by the investors who have preceded you in investing in the presale under question. Out of the reviews, make sure that you have a general idea or glimpse of what other people perceive and think about the ICO. This will act as your

navigator and you will finally end up making a wise decision.

- Funding by well-established companies. Ensure that you carry out your research to find out if the company that is behind the pre-ICO in question has any parent organization or partnership with a bigger company. This is yet another criterion that indicates whether the ICO company is legit or not. More often, ICO presales that have partnered with well-established companies end up being very successful. Such ICOs have a lower probability of fraudism and are likely to have exceptional offers.

- Rumors. Always keep your ear open to what people are saying about a certain ICO presale in social media and other forums. Consider whether people find the ICO presale trustworthy, suspicious, or interesting. Even if rumors are not a credible source of information, sometimes they can bear some leaked information about a given ICO. At the same time, remember to read what ICO experts are saying about a certain presale.

- Hype. Make sure that you have a good understanding of what the product is and what the company is offering and try to figure out whether it is worth that. Concurrently, make sure that you avoid the “too good” kinds of offers as most such exciting projects end up being big scams that rob people their hard-earned money. If the ICO presale is good, you will encounter it in social media and various cryptocurrency forums. A good presale will also have a good customer support desk that is responsive and ready to answer all customer questions.

On the other hand, after the presale period, the ICO is then released to the public whereby anyone can buy the tokens if they are willing and able to meet the established requirements. During this going-public-period, the tokens are always sold at a higher price when compared to the presale period where only a few people were willing to risk their funds in investing at that initial point.

After carrying out your research, settle on a certain ICO that you are confident enough to invest in and if the ICO is good enough, think of making a presale purchase of the coins because, at this point, you will be able to buy the tokens at a relatively cheaper price, regardless of the quantum of tokens that you need. Sometimes, at this point, willing investors may be offered up to a 50 percent discount and if one purchases a handsome number of tokens at this point, one is assured of reaping great profits when the tokens are released publicly where their value becomes a multiple of the original value at the presale period.

The bottom line on this issue of ICO presale and public sales is that buying the tokens before the official launchoffers more value for your investment than buying them after launching.

Maximizing Your Profits If The ICO Takes Off

An ICO is a great venture with amazing profits if it is well undertaken. For example, if you purchased $100-worth of BTC on 2011, it would have cost $0.30 per BTC, and with your $100 investment, you would have received 333.33 BTC then. If you kept these Bitcoins for seven good years, by 2017 the price of BTC had shot up to about $11,000 and your initial $100 would be currently worth about $3.5m. By simple mathematics, this is a 35, 000 percent profit within seven years! This makes ICOs and the entire crypto world one of the most profitable investments in history. This meteoric rise of Bitcoin excites investors about cryptocurrencies and with heavy and smart investment by buying promising tokens. But just to guide you, this is how you can grow your crypto investments and maximize profits and make moneywhen the ICO of your choice takes off.

We have seen much about ICOs, and when you participate in an ICO, you receive coins or tokens as a contributor to the project. Now, after receiving the tokens, you must get your investment back and maximize profits. How do you retrieve your investment after receiving the tokens? How do you maximize profits after receiving the ICO coins? Among others, these are some of the common questions that every ICO investor cannot avoid asking themselves. These are good questions and, in this eBook, you will learn how to do all this as a newbie in ICO investing.

The tokens and the coins are also commonly referred to as altcoins and are usually issued by ICO- based projects. Thisvaries from one platform to another and different tokens are stored in their corresponding wallets. For example, Bitcoin has several variants with different wallets like Trezor, Armory,and Electrum where one can store the tokens. Foe Ethereum-based tokens, they are usually ERC20s tokens and MEW and MyEtherWallet are the best wallets to store them. Other token variants have their specific wallets depending on their platforms.

Understanding this issue of wallets for various tokens is very important so that you can store

your tokens in the appropriate wallet, and this is always the first step in turning your altcoins into liquid cash. To protect your investment, it is important that you transfer the altcoinsfrom the company's or project's ICO page to your personal wallets, which are more secure. This is more like putting your stock bonds in a vault. After this, the next thing is always to wait until the altcoin you have invested in is listed in the exchange system. In simple terms, an exchange is a market where you can sell or buy commodities and this system is more like the stock exchange. Here, your altcoins work like the stocks.

Secure The Bonus Tokens

Many ICOs tend to offer bonuses as incentives to investors who contribute early, before the ICO is officially launched publicly. For instance, the minimum requirement of investing in the LiveEdu ICO in the initial stages was $3. But at this stage, one qualified for at least a 25 percent bonus if they invested 50 percent or more and that is why serious investors should invest in the pre-ICO stage because, with the bonuses, you are assured of receiving more tokens in addition to what you have targeted for your investment.

Hold And Sell Some Technique

After receiving the tokens, you can start trading them on exchange for different cryptocurrencies like ETH or BTC or, sometimes, cash. After receiving the coins, a good idea would be to immediately sell about 30 percent of the tokens so that you can recoup your initial investment and then hold the remaining 70 percent for some time before you think of selling them again. Still, the cryptocurrency market is very volatile and a lot of uncertainty and fear surrounds the ICO tokens. However, this should not hinder you from investing.

Keep things simple

Investing in ICOs comes with risk, but never allow these risks to force you into overthinking; In fact, risk-taking is common in every business. Always do your best and make sure you carry out some research before investing in a certain token. In this, you do not need to use some complicated scientific modelsto predict which tokens will yield great returns. You just need to understand a few things about the product offering before investing in it. And to make huge profits, keep your eye on promising tokens and make sure you are involved early enough.

Chapter Three: How to Pick a Winning ICO

The cryptocurrency sector is a rapidly growing market with a very high potential but before you jump into this market with astonishing profits, it is very crucial for you to understand how to choose a good ICO to invest in. The success of any ICO coin is influenced by several aspects and in this chapter we will look at how you can choose a winning ICO.

At this point, it is worthwhile to mention stories of failed ICOs like the Mycelium ICO, whose developers disappeared after raising the money. It was afterward reported that they used the funds for their vacation. The increased lack of regulation of this sector may be the reason $7 million was hacked and stolen from the Coin Dash's ICO. This happened just before the sale of the tokens began. The hacker broke into the system and the ICO wallet address was replaced with the hackers' address.

Based on the above incidents, ICOs are a very risky way of fundraising and it is important for you to take precautions by never attempting to invest what you cannot afford to lose in case the project fails, because you will have difficulty in getting your money back. Before investing in a certain ICO, consider the following issues.

Issues to Consider

1. Consider the team behind the ICO project

When researching on the coin to invest in, always check everythingrelated to the development team plus the body that offers advice to the developers. Scrutinize the individual members of the team by considering their knowledge and experience in starting and running ICO-based projects and their overall experience in the cryptocurrency world. You can visit their LinkedIn profiles, Google the names of the individuals involved, and look for any famous names on the advisory board. Generally, check the ICO projects they have been involved in; you can research further and check how successful their earlier projects have been.

2. Carefully evaluate the white paper

Most investors never bother to read the white paper, even if it contains all the necessary information about the upcoming ICO project. As an investor, always make sure that you read the entire white paper and make sure that you identify the negative and positive aspects of the project and include this in your research. After reading the whole white paper, make sure you can explain what the project is bringing to the world and make sure you have a good grasp of what ICO you are investing in.

3. What is the token needed for?

An ICO is essentially meant for the creation of a new token dedicated for a specific project. The most evident question here is what the token is meant for. Why aren’t Ethereum and Bitcoin sufficient enough to serve as the tokens of the project being

undertaken? You must ask yourself such questions because some projects just make up a scummy story to back up their venture. However, remember that an ICO cannot be a perfect ICO if it has no dedicated token. These questions still must be asked about the usage of blockchain technology on that project.

4. Social media and online presence

As an investor, when you Google the name of the company, you should be able to find sufficient information regarding it. Check out the press releases of the company, their blog, and their social media activities. With the information from those sources, you will be able to gauge their trustworthiness and monitor their activities. Also, remember to check the opinions of your fellow investors on the platforms that have been dedicated to the cryptocurrency investors regarding the ICO project in question.

5. Is the ICO a hard cap or unlimited?

In past years, a hard cap and open ICOs did not have as muchimpact as today. An open cap gives investors the opportunity to send an unlimited amount of funds to the ICO project wallet. On this issue, many tend to forget that if many coins are circulating, the token becomes less unique and afterward there may be difficulty in trading the coin because the demand will be low. On the other hand, make sure that you are not the only person investing in a certain project because exchanges always have little interest with the projects that raise little because this makes it difficult for you to trade the tokens after they are released.

6. Check the quality of the codes

If you have basic programming skills, you can apply the knowledge here. The quality of

the ICO project developer can be understood by just carrying out a simple analysis of the codes. As a non-techie in the programming world, you can simply evaluate the quality of the code by checking the consistency of the code.

ICOs are becoming a main stream fundraising method and, based on the many upcoming projects that are using ICOs. However, by following these key guidelines, you can easily pick out all the negative and positive aspects and be able to make a wise decision on which ICO project to invest in.

Chapter Four: How to get started

Know Your Customer Protocol

Verification is a great challenge all over, and the digital world is not an exception. Companies take strict measures to scrutinize and verify the identity of their clients and at the same time, customers are becoming more cautious and sensitive with most companies, especially when it comes to giving out their information, which is sensitive, or when investing with a given company. In the cryptocurrency world, various regulators in various countries across the globe are becoming more interested with ICOs and this has brought a lot of uncertainty to both those who are offering the ICOs and those who are willing to invest in them.

There are many reasons why one should opt to invest in ICOs and this ranges from the speculation that the value of the coin will rise to the belief of high utilityfor a new piece of crypto. Unfortunately, lack of regulation in the crypto space means that anyone willing to invest in a given project always feel they are risking being treated like money launderers. Because, most of the time, legislation may be unclear or absent, know your customer (KYC) is a broadly used concept in the finance world globally.

Currently, the regulation of ICOs is based on KYC and this has turned out to be a necessity to ensure that potential investors can legally and willingly participate in the ICO investment. This is mainly because scamming activities have been spotted and the KYC-related policies and issues that have been implemented within the financial institutions have been incorporated into the ICO sector.

Importance Of KYC Compliance For An ICO

The incorporation of KYC in the ICO world is because of true incidents because many investors and ICOs have suffered and many crypto scams worth millions of dollars have already occurred. Due to lack of proper regulatory measures and policies, fraudsters from both the investment and the ICO side have taken advantage of this loophole and this has resulted in some serious scams and money laundering using the ICO system. Any investor found undertaking money laundering activities will put all the involved entities to the investigation, including the ICO issuer. This narrows all the way to Anti Money Laundering (AML), which is one of the basic requirements of KYC.

How One Can Ensure KYC Compliance

One can essentially ensure KFC compliance in several ways. For example, if you are offering a service or a product that makes it necessary for the client to walk in and register so that they can be allowed to purchase the product, then you can have all the information verified face to face. It's the same case in the digital world, whereby, if you are providing online services or offering products like ICOs, then the best option is to get the information from a third-party identity verification service provider.

The KYC procedures are based on the collection and keen analysis of the identification documents of an individual as well as the data about the funds used for the purchase. The main purpose of this lengthy procedure is always to deter the activities of criminals who want to use legitimate market platforms for fraudulent activities like tax evasion, terrorist funding, and money laundering. The crypto world has already experienced these malpractices and this has raised the need for good KYC compliance, to make sure that all things are streamlined and both parties are safe.

KYC steps

- **Verification of the client's profile**

  Before beginning the KYC process, just ensure that you have a copy of your identification card and any valid document like a passport in electronic form, for the purposes of uploading. These personal details are legally required and both parties must provide this data in the ICO investment contracts.

- **KYC verification**

  Your personal ID is then compared with the data in your profile and any mismatch will be automatically detected by the automatic compliance check. At this stage, make sure that you provide the right information and let your profile and documented information

be the same.

- **Video verification**

  At this stage, you should be ready with your ID for video identification, where you will be asked to display all your documents in the video call. Make sure that your ID document is still the same as what you used in step one. You can schedule a video call, but if the agent is available at that moment, then you can proceed with the video call immediately. The agent will then ask you several questions to verify your identity.

- **Digital signature**

  This is always the last step, and once the agent has fully verified your identification, you will then digitally sign. Mostly, a code is sent to you via mobile text within a few minutes. Feed the code into the system and the process will be completed.

Sometimes this process maybe daunting and tiresome, but the level of complexity will depend on the protocols that have been set in place by your token provider. However, this is a very important step because it ensures that, as a contributor to the ICO project, you are fully protected. With the KYC verification procedure, you are always sure that not only is your project secured, but also that you, as a token buyer, are protected from any possibility of anyone claiming that the resulting funds are not legitimate.

Crypto wallets

A crypto wallet is simply a digital wallet that is used to receive, send, or store digital currencies like Bitcoin or Ethereum, among other currencies. Most of the coins have an official wallet where they are stored or a third-party wallet that has been approved where one can store the digital coins.

Ideally, they are just like normal leather wallets in real life, used for carrying cash or our credit cards. The only difference is that the cryptocurrency wallets are in a virtual form. However, this virtual wallet, unlike the traditional wallet, tells you the balance that you have, your last expenditure, and such things that your leather wallet cannot tell you. Like digital applications, cryptocurrency wallets are smarter in the sense that they combine all the benefits of your physical wallet with more flexible and sophisticated features. With just one wallet, one can hold many digital currencies without ever worrying about something like running out of space.

As a cryptocurrency investor, you must familiarize yourself with how the wallets work so that once you acquire your tokens; you can have a smooth ride in trading in the ICO world.

The Working Mechanism Of Cryptocurrency Wallets

Cryptocurrency wallets work in the same way as a safety deposit box that you use to store your treasures like jewelry, certificates, or a will. You cannot afford to lose the key of such a box because it means that you will essentially lose ownership of the expensive possessions therein if the key falls into the wrong hands.

Cryptocurrency wallets work in this manner, only, instead of having physical keys, you will have a digital keycommonly known as a master key. Some people refer to these as private keys. They always come in the form of hexadecimal codes and they may look like this:

2940447a4ed5eef7f46bcc185cb2f21d2a8bffcde5418156a9d1a44aa137558

At first glance, they may seem to be complicated and daunting to understand, but with time, you will master them. When investing in ICO tokens or any other digital assets, make sure that you secure your wallet by taking care of your private key. You will always need the key to get access to your assets and authorize transfers from your wallet. So always keep your key in a safe place where you can easily retrieve it any time you need it.

Where Can You Get A Cryptocurrency Wallet?

You can easily get cryptocurrency wallets by signing up for one of the wallets. The cryptocurrency wallets are available in the following forms.

- **Desktop**

  These are wallets that are downloaded and stored on a laptop or PC and they are only accessed through the computer on which these wallets were downloaded. Desktop wallets are very secure, but this security can be compromised if your computer gets a virus or is hacked. But generally, desktop wallets are some of the safest wallets that you can use.

- **Online wallets**

  This kind of wallet runs in the cloud and one can access it using a computing device from any location. They are easy to access and more convenient, but the key is stored online by a third party and this makes it more prone to hacking.

- **Mobile**

  These wallets run on an application installed on your mobile phoneand they are very convenient because they can be used in any place to carry out ICO token-related transactions.

- **Hardware**

  These ones are different from software wallets because the private key is stored on hardware like a USB device. Although, with the hardware wallet transactions are still made online, there is better security with this kind of a wallet because everything is stored offline. The user just needs to plug in the hardware to an Internet-enabled device from any place and then he or she can make transactions.

Single Currency Or Multicurrency Use?

Bitcoin is the most known digital currency but many altcoins have emerged, each with a unique infrastructure and ecosystem. But the good news to those investing in several ICOs is that there are some wallets that support several coins. You do not need to have a separate wallet for your coins; you simply must set up a multi-currency wallet which will effectively enable you to concurrently use several coins from one wallet.

Are the crypto wallets secured?

Cryptocurrency wallets have been built to be very secure, although the exact level of security will differ from one wallet to another. But in general, like your usernames and passwords, the security of your wallet is ensured by strictly following best security practices. Just to guide you, these are some of the practices to secure your wallet:

1. **Obtain a secure wallet**

   With many cryptocurrency wallets available out there, it is wise to locate a wallet that is secured above what is offered by common wallet providers. Some wallets are now incorporating encryption techniques to add extra privacy to private keys.

2. **Use cold storage technique**

   Users should have at least two wallets, but the number should depend on the amount of crypto funds that a user has. One wallet should be strictly for transactional and trading purposes while the other wallet should be used only for secure storage of the ICO tokens. This type of wallet, that is only used for storage and never involved in any transaction, is usually referred to as a cold storage wallet. Always ensure that in the trading wallet, you have only a few ICOs that are sufficient for your current trading activities.

3. **Wi-Fi wisdom**

Always be cautious about the sites you visit online using a device that has ICO wallets in it. Risky Wi-Fi, and some malicious websites, may put your wallet to risk. Also, remember that you should attend well to this device and never lend it to any person.

4. **Gone phishing**

In the crypto world, there are many phishing scams through emails or Google Ads. Phishing scams are very common, so always ensure that the emails you receive from the wallet companies always have their domains spelled out clearly and never look for their web addresses by clicking on a Google Ad.

5. **Turn off any auto updates**

You should turn off the auto updates for all your applications related to the crypto sphere because most of the application bags have the potential to cause harm to the wallet owner.

6. **Double check all the addresses**

It is always important to make sure that you have double checked all the addresses that you are sending any payments to. This is because there are malicious programs that can copy the procedures and then paste them to a different address belonging to the attacker.

Which are the best wallets?

The number of wallets is increasing every day and users have many options to choose from. However, before you settle your mind on which wallet to use in your ICO investment, just consider these following key things:

- Are you planning to invest in several ICOs or one?
- Do you need to access your digital wallet from any place or will you use it only when at home?

- Will you use your wallet for everyday purchases or are you interested in just buying and holding the coins as your investment?

Having asked yourself those few questions and having assessed your requirements keenly, then you can easily settle on which wallet will serve your interests well and by this, you will be able to choose the most suitable wallet.

Some of the best crypto wallets for ICO tokens:

1. **MyEtherWallet**

   This is one of the most popular wallets in the crypto world. It can be effectively used to buy, sell, and store the ERC20 tokens that have been obtained from ICO token sales. It is one of the most accepted wallets because is a wallet available online in addition to providing an offline wallet at the same time.

2. **Jaxx**

   This is another awesome wallet. It can hold, trade, and control your Bitcoin, Litecoin, Ethereum, Augur, and dozens of blockchain-based assets. It gives you complete control of your key, on top of having simple but great features.

3. **Trezor**

   This is a hardware wallet that offers a very secure way of keeping your coins safe from hackers and malware. Its most conspicuous features are cross-platform support and the OLED display.

4. **KeepKey**

   This is yet another hardware wallet that secures Ethereum, Bitcoin, Litecoin, and other tokens. It also offers a USB connection as one of its unique features.

5. Exodus

This a multi-digital assets wallet and the first desktop wallet to have an inbuilt Shape Shift that allows for easy and fast conversion of various cryptocurrency tokens and altcoins. It also enables one to store the private key in an application that has a user interface which is customizable.

Legal Status Of ICOs In Various Countries

Currently, most ICO projects are defining themselves simply as presale program tokens. But from a legal point of view, they are most like selling early access to online games. Project owners tend to use the terms "mass sale" and "donations" instead of ICO so that they can escape from falling under the stock trading companies' category.

Determining the legal status of an ICO in your country is beneficial because, without a good legal framework, few investors from the real economy sector will be interested in investing their funds in ICO startups. Without a good legal framework, ICO tokens will be unattractive and this may limit the development potential of this sector.

On this issue, others still believe that the industry will be better without regulations because the authorities will not interfere with the ICO projects into which the investors are chipping in their funds. The downside of this issue is that with the absence of a good legal framework between token sellers and the investors, the ICO niche remains open for scammers who are always ready to profit from the investors who dream of making money from the tokens they purchase.

Perceived Challenges With ICOs

Many countries are reluctant about ICOs mainly because there are no good regulatory mechanisms put in place and technically, they represent a regulatory workaround. The issue behind this is that instead of seeking an initial public offering, businesses can be funded without any regulatory requirements, due diligence, time, or any fiduciary permission compared to the traditional IPO requirements. This peer-based system offers funding opportunities to ICO startups that would not be eligible for funding through the traditional approach.

Many countries argue that this approach is very comparable with fraud, and this is the main reason some countries like South Korea and China have banned the selling and creation of ICOs in their countries because there is a big door that scammers can use to defraud innocent investors in the ICO sector. Meanwhile, many countries are pursuing changes to their policies so that they can codify adherence to anti-money laundering issues. On top of this, if an ICO relates to flat currencies or property transfer, this may be essentially dealing with securities and this causes effects on the securities' integrity and taxation issues.

Progressive Countries In Terms Of ICOs

Applicability of ICO products, professional support teams, and extensive marketing campaigns on top of well-organized documentation are still insufficient for an ICO to succeed. Choice of jurisdiction is another vital aspect. The most favorable and progressive jurisdictions towards ICOs and the crypto sector are Singapore, the US, Scotland, Switzerland, and several more nations. Such countries that are supportive of the ICO have well-dictated procedures that give ICO projects a legal entity and tax legislation and this makes them friendly and favorable to the ICO startups.

Vitalik Buterin's Ethereum is an example of how Switzerland is favorable to crypto companies. The Swiss government has a good predisposition towards ICO startups because of their significant contribution to the economy of the country. Favorable conditions for the development of new crypto startups are the main reason why many cryptocurrency-based companies have been established in Switzerland. Even though Switzerland is one of the most ICO-friendly countries, most of the European Union members remain adamant and they are not the best choice for ICO-related ventures. One of the greatest challenges in these countries is the data protection laws whereby the financial companies must delete all information of transactions that have been processed by the clients from the database whenever a client requests it. But in the blockchain, one of the distinctive features is that information cannot be deleted and this is always interpreted as a violation of data protection laws.

Singapore is another good country but the charges may be high. The government is well-disposed to technology and it is very favorable to ICO investments, although Hong Kong is cheaper and a better choice than Singapore. However, they have very strict taxation policies. Being the mother of the technology, the United States is very friendly to ICO investments and has excellent jurisdictions for the ICO, but this is exclusively for its residents. Nonresidents may be subjected to serious expenses and, in my experience, severe scrutiny.

These are just a few examples of the countries that have fully incorporated ICOs into their economic sector. As an investor, carry out some research to know the jurisdictions on cryptocurrency that have been established in your country. Before investing, make sure that your country is ICO friendly and, as an investor, make sure that you comply with the laws that have been established to govern ICOs in your country.

The Future Of ICOs In Various Countries

Currently, the cryptocurrency market is worth billions of dollars and, based on this capitalization, different nations have realized the importance of being involved in the crypto arena. Even the skeptics now have less to question about the prospects and benefits of this technology. Based on the potential gains in this sector, many nations are coming up with regulations that will have an effect on the crypto world.

The current unregulated nature of the crypto marketmakes it more exposed to excessive regulations that may have a chilling effect on the ICO development. This is because many countries are seeking to close all the loopholes, and as the countries seek to become leaders in the ICO world, more regulations are expected. While the upcoming regulations are expected to minimize the expected investment risks, the investors still must take responsibility for their investments or their due diligence when investing in ICO tokens.

Registration With ICO

Tokens or ICOs are gaining exceptional experience from institutions and individual investors as well. ICOs are also referred to as next-generation crowdfunding or new IPOs. However, the blockchain-based ecosystem is still new and lacks some standards, thus, registering and making some token sales may be tricky to some people. Here is a quick guide to help you in registering and participating in the sale:

1. **Registering through the ICO project site itself**

   All the legitimate projects that use an ICO to raise funds have a website where they have a clear explanation of what the project is all about, their objectives, funds needed, how long the funding campaign will be, and all other necessary details. On this website, you can register for the ICO as an investor. You will have to fill in your information and verify all the details.

2. **Get Ether or Bitcoin**

   To purchase ICOs, you need Bitcoins or Ethereum cryptocurrencies. Once you have these coins in your wallet, you can then visit the project's website where you will be presented with all the information needed; you can see the amount that has already been raised by the project and which is required for you to participate; you must then accept the conditions and terms of service in order for you to continue. From this point, you can then buy project tokens. The minimum amount that you are required to invest depends on the ICO you are interested in, but the common amount is always in between $10and $100. This amount is always stated in the project's white paper and it can also be found on the project's website.

3. **Move the coins to the wallet that you control.**

   This has been said countless times, that never keep your cryptocurrency coins in the

wallet that was initially provided by the exchange. This is because, in the exchange wallet, your funds may be jeopardized because you have no complete control of your wallet.

4. **Buy the Initial Coin Offering Tokens.**

After registering for an ICO and having your funds available, all you must do is send the amount of the cryptocurrency you are willing to invest to the address of the ICO campaign that you have opted to invest in. The basic goal of every ICO campaign is always to get money and for this reason, the process is not trivial and the project website provides clear guidelines to the investor.

5. **Accuracy**

When sending your funds, be careful and always ensure that you double check the website address because theremight be fraudulent ICO websites on top of your Google search outcomes. They resemble the actual website but several symbols in the address are different.

6. **Get ICO tokens to your address**

You will then receive the new tokens that you have purchased into your wallet's address and if it does not happen instantly, be patient for a while. The time it takes for you to receive the tokens depends on the campaign, and sometimes it may take even weeks before you receive the tokens. Also, to keep yourself updated, communicate with your fellow ICO investors in various forums and dedicated platforms. Sometimes, you may not be able to trade the tokens immediately after receiving them, but this depends on the rules established by the ICOs. The time to wait, when to begin trading, and any other necessary information is always provided on the website of the project.

What is gas in ICO?

Gas is the cost that is used to facilitate transactions in Ethereum, usually in the form of Szabos. (One Szabo is 1/1,000,000 of an Ether). The price of the gas for every transaction based on what is needed toturn the complete the process based on the EVM (Ethereum Virtual Machine Code) and the idea is always to limit the loops. For example, 0.00001 Ethers or 10 Szabos, also known as 1 gas can, execute a given line of command effectively. If the Ether balance in your account is insufficient to run the transaction or send the message, then the action is considered to be invalid; to avoid this, always ensure that you have a handsome Ether balance in your account when carrying out a transaction.

The amount of gas used depends on how heavy the command being executed is. For example, if you want to send 1 Ether to another person, the total cost of the transaction will be 1.00001 Ether. This is just an example of a simple code. If you run a heavy code, for example, forming a contract based on the future price of Ether with another person, more gas will be consumed because several complex codes must be executed.

MetaMask Wallet

The broad Ethereum community has recently come up with MetaMask, which is a new tool that is able to bring Ethereum to the user’s browser via a plugin that is currently available for Google Chrome. This tool essentially enables one to run Ethereum dApps in the browser without the need to run a complete Ethereum node.

Benefits of MetaMask

Using MetaMask, the Ethereum system has been made very accessible to average consumers and this has been a very smart move. It is evident that the Ethereum ecosystem has many advancements to offer, but many people find it difficult to adapt to them because even accessing the dApps remains challenging to many because you have to run a complete Ethereum node. The MetaMask tool thus brings great relief to the average ICO investor because this tool has bridged this gap.

MetaMask addresses most of the problems experienced by common people because the plugin allows the user to access the dApps directly from the Google Chrome. This alone is agreat improvement since doing so has been a great challenge to many people because the dApps were not appealing because of the complicated process involved.

MetaMask also provides a secure identity vault to the user, thus allowing them to manage their identities across various websites, and these identities can also be used to sign the blockchain transactions. This tool also has a convenient user interface that presents things well, thus lowering the barrier to entry and usage as far as dApps and Ethereum are concerned. MetaMask is expected to bring the Ethereum ecosystem a notch higher in the coming months and years.

Chapter Five: Things to Avoid

Just like any other cryptocurrency, ICOs come with risk, and to make a sound investment into an ICO, you must perform due diligence. There have been many initial coin offerings that have failed for various reasons such as the token being offered not offering utility or security, and the company being unable to achieve a growth in price. ICOs are mostly underrated but have great importance as they represent huge returns on investments.

In ICOs, tokens are used as a medium of information exchange using a token-based model which implements blockchain technology. A company will experience greater demand through numerous buyers obtaining the altcoin. The more buyers and holders of a certain altcoin, the greater the demand and user base that company will experience. Therefore, crowdsourcing is done through token sales rather than direct interaction between buyers and users.

For instance, when 5,000 new users sign up and purchase tokens in an ICO, the financial “get” from the purchase of tokens is not only used as the first funding of a project but also to expand the value of the tokens in question. One example of this is the Bancor ICO, which took in over $153M in its ICO. These early buyers of the Bancor token are the most likely future users and adopters of the core protocol and services that Bancor provides, as well as the support team that will help sustain it.

Exit Scams

Despite the popularity of ICOs, coupled with successful projects, there have been several exit scams which seem to be rising daily. An exit scam is a fraudulent practice by unethical cryptocurrency promoters who vanish with investors' money during or after an ICO. Exit scams happen in a very simple way: first, promoters launch a cryptocurrency platform based on a promising concept. Then the ICO raises money from various investors for a specified period before disappearing, leaving investors in the lurch, unfortunately, this is a worrisome trend in the world of ICOs and cryptocurrencies and will end up tarnishing the reputation of ICOs for quite some time to come. It is difficult to trace scammers in these exit scams due to the decentralized, anonymous, and regulation-free operations of the virtual currency ecosystem. Some recent ICO exit fraud examples include Bitcoin, PlexCoin, and Confido. All these projects raised a small amount of money before effectively calling it quits and disappearing altogether. In 2018 alone, a total of $8.4m has been stolen to date, but the amount of stolen funds remains small compared to seemingly legitimate projects raising $50m or more.

Due to increased exit scams, ICOs have been discouraged and burned on various platforms. Investors have been warned by the U.S Securities and Exchange Commission (SEC) of the presence of scammers who utilize the ICOs to generate interest by driving up the value of the coins. ICO and cryptocurrency advertisements have been banned on various social media platforms including Facebook, Google, Snapchat, LinkedIn, and Twitter due to increased scams and the incredibility of their operations. Chinese Internet platforms Baidu, Tencent, and Weibo have also prohibited ICO advertisement. The Japanese platform Line and the Russian platform have similar prohibitions.

The SEC has also acknowledged that ICOs "may provide fair and lawful investment opportunities." The UK Financial Conduct Authority has also warned that ICOs are a very high risk and speculative investments, are scams in some cases, and often offer no protection for

investors. The European Securities and Market Authority(ESMA) notes the high risk associated with ICOs and the risk that investors may lose all their currencies.

Identifying Exit Scams

Identifying exit scams in their early stages can save investors a lot of investments. Although it is evidently tough to recognize a dubious ICO, investors can monitor the ICO using the following key points before making an investment decision.

1. **Team Credibility**

   Accountability and ownership have been the biggest challenge in the ICO world, with every developing ICO looking promising at first for investors but later turning out to be an exit scam. Investors should, therefore, verify the credentials of the crypto team before investing their hard-earned cash. Investors should be aware that these fraudulent schemes are set up with huge starting capital. Therefore, they can do a lot to assure prospective investors of their credibility including buying likes, tweets, and followers on various social media platforms to build fake online credibility. They should perform a rudimentary check on ICO sponsors and on the promoters of cryptocurrency projects and the kind of networks they subscribe to.

2. **Extravagant Return Projections (too good to be true)**

   When the deal is too sweet, think twice. An ICO promising an unimaginable return on an investment is definitely an exit scam. For instance, BitConnect promised a steady one percent daily return on an investment which would transform an initial investment of $1,000 into a return of more than $50 million within three years, attracting numerous investors despite the warning of a Ponzi scheme by Ethereum founder. Unfortunately for them, BitConnect abruptly shut down its lending and exchange services in January 2018 after experiencing a meteoric rise and burgeoning client base since its ICO in December 2016. The market cap of BitConnect, which exceeded $2.7 billion in December 2017, suddenly tanked to $17 million by March 2018, leaving investors with huge loses.

Investors should think critically before making an investment decision.

3. Document Standard

Documentation is key in identifying fraudulent ICOs. The white paper is the key document explaining how an ICO project should function based on its design. Potential exit scams are usually characterized by unclear and ambiguous white papers. This should be a red flag to prospective investors.

4. Non-existent Working Model

Does the cryptocurrency project have a bare-bones working model? If it is a concept-only, non-existent product, then it probably will not function. ICO project promoters should prove that their developments function effectively and therefore can be worth investing in. Investors should clearly understand the functionality of a certain project before capitalizing on it.

5. Severely Promoted Offerings

A new ICO can be heavily promoted through expensive full-page ads, celebrities, and paid bloggers to relay false information. These are signs of exit scams and investors should be very careful when investing in such ICOs. Basically, it comes down to a renowned investmentadvice—if you do not understand the business of the company, and do not trust the people behind it, don’t invest in its shares. The same holds true for cryptocurrency projects.

Multi-Level Marketing Systems

Multi-Level Marketing Systems are also fraudulent schemes in the world of ICO and should be completely avoided by investors. Multi-Level Marketing Systems work based on Multi-Level Tokens (MLT) which are inbuilt in the system. MLT is an ERC20 token built on the Ethereum blockchain. The token is a derivative structural product that gives token holders the right to acquire income out of the increased value of Ethereum. Token holders will also earn “coupon revenue” from a bonus program built into the token’s smart algorithm. The bonus is earned through referrals; therefore, you are encouraged to convince friends and family to buy the tokens, in order for you to earn. Many Multi-Level Marketing Systems are fraudulent schemes where the bonus earned is not usually paid out, but rather, the investors disappear with the income received during referrals.

The Multi-Level Marketing System way of operation can be equated to a Ponzi scheme, which is a fraudulent investment promising high rates of return with little risk to investors. The Ponzi scheme generates returns for older investors by acquiring new investors. Just like the Ponzi scheme, Multi-Level Marketing Systems focus all their energy on attracting new clients to make investments through buying tokens. The income earned through the referrals is then utilized as a return on investment on the project’s founders. A constant flow of new referrals is necessary for the scheme to sustain itself, together with the founders. When this flow runs out, the scheme falls apart, leaving token buyers with huge losses and in disarray.

Characteristics of Multi-Level Marketing Systems

It is simple to identify and avoid fraudulent Multi-Level Marketing Systems since they share the same characteristics listed below

- *Guaranteed profits, coupled with few risks involved*
- *High returns, inconsiderate of prevailing market conditions.*
- *Investments that are not recognized by the Securities and Exchange Commission (SEC)*
- *Secretive investment strategies*
- *Clients having difficulties accessing their returns on investments in terms of money*

Regulation

Following increased frauds associated with ICOs, including cyber thefts using Multi-Level Marketing Systems and trading halts due to exit scams and possible market manipulation, different countries have setup various regulations which are continually changing. Cryptocurrencies are based on distributed ledger technologies enabling people to acquire or transfer their cryptocurrencies directly to another person without the need of an intermediary. Therefore, they are exposed to fraud. It is difficult to regulate ICOs and cryptocurrencies using a central authority since they can easily be moved across national and jurisdictional boundaries. However, countries have developed varied approaches to regulate ICOs and cryptocurrencies, depending on the nature of the cryptocurrency.

Controlling cryptocurrencies can be broken down into two forms: utility tokens and asset-backed tokens. Utility tokens hold more value than asset-backed tokens since they are essential for the holder to exchange a token for a good or service in the future, for example, Bitcoin. Asset-backed tokens may have value because there is an underlying asset which the holder of the token can attribute a value to. In most countries, asset-backed tokens are regulated, rather than utility tokens, which are not prone to fraud. ICO regulation is still under development in most countries including Australia, Canada, and France. Countries that have already developed and implemented ICO regulations are the United States, United Arab Emirates, Switzerland, Gibraltar, and New Zealand. In China and South Korea, all ICOs have been banned completely. Owing to the difference in regulations per country, ICO investors must analyze which countries to sell their coins or tokens in based on set regulations, therefore increasing the complexity in trading cryptocurrencies. Prospective purchasers of cryptocurrencies also need to understand regulations in each country before engaging in any transactions.

The Gibraltar British Overseas Territory Financial Service Commission is in the processes of developing a framework to implement a worldwide regulation governing cryptocurrency

transaction to eliminate the complexity of transactions due to different regulations in each country. Investing in cryptocurrencies and Initial Coin Offerings (ICOs) is highly risky and speculative. Investors should be careful not to get scammed by identifying exit scams early enough using the key points we have mentioned above. Additionally, Multi-Level Marketing Systems should totally be avoided as they are fraudulent ways to benefit initial investors. Whether the development and implementation of regulations will help curb scammers in the ICO world, time will tell.

Chapter Five: Wrapping It Up

If you had purchased $100 of BTC on Jan 1, 2011, it would have cost you $0.30 per BTC, amounting to 333.33BTC. Seven years on and BTC has hit an all-time high of $11k, exchanging at $9,315.28at the time of writing. Assuming you had kept your 333.33 BTC, they would be worth an incredible $3 million today. That is not a bad return for a $100 initial investment. Just like BTC, Initial Coin Offerings (ICOs) may have similar profits, butonly if carefully traded. In this chapter, we are going to discuss stages and tips in investing in ICOs.

Step in ICO Trading

1. **Research Extensively on Upcoming ICOs**

   Extensive research is vital in ICO trading since it is the only means by which an investor is guaranteed a return on his or her investment. An investor should look at resources or outlets that feature the latest ICOs. Knowing which ICOs are coming up will enable an investor to plan, especially for ICOs that have a whitelist. A whitelist ICO enables prospective investors to register in advance to participate in the ICOs, which are usually hallmarks of popular ICOs that have a limited number of coins to offer. The best websites to research upcoming ICOs are Top ICO List and ICO watchlist. At the time of writing, Top ICO List had placed TRIPBIT, COTI, and Qurrex as the top lucrative upcoming ICOs to invest in, while ICO watchlist had noted Payera, Xsolus,and Global Reit as the top upcoming ICOs. Therefore, prospective investors should carry out extensive research before deciding on which ICO to invest in.

2. **Act Diligently**

   In the previous chapter, we discussed how ICOs are prone to frauds such as exit scams and Multi-Level Marketing Systems. Due to this reason, investors should perform their own research to ascertain that an ICO is a good and credible project and hence avoid being defrauded of their hard-earned investments. Research done should involve reading reviews and analysis done by others to verify the potential of the ICO. There are so many good ICO review resources that can be accessed at Crush Crypto and Reddit websites.

3. **ICO Participation Process**

The ICO participation process entails three main steps.

   a. **Opening an Exchange Account**

After extensive research and assurance in the credibility of an ICO, the next step is to open an exchange account to participate in the ICO process. The account should be able to accept fiat cryptocurrency to convert the domestic fiat currency into popular cryptocurrenciessuch as Bitcoin (BTC) or Ethereum(ETH).

b. Opening a Wallet Account

A wallet is essential to participate in an ICO. Participating in an ICO requires an investor to send BTC and ETH from their personal, private wallets. If they send it from an exchange, they will not be able to access the ICO tokens since the transfer originates from the wallet of exchange and, technically, they do not own any wallets in an exchange. Note, exchange accounts such as Poloniex, Bittrex, and Kraken are not personal wallets. There are numerous wallets available but the most recommended wallet is MyEtherWallet (MEW).

c. Follow the ICO Instructions to Trade

In most ICO trading platforms, a step-by-step guide to participating in the ICO is usually provided. A means of communication is also provided for the latest updates and to answer questions in real-time. Investors should ensure they follow the instructions to participate correctly.

4. Exchange to Trade ICO Coins

You should exchange coins to make substantial profits. You can hold coins for the medium- to long-term, depending on your price target i.e. (two times, three times,10x the capital. Alternatively, you could just flip the coin and sell it once it reaches an exchange that usually lists an ICO. Also, if you missed out, an ICO can be bought at an exchange.ICO coins can be listed on various platforms such as Ether Delta, Bittrex, Poloniex, and Binance.

Tips on Trading ICO Coins

After you've opened an account, let's now go over some of the essential tips in trading ICO coins for maximum profits.

- **Have a Reason for Entering each Trade**

  You should only start a trade when you know why you are starting and have a clear strategy afterward. Not all traders make gains from trading since the trade is a two-way traffic, i.e. for everyone who benefits, someone else loses on the other side. You should also understand the risk involved in trading and the risk of costly mistakes.

- **Focus on Coins that are on Reputable Sites**

  Coins from reputable sites guarantee you of their credibility. Trading in non-reputable coins is risky as they are associated with fraudulent schemes to extort traders of their hard-earned investments. As discussed above, sites such as Top ICO list and ICO Watchlist are renowned for dealing with credible coins.

- **Target and Stop when Starting a Trade**

  For each trade, you must set a clear target level for making a profit and more importantly, a stop-loss level for cutting losses where the trade will be closed. It is important to consider several factors when choosing a stop-loss level correctly. Most traders end up taking huge loses because they are unsure of the top level.

- **Do not put all Your Eggs in one Basket.**

  To be a profitable trader, you must manage your risk by looking at the peak of the movement. You should look for small profits which will eventually accumulate to large profits. You should spread your risk across your portfolio. For example, you should never invest more than a small percentage of your portfolio in a non-liquid market with

very high risk. Also, invest with various cryptocurrencies such as Bitcoin and Altcoins which have inverse relationships, i.e. when the value of the Bitcoin rises then Altcoins lose their value against Bitcoin and vice versa. In this way, you are guaranteed a profit in the volatile market common with Bitcoins.

- **Secure Bonus Tokens**

  Most ICOs tend to offer some sort of bonus to incentivize investors to contribute early. For the LiveEdu pre-ICO, for instance, there was a minimum required investment of $3. However, investing $50 or more qualified you for a bonus of at least 25 percent. Savvy investors should look to get involved in ICOs from the pre-ICO stage. If you can get a bonus, then you will receive extra tokens for your initial investment.

- **Hold, Sell, Hold Some More**

  This is a very good idea to increase your investments. For instance, on receiving your tokens, it is wise to exchange them for other cryptocurrencies such as ETC or BTC. The cryptocurrency market is highly volatile and dynamic and you can release a higher return on investment.

- **Set Goals and Place Sell Orders**

  Always set your goals by placing sell orders. A successful strategy regarding this is placing very low buy orders. For instance, the Augor coin was down to 25 percent of its value. After a short while, the market recovered slightly and anyone who had low buy these low orders could easily double or triple their investment. Placing buy orders requires special care .Do not wake up when you are far away from the market to find your buy order is suddenly higher than the current market price!

- **Buy the Rumor, Sell the News**

  ICO trading requires you to always be informed on the current trends. When major news

sites publish articles, it is usually at exactly the right time to actually get out of the trade and you will realize an immense return on investment.

- **Enjoy the Investment Process**

  Enjoy the dynamism of the whole investment process and this will enable you to put your ego aside, which is necessary for making profits. The goal here is not to be right on your trades, but to make a profit. Do not waste resources (time and money) to try to prove that you should have entered that trade. Remember, there is no trader who never loses at least sometimes. The equation is simple—get the total profits to be higher than the total losses.

- **Keep It Simple**

  While investing in ICOs, it is important to minimize over thinking and the worry of losing your hard-earned investments. Also, think critically about the most suitable ICO investment for you after extensive research.

Conclusion

I hope this book will clearly guide you as you make your next investment step in the ICO world. Always remember to be extremely careful when investing in ICOs as they can be fraudulent schemes. ICOs provide a means by which startups avoid the costs of regulatory compliance and intermediaries, such as venture capitalists, banks, and stock exchanges. Therefore, they can be a great means to start a company.

Cryptocurrency 101

Introduction

This book is about trading Cryptocurrencies. The premise is that you are new to cryptos. As such, we will take you through a comprehensive introduction to what it is, how it works, and from there you will be able to understand the material on how to trade it.

Cryptocurrencies use a number of terms in the common analog-age lexicon. From the term ‘coin’ to the term ‘blockchains,’ to even the concept of ‘payment’ and ‘ownership,’ and seemingly unrelated terms like ‘mining’. I will tell you here and now, none of these terms are used in the way they used to mean, and you will see why in just a moment.

We will show you what they really mean and put you on the path to understanding how to trade these coins, and what instruments you can use to approach this market with competence and confidence.

We will also show you how to look for opportunities and even use algorithms to trade rapidly, instead of manually clicking the buy or sell button, or manually drawing lines and charts to anticipate movements. We will show you how it works, but we will also explore the software that can do it at lightning speed.

Why would you want to trade Cryptocurrencies?

It’s not because it is the latest craze, but because it is the latest money-making potential that rivals the early days of Wall Street, and the Forex market. It is a market that naturally lends itself to electronic trades, and thereby makes entry and exit fluid and efficient. Can you lose money on this? Sure you can. Nothing is guaranteed and, in fact, not only is it not guaranteed, the chances of you losing money trading cryptos is very high if you do not know what you are doing.

That is the perspective we are going to take in this book. We are going to come at it from the perspective of losing money and set up all the necessary tools, strategies, and skills needed to prevent that from happening. That way we have the necessary skills to keep the hard deck.

Once you learn how not to lose money on every trade, you can start to look at the strategies needed to navigate the market and the sentiment. The final step is to get one of two things – either the gut instinct to know a trade in real-time, or to have your AI module trained so well that you can almost fly hands-off.

The central aspect of this book is to get you trading as fast as possible, and to do that you have to get familiar with a load of information, then internalize it so that you can be quick on the draw.

With that in mind, we are going to cover the basics in Chapter One. Once you have an idea of those basics, then we will look at the basics of trading in terms of the where and the how. This is so you will get an idea of how to open an account and what you need to look out for in all the infrastructure to begin trading.

In the third chapter, we will look at the tools you will need. This chapter takes it slow. Here we will look at the basic tools and show you how to hand-fly easy trades.

In the fourth chapter, we will look at conducting day trades and the different statistical indicators that will give you rudimentary buy and sell signals. I will share with you the ones that have brought me success, if used correctly. They need tweaking, and that is part of your growth as a day trader.

In the fifth chapter we will look at automated trading software and how to deploy it. What I am most interested to share with you in the latter part of the chapter is the use of AI in developing auto traders for cryptos. Cryptocurrencies are perfectly suited for this, and you should use the latter part of chapter five as a launch pad for looking at AI as a path toward trading all the various cryptos.

While we are at it, let me just add one basic point about getting a wallet. There are three ways you can do this. You can either get straight to an exchange, pick one and open an account. They will give you the option of keeping all your coins with them online. The second way is by downloading a wallet and keeping your coins in that wallet and moving them to the exchange as

and when you need them. Finally, get a small device and load the wallet software on to that, and then transfer what you need to the desktop or laptop that you are trading on as and when you need it.

Let’s be clear about wallets. The wallet only does one thing of primary importance (it does other things under the hood too, but they are not important for the trading aspect of cryptos). It keeps the private keys that you have for the address safe and private. In this regard, there are a few things you must understand. It is not only important where you keep your Private Key. It is also important that you don’t allow accidental duplication of it. So, for instance, if you are using a wireless system at home, do make sure that you do not transact over that Wi-Fi network because anyone who understands that you are doing this can do what is called a Man in The Middle (MITM) attack, and copy all traffic that is passing through your router. Just keep that in mind.

The next thing is to make sure that you have multiple addresses. A wallet is an app that can hold multiple addresses, and those addresses each have a private key, which you’ll need to be able to spend your coin. Create an address for groups of coins and once you have all your coins put into multiple addresses, take what you are not using offline.

When you open your account, it is possible to place all your coins at the exchange. The exchange will keep your coins in a safe wallet, and when you want to withdraw it, you must let them know. In some cases, the withdrawal is instant. In other cases, you may have to wait for a short period. You have to know that keeping your coins in a third-party-controlled wallet is never a good idea, in my opinion. If you can create the necessary measures in your setup, then you will not need to worry about being hacked.

So now that you have an overview of the book, let’s dig in and get started.

CHAPTER 1: Fundamentals of Cryptocurrencies

Before we get to trading, let's start with the basics and understand what cryptocurrency is first. Cryptocurrency, or crypto for short, is an electronic form of currency that allows the transmission of value between two nodes on a network. There are two specific networks that you should get familiar with, because they are currently the most widely known and the ones with the most activity. Fair warning: that could change over time. But as long as you understand the basics, it doesn't matter what the branding is. The first network is the Bitcoin network and the second is the Ethereum network.

What do coins and currencies have to do with networks? Think of Bitcoin and Ethereum as two individual networks. Although they comprise of thousands of nodes and hundreds and thousands of users, the ecosystem is a closed loop. The coins never actually leave the network and that network is defined by the existence of nodes.

Nodes

Nodes are computers that are part of the network. To become a node, users download and install the relevant software. The software itself is free, and once installed it opens up a port on the host computer and automatically connects it to a number of other nodes within the network. Each node connects directly to any node in the network, usually only around six at a time. At the last count, there were almost 12,000 of these nodes and each node connects to six others. It may not seem like much, but if you wanted to send a message to the entire network, all you have to do is send it to the six you are connected to and they will relay it to the six each of them is connected to and those nodes will relay that message on, and within 5 to 6 hops, your message will have spread to all 12000 nodes.

Why are messages important? Because the message is the root of the transaction. We will look at the transaction next.

Transaction

The transaction needs to have two elements to it to make it legitimate. First it needs witnesses, and second it needs a reason. A reason is typically, within the Bitcoin network, the movement of tokens from the sender to the receiver. The sender initiates a message on the network messaging system and sends it to the receiver's address.

Imagine if I send you a letter saying that I will give you a dollar and everyone in this town is a witness to that. There is no way of reversing that transaction. The promise is irrevocable. The transaction in Ether or Bitcoin is as simple as that. To initiate a transaction, the sender must have the funds and he must send the message. When he has the funds and sends a message, so that all the nodes bear witness to it, that transaction is legitimized.

Transaction Value

The value of the transaction can be any amount. If it’s Bitcoin, it can be as small as 100 millionth of one Bitcoin (0.00000001). That is the smallest value that the messaging system recognizes. It is also called 1 Satoshi (in honor of the person who developed the Bitcoin system). The largest amount is whatever amount you have in that wallet, and you can have as many wallets as you like.

Wallets

Wallets are not the kind that you place in your pocket. On the surface, the wallet is the mailbox that holds the coins that you receive in a message. When you send a message out as part of a transaction, it will come from this mailbox – specifically called an address. If that address (we called it mailbox here for recognition of concept) has previously received coins, then it has the ability to spend those coins. If it has no coins, that address will not be able to send out a transaction message.

A wallet is really an app installed on your device (computer or mobile device) that looks across all the transactions and finds out which transactions in the entire ledger relate to that address. All transactions are categorized as either incoming or outgoing. It adds up all the incoming transactions, and then it separately adds up all the outgoing transactions, and the difference results in your account balance – or the maximum amount that you can transact out.

The only other thing that you need to know is the difference between hot and cold wallets. Hot wallets are ones that are constantly connected to the Internet and accessible at any time. Cold Wallets on the other hand are ones that are not online and can’t be accessed via the internet.

The Coin

It’s hard to wrap one’s mind around the concept of the coin, or the crypto coin as it is also known. The reason is psychological. We see it as a coin because coins represent tangible currency in our mind. It gives us a frame of reference as a vessel of value. When we mention a coin, it wraps our mind around a new concept using old and familiar vernacular. But the coin in the crypto economy is nothing like the coin we think of that is typically round and flat with engravings on both sides. In fact, all the images you see online that represent Bitcoin as a golden circular coin are merely imaginary. It does not look anything like that.

Some even think of the coin as a string of bits – ones and zeros of binary computer language. But it’s not. There is no physical coin, and there is not an electric coin either. In fact the coin is not even cryptographic. I know that this goes against all you have heard, but hang in there, you will see what it is in a minute. What it really is, is a cryptographic intra-network messaging system that cannot be forged or hacked. The key to why it can’t be forged or hacked is because it is based on a transparent and decentralized system that is encrypted – more on the encryption and security in the next section.

The coin merely represents an irrevocable act of paying a certain value that is mentioned in the message. And because this is a trustless system, that promise is instantly verified by the system, which knows if the address from where the message is being sent has enough value to be transmitted. It is that value that is described as a coin.

In essence, crypto coin trading is as efficient and pure as it gets, because you are trading our purchasing value. But because it is hard for most people, who are not deeply familiar with the inner workings of the system, the term ‘coin’ gives them a sense of comfort by referring them to the objectification of the value that is being transmitted.

For the promise to have value, it must have been derived from value. You cannot just take

something and arbitrarily bestow value upon it. Before it can have market value or face value, it must first have some form of intrinsic value. Without that the value is untradeable. You must understand this at the core of your foray into crypto-economics and cryptocurrency trading.

The intrinsic value the ‘coin’ gets is derived from the physical labor that is performed to bring that ‘coin’ into existence. Resources need to be spent, and effort needs to be applied in creating each ‘coin,’ and that is why it is referred to as mining. Just as precious metals need to be physically mined, cryptographic value needs to be created by the expense of computational resources and cryptographic processes, and this is done by mining. The next section will describe the mining process.

Essentially, then, coins are brought to life as a reward for the mining process, which requires the expense of resource and cannot be derived for free. It is the nature of the Bitcoin system. In Ethereum, the expense of bringing a coin into existence is done by the expense of resources as well, but they will be converting from the Proof of Work model to the Proof of Stake model in the coming months, barring any unforeseen changes. Either way, a value of some sort needs to be applied.

Once the coin is received by the person who expends this effort, he has the ability to spend it any way he wants. He can even give it away for free or he can use it as consideration for any product or service, as long as the recipient is willing to accept it. But let’s look at that carefully for a minute.

The person who receives it from the system is called the miner, and we will explain that next, but for now, just know that in return for his mining, the system gives him and only him a certain number of coins (remember that coins in this context is just a value with no physical features). When he spends that coin, he can only do it within the network. Of course, he can purchase whatever he wants, as long as the person he is buying from is within the network and has a valid address to receive that payment.

So now that value expended during the mining can be exchanged for anything and it is done so by a message that forms the transaction.

When you trade, that is what you are trading. That is what is called a coin.

Mining

Mining is discussed in this book for two reasons. The first is that it gives you an opportunity to invest in Cryptocurrencies in the form of mining. Even though you are interested in trading, mining is a form of investment in cryptos that are worth thinking about because the cost of mining has only a few factor inputs: electricity to run the computers, purchase of the computers, and the software and whatever labor costs the miner needs to perform the tasks. The hardware costs are typically one-off (there are also replacement costs, because the processors can burn out and might need replacing). Once you acquire the coins in this way, you can then use them to trade. That's one way of doing it. But not everyone wants to get knee-deep in the process. For those folks, we advise just getting to the exchange and starting your trading from there.

We mentioned earlier that mining is the process that brings the coins to life. But now we are going to look closely at what that is. In the next section, we will talk about the blockchain and what it is, but for now, just know that it exists.

While mining efforts result in rewards in the form of coins, the actual mining is the process of computation. In other words, mining is just really a ring of millions of computations to solve a puzzle. The first one to solve that puzzle will be awarded the coin. Thus, the question here is: what is the puzzle?

Without going in too deep, the puzzle relates to hashing. Hashing is a branch of mathematical cryptography that uses a one-way function that is deterministic. That means if I took a word and hashed it, I would get an unpredictable sequence of characters that cannot be reverse engineered. I could take this entire book and hash it and what I will get is a string of characters that look like this (this is the hash of the following sentence: The rise and fall of the Roman Empire):

5C94D7845A6A2163D39CA32A0D19122C6B95FA591CF58636DBEBB475EDA4A160

That hash is so unbreakable that even if I were to change one letter, or even the capitalization of that letter, see how the entire hash changes. I will hash the same sentence but with a minor change: the rise and fall of the Roman Empire. In this case, if you notice, the first alphabet has been changed to a lowercase.

AFC44E6D243443A56A2D65357FA98EA61A6A5997BD2975C4435B9A4BCCCFB763

If you observe the two hashes, they look very different. There is no way you could reverse engineer it, even if you knew how it was hashed.

Now remember, these are just the basic parts of hashing. If you want to know more, there are numerous books that you can get to understand the hashing and cryptographic process in deeper detail.

Back to mining.

Every time a transaction is completed (a message to send coin from one account to another is broadcast through the network) two things happen. The first, is the nodes that receive the broadcast check to see if it is a valid transaction – specifically they see if the sender has a sufficient balance. The second thing they do is confirm if the message is properly formatted and all the details are present. There are about 16 checks that the nodes execute, and if all is okay, they place the transaction in a queue. At this point the transfer of value is not yet confirmed.

There are hundreds of these messages on an hourly basis in the queue.

The next thing that happens is the miners pull all these transactions (they take the transaction IDs) and put them together and hash them. There is a specific way to hash them and it has to include a few things. It needs to include the TXIDs, the header, the hash of the last block, and one more item called a nonce.

This nonce is a random number, but this is where the puzzle that needs to be solved comes into

play. If you take all the information that goes into the block and run the hash function, it will result in a specific string of characters – just as the sentence “The rise and fall of the Roman Empire” above did.

Now look at the sentence again, and the corresponding hash for it:

the rise and fall of the Roman Empire

AFC44E6D243443A56A2D65357FA98EA61A6A5997BD2975C4435B9A4BCCCFB763

The rule is that you can’t change any part of the sentence, but you can add random characters after it. With that in mind, what if I told you that the puzzle was to find the hash that started with the character 0 (zero)? Since you can’t reverse engineer the hash, you have to randomly keep trying with different strings of characters that you can append to the sentence to make the hash start with 0. It would look something like this:

the rise and fall of the Roman Empire 5134525

52CBF3DF5DFA63DA68F55AA5BC321F36597E53D96001B5D1E14668DE79F444E7

This wouldn’t work because the resulting hash didn’t begin with 0 as the system required.

The next try:

the rise and fall of the Roman Empire 4749q0r58tj

423C9570BC80747EC346626C8049208DBA52753BA303516817D9CFC6390D1D10

This didn’t work either. But just to make the point, after a few hundred tries the random number

that worked was this:

the rise and fall of the Roman Empire 090989897934

Which resulted in the hash as below:

0C3EE05D5788E2FD0DFE4D49AE6109A1AFE36523F0D99ED6DC48A4ECF8681622

That hash satisfied the requirement, and as such, the puzzle is solved.

Once the puzzle is solved, the coins are awarded to the miner that solved the puzzle and all the transactions that were included are now said to be part of a block with a specific hash. That hash becomes part of the record and can never be altered. If the block can't be altered (because if you alter the block, the hash would change, and the system would know that there was a problem and reject that block) then the transactions within it can't be altered, either.

Once that block is confirmed, all the transactions in that block are confirmed and the person who received a payment will now see that his payment is confirmed. So, on one side, the mining keeps the integrity of the coins, and on the other side, it generates more coins into the system.

You can't change any of the transaction IDs without changing the hash. This keeps the whole thing secure.

Blockchain

In the last section we talked, in passing, of a Blockchain. Now, it is time to look at that in a little more detail. If you notice that the messages that the sender initiates are not just sent to the address he is sending the coin to, he sends it to all nodes in the network – via the six (or more) nodes he is directly connected to. In just a few seconds that message reverberates across the entire network and all the nodes take note of that message. Once that message is released, and the rest of the nodes bear witness to it, the nodes now deem that the recipient is now the owner of more coins, and that the sender has less.

Let's put this to use in an example.

Let's say Andy wants to pay Bob 1 BTC (BTC = Bitcoin) for whatever reason, which is immaterial to the network. Bob creates a wallet and gets an address. That address belongs to him and it comes with a Private Key. In the meantime, Andy, who already has his address, Private Key, and some Bitcoin in his wallet, takes Bob's address from him and broadcasts a message to the entire network that he is sending Bob 1 BTC. You've already seen how that is then placed in blocks.

Once it is placed in a block, the entire block is hashed, and that is then placed inside the next block and the miner proceeds to solve the puzzle. Once the puzzle is solved, that hash is then placed in the next block of transactions, and so on it goes.

That results in an unbreakable chain. Once the transaction is confirmed, it cannot be canceled or reversed. It lives forever, because a change in even one digit will change the hash, and that change in hash will not jive with the hash that is already recorded in the preceding block.

This blockchain record is kept on all full nodes. That means there are thousands of records of this blockchain, which means it can't be altered.

The fundamentals of Cryptocurrencies in this chapter looked primarily at Bitcoin and to a brief

extent, Ethereum. But all cryptos have some form of mechanism that is similar. All of them have the same concept but execute it differently, and by that you get different coins and networks.

The volume of coin demanded and the supply at any given point give rise to a value, and that value is made more fluid and the asset is made more liquid by a vibrant market. Trading in Cryptocurrencies is a three-dimensional proposition. You can either trade fiats for cryptos, or you can trade one crypto for another. We will get into those details in the next chapter.

Buckle up!

CHAPTER 2: Basics of Trading

Trading cryptos is simple. You buy one of many existing Cryptocurrencies that are offered by the exchanges. There are a number of exchanges that exist in the US and in other parts of the world. Before you think about where you want to open an account, here is what you need to consider.

The first thing is that you need to open an account. If you prefer, you can open an account in a location that is not going to impose a tax liability on you in any jurisdiction. So this deserves some study. This book is not going to give you tax advice, but you should know that there are jurisdictions that will consider profits from Bitcoin trading to be taxable. If you look at it as a currency, and that it is not legal sovereign tender, then it is tempting to think that it is not taxable. This is wrong. Most tax jurisdictions do not differentiate the underlying asset when accounting for profit.

The other thing that people are quick to assume is that Bitcoin transactions are anonymous. Well, they are to a limited extent. But there are easy ways to see who owns what, unless you go through extreme measures to protect it. When people say that Bitcoin is usually used by the shady elements to hide their activities, they don’t really know what they are talking about.

Exchanges

There are more than a hundred exchanges that you can get on to be able to trade the currencies that we talk about in this book. We will stick to one hundred, and you can look at each one of them to see which ones you would like to pick. You should have at least 10 exchanges in your basket, and you should use the ones that allow you to keep your coins wherever you please and transfer to them only when your trades are open, find an exchange that is quick with withdrawals and an exchange that executes rapidly without the need for brokers. Brokers work against your interests because they cost more and they are unable to execute rapid trades. Here is a list of exchanges that you can evaluate:

1 Abucoins
2 ACX
3 AEX
4 AidosMarket
5 alcurEX
6 Allcoin
7 Altcoin Trader
8 Bancor Network
9 BarterDEX
10 BCEX
11 Bibox
12 BigONE
13 Binance
14 Bisq
15 Bit-Z
16 Bit2C

17 Bitbank
18 BitBay
19 Bitcoin Indonesia
20 BitcoinToYou
21 BitcoinTrade
22 Bitex
23 Bitfinex
24 BitFlip
25 bitFlyer
26 Bithumb
27 Bitinka
28 BitKonan
29 Bitlish
30 BitMarket
31 Bitmaszyna
32 Bitonic
33 Bits Blockchain
34 Bitsane
35 BitShares Asset Exchange
36 Bitso
37 Bitstamp
38 Bitstamp (Ripple Gateway)
39 Bittrex
40 Bittylicious
41 BL3P
42 Bleutrade
43 Braziliex

44 BTC Markets
45 BTC Trade UA
46 BTC-Alpha
47 BTCC
48 BtcTrade
49 BTCTurk
50 Burst Asset Exchange
51 BX Thailand
52 C-CEX
53 C-Patex
54 C2CX
55 CEX
56 ChaoEX
57 Cobinhood
58 Coinbe
59 Coinbene
60 CoinCorner
61 CoinEgg
62 CoinEx
63 CoinExchange
64 CoinFalcon
65 Coinfloor
66 Coingi
67 Coinhouse
68 Coinlink
69 CoinMate
70 Coinnest

71 Coinone
72 Coinrail
73 Coinrate
74 Coinroom
75 CoinsBank
76 Coinsecure
77 Coinsquare
78 Coinut
79 COSS
80 Counterparty DEX
81 CryptoBridge
82 CryptoDerivatives
83 CryptoMarket
84 Cryptomate
85 Cryptopia
86 Cryptox
87 DC-Ex
88 DDEX
89 Dgtmarket
90 DSX
91 ETHEXIndia
92 ExcambrioRex
93 Exchange
94 Exmo
95 Exrates
96 EXX
97 ezBtc

98 Fargobase

99 Fatbtc

100 Foxbit

101 FreiExchange

102 Gate

103 Gatecoin

104 Gatehub

105 GDAX

106 Gemini

107 GetBTC

108 GuldenTrader

109 Heat Wallet

110 HitBTC

111 Huobi

112 IDAX

113 IDEX

114 Independent Reserve

115 InfinityCoin Exchange

116 Iquant

117 ISX

118 itBit

119 Koineks

120 Koinex

121 Koinim

122 Korbit

123 Kraken

124 Kucoin

125 Kuna

126 LakeBTC

127 Lbank

128 LEOxChange

129 Liqui

130 LiteBit

131 Livecoin

132 LocalTrade

133 Luno

134 Lykke Exchange

135 Mercado Bitcoin

136 Mercatox

137 Mr

138 Negocie Coins

139 Neraex

140 NIX-E

141 Nocks

142 OasisDEX

143 OEX

144 OKCoin

145 OkCoin Intl

146 OKEx

147 Omni DEX

148 OpenLedger DEX

149 Ore

150 Paribu

151 Paymium

152 Poloniex
153 QBTC
154 Qryptos
155 QuadrigaCX
156 Quoine
157 Radar Relay
158 Rfinex
159 RightBTC
160 Rippex
161 Ripple China
162 RippleFox
163 Simex
164 SouthXchange
165 Stellar Decentralized Exchange
166 Stronghold
167 SurBTC
168 TCC Exchange
169 TDAX
170 The Rock Trading
171 Tidebit
172 Tidex
173 Token Store
174 TOPBTC
175 Trade By Trade
176 Trade Satoshi
177 TradeOgre
178 Tripe Dice Exchange

179 Tux Exchange

180 Upbit

181 Vebitcoin

182 VirtacoinWorld

183 Waves Decentralized Exchange

184 WEX

185 xBTCe

186 YoBit

187 Zaif

188 ZB

189 Zebpay

** Please note that these sites have not been vetted, and as such you need to do your own due diligence before using their services.

Market

If you want to trade cryptos actively, it is not a difficult process once you get your fundamental study and technical study internalized. There are few, if any, regulations on it that you need to abide by, and as long as you do not engage in fraud or theft, and you conduct yourself equitably, you won't need to keep looking over your shoulder.

Remember that cryptos are not physical assets like shares of companies, or fiat currencies that have the legal sovereign banking system – and then further substantiated by other countries, and by the world's banking institutions. Currencies have that, cryptos don't. So that is the first risk that you need to keep way back in your mind. What's the worst that can happen to cryptos? They could be outlawed around the world. The chance of that happening is low, but nonetheless it exists. In our case, that is a good thing because it adds to the push and pull of the market, creating opportunities to buy and sell. It is also one of the reasons you should not keep an open position overnight.

More importantly, unlike shares and currency, they are not physical assets that can be held and kept – cryptos are not physical in any form. These are conceptual assets, and as we advance as a society we will see that cryptos will end up being the most efficient currency in use. Imagine a time when we eventually reach space and have colonies – cryptos would be an ideal way to facilitate commerce.

Up until this point, what we have been looking at has been the ecosystem of the crypto economy – specifically the cryptocurrency. That gives us the basic knowledge to start understanding the factors that come into play for the market that we are interested in. Our next goal is to look at the market. I will compare the crypto market to traditional financial markets, if necessary.

The first thing you need to know is that the crypto market is not centrally regulated. That means there are no rules yet on what you can and can't do, but there are limitations as to what is

acceptable in the marketplace. You can trade manually, you can use program trading, and you can even use artificial intelligence.

There are no rules, and that makes it a very lucrative opportunity if you do three things. The first is make sure you understand the basics. Second, start small – the minimum trading size for a few exchanges is 0.001 BTC. You need to get the feel for how things happen, and that gets your confidence and experience up. The third is that you do not stop at plain vanilla trades. If you just want to get into it and trade one or two times a day with plain vanilla trades, then this is not something that you will succeed at in the way that you imagine. Bottom line: start small and crank it up.

I hear many would-be traders complain that the Bitcoin market is volatile. It is, but that is a good thing. There are two kinds of volatility. One where there is high volume (and the volatility is driven by a different factor) and the other where there is insufficient volume.

Tradability

Bitcoin is not the only crypto out there that you can trade. And the USD is not the only fiat that you can trade that against. There are over 1000 cryptos in the market today and over 100 fiats that are worth trading. However, mastering all those pairings creates a nightmare. You should focus on just a few. In my experience, the US Dollar, the Japanese Yen, and the Euro are your best fiats to be traded against cryptos. Among the cryptos, aside from Bitcoin, which is the obvious trading opportunity, there are eight alternatives you can choose from as follows: Ethereum, Litecoin, NEM, Dash, Ripple, Ethereum Classic, Monero, and Zcash.

That gives you more than 50 possible trading pairs - USD v BTC, USD v ETH, USD v NEM, and so on. It may seem like a wide field to choose from, but let me tell you that, as a beginner, it is indeed too many. As a manual trader, it will be completely overwhelming for you to understand, track, and execute the entry and exits of each pair.

To effectively choose the pairing, you need to be intimately familiar with the nature of the individual currency and the nature of their pairing. To do this you need to observe and understand the critical factors of tradability and liquidity.

Tradability is a combination of volatility and breadth. Volatility is the frequency of movement that it makes in a given period of time, and breadth is about the gap between the movement of the price's high and low. You need both to make it tradable. Tradability is a lot different from buying and holding for future profit. That does not require the higher frequency movements. On the other hand, if there is no breadth, then it will be hard to enter and exit the market profitably, since there are spreads that you need to consider. For instance, if you are looking at a pairing between A and B, the exchange rate is 1:1.9. In actuality, the rate is spread between 1.85 and 1.95. Your buy price would be 1.95 in this example and your sell price would be 1.85. This spread would cause you to lose 0.1 if you were to do an instant entry and exit. The point of highlighting this is to show you that, even if the price didn't move, if you entered and exited

within moments, you would still lose the spread.

Because of this, breadth of movement is important, especially if you want to do fast trades, which cryptos are capable of. You want to be able to have it move at least across the spread and cover your fees and other costs, and if that happened, you could scalp the market many times during the day and make a tidy profit. We will look at this again later.

The way volatility helps is that it gives you many opportunities to trade in a day. You need to think about trading as a two-way street, and not as you would if you were buying stocks. In this two-way street, you are exchanging one currency for another. And so, if you think that BTC v ETH is rapidly fluctuating, that means the BTC will rise against ETH and then fall back. When BTC falls back against ETH, it means the ETH is momentarily appreciating. Your opportunity comes from riding those ups and downs.

If an asset is not volatile, it may be a great asset to purchase for the long-term, but it won't be a good candidate to trade rapidly or day trade – which is what you want to do with cryptos. Try not to leave a position overnight when it comes to these assets. It is too high a risk to leave open positions unattended – unless you are doing program trading or using AI.

The crypto market is unlike the stock market. If they are not volatile, they present no opportunity to trade profitability – remember we are talking about trading here. Buying an asset for long-term appreciation is not covered in this discussion.

On the other hand, if they are too volatile, they present reduced security and predictability to trade. So a balance must exist in the level of volatility. These untenable volatile situations arise due to volume. If the volume is low, prices tend to be volatile but they are not tradable. This is because the price fluctuates too rapidly to allow the entry into the market to be predictable, and then once in, it becomes too difficult to exit the market effectively. The average volume is a key factor in accepting the volatility pattern of the asset. This leads us to liquidity – the second of the two factors we mentioned.

What is liquidity?

Liquidity has to do to with volume and efficiency. You can think of it as friction. If you get into an asset, you want it to be as frictionless as possible. That means you get in when you want to and you get out when you want to. There are a few situations that may make that untenable. One scenario that could happen is when everyone wants to sell, you will find that there are no buyers – that's not a liquid market. You may discover that finding a seller or finding a buyer is not easy because there is lackluster interest in the asset; or you may find that there are not enough exchanges supporting the market, which reduces the potential trader's access to that asset. These are just a few ways the asset is illiquid – there are more. But you get the point. When you consider an asset, you need to assess its liquidity and its volatility. Liquidity without volatility does not give you tradability, while volatility without liquidity doesn't give you predictability.

This is partially the reason Bitcoin is more valuable and in demand than its alternatives and the USD-BTC pair is a popular investment tool for day traders. It is also because there is sufficient liquidity to make your trades almost seamless and efficient. This is called a liquidity premium, and it is one that you should be willing to pay, as the payoff is worth it.

But that is a fiat-crypto pair (meaning it is the trade between a fiat currency and a cryptocurrency). What about a crypto-crypto pair? Well, there are several large volume and liquid pairs that you can work with. One such pair is the BTC-ETH pair.

With respect to tradability, you should have your basket well differentiated between fiat-cryptos and crypto-cryptos, and even have a basket that is fiat-crypto-fiat or crypto-fiat-crypto, or some other three-way combination.

You want to be an expert in at least two or three combinations, and that expertise comes in the form of study and practice. You have to study the fundamentals and you have to practice the art of reading the charts. In the trading business these are called the fundamentals and the technical. You have to study the fundamentals – which includes knowledge of the asset, how it works,

market sentiment, regulation, and analysis. On the other hand you have to know how to read the charts. The charts and the analysis of the movement of price is a comprehensive mathematical and statistical representation of the psychology of the market. It is fairly plausible to understand where the market is moving in the future by looking at sufficient data from the past. That’s the technical aspect of the analysis.

Become an expert at BTC vs Ethereum and BTC vs USD to start.

CHAPTER 3: Crypto Trading

There are two ways you can get into active trading. One has a cost advantage, so it is good to get started with this. The second has an accuracy and professional advantage but the costs are significantly higher. It's not always a simple choice between one and the other, but rather a case of growing from one and moving on to the next.

When you start off, it is best that you take the one that gives you the cost-benefit, this is assuming that you start slowly. If your initial foray into the market is between 5 and 10 Bitcoin, then going online would not be too obstructive. With that amount, you would probably conduct between three and five trades per day (24 hours). In this case, the online exchanges are absolutely fine.

The online exchanges and trading houses provide you with the ability to execute trades, as well as use trading tools to find buy and sell points. A few of the reputable intermediaries have this, and most of them are free if you place a certain minimum amount with them.

The other option is for you to stay away from the online trading platform and get the price feed you need from the Bloomberg Terminal. Bloomberg now offers real-time quotes for most of the major cryptos, and even some of the more recent ones. It is surprisingly extensive. When I first started using it, they only had the USD-BTC pair and over the last few years they have added most of the others. They also offer the ability to chart all the cryptos and even give you the flexibility to program your strategy directly from your feed. My current setup pulls the real-time feed from the terminal, which then gets fed into an AI algorithm that we have developed.

If you are considering taking this on with any level of seriousness, then you should not skimp on the equipment that you are going to need. If you do decide to go the Bloomberg Terminal route, then go ahead and get the T1 line put in as well. That way you are getting super-fast real-time feeds on pricing.

If you end up doing trades that are rapid-fire, and if you use an online system, even if you do have broadband, then you will end up having a lag time, which is not acceptable for any level of serious trading.

When I got into trading, I had no choice but to do it online, but jumped to BT as soon as they started to offer it. The speed of the T1 line and the accuracy of the prices allows me to execute rapid turnarounds and trade higher volumes in a day and to have higher frequency of multiple pairs. 90% of my trades are not manual, they are program trades, 5% are AI trades, and 5% are manual trades.

When you do program trades, the programs are scanning for opportunities across the market at a rate that is significantly more efficient than a human possibly could. This brings more trading opportunities to my attention, which increases my volume and my profit potential. I suggest you do the same.

Trading Strategies

There are three trading strategies introduced in this chapter. These strategies will form the foundation of other strategies that you will surely get used to as you mature in your trading abilities. This is assuming that you are new to cryptocurrency trading and have minimal knowledge and understanding of what it is and how to do it.

Remember that this market moves constantly. Hardly a second that goes by when a trade is not being conducted. With more than 50 pairs of currencies and fiats, trading can easily become a full-time occupation.

Buy the Dips

Always remember to buy the dips. Dips are moments in the price movement that a march forward is followed by a momentary step back. This is the characteristic of most markets. When you are new to any market, it is an effective way to identify trends. When you are day trading, trends are not what they would be if you were a long-term trader. A long-term trader considers a trend to last anything from a few days to a few months, and enters his position and leaves it for days, weeks, or even months. A scalper in cryptos or a day trader doesn't do that. He actively trades the waves, both up and down, and exits in minutes, or hours, at the most.

Since you are doing rapid trades, you can use the dips to get a better entry point once a mini-rally has started. This is your first strategy. When you first get started, observe the graphical representation of price movements. Don't look at the numbers, as the numbers can't give you an image of the price as it takes shape. Watch the chart and adjust the timescale to 5 seconds, 10 seconds, and 1 minute to get an idea of the nature of the movement. You will notice that every advance is punctuated by a retracement and every fall is retarded by a momentary uptick. Get used to this patter and use it in your ability to buy the dip.

Never place an order as soon as the market turns from one trend to the next. Wait for the dip,

then buy on its next run. That way you can see the rally form rather than face the retracements soon as you get in. It also gives you an opportunity to confirm the push forward. Use the dips as a trigger for your market entry.

Do the same thing when you are shorting the market - wait for the dip. In this case, the dip means that it is backing off its downward trend and momentarily ascending. Wait for it. When it reaches its apex and starts back down, that's when you catch it. Make it a habit to never try to catch it at its peak. Fortune may grant a perfect catch while the price peaks, but it's never a good long-term habit to have.

The apex and the pit have a specific purpose, and that purpose is not for you to harvest or liquidate, but for you to prepare for the next move. Those are your trigger points.

Arbitrage

This is an advanced strategy only as far as beginners go, but it is something that you should master right away. Arbitrage doesn't focus on the ups and downs of the market, but rather the mispricing of the market. In cryptos, this is an underutilized strategy, and if nothing else, this is the strategy you should take away from this book.

When there are so many pairings, your best bet is to use the automated programs that I use (as described in the earlier part of this chapter). Without automation, you are not going to be able to make use of the greatest benefit that cryptos provide – and that is tradability and volatility.

Back to arbitrage.

In arbitrage, the thing that you are looking for is a mismatch in price between pairs. So, let's say for instance you have the price of A vs B, price of B vs C, and the price of C vs A. If all goes well, and the A:B is 1:2, B:C is 1:3, then it should be that A:C should be priced at 1:6. But in a pricing mismatch, A (in this example) is bidding at 1:6.5. What happens in this case? Look at how simple this is. If I use one unit of A to buy C, I get 6.5 in return. With 6.5, I can use C to

buy B at the rate of 1:3, which will get me 2.167 of B. With 2.167 of B I exchange that back into A to get 1.08 of A. When I first started the arbitrage exercise, I walked in with only 1 unit of A and I exited with 1.08 units of A. This example shows an 8% return. That's not so important, because the numbers are only examples. The point is that this trade would take just 30 seconds to complete.

Now let's look at how you set this up on your trading. Before I forget, there is something that you should do on a daily basis. On any given day, there are numerous mispricing opportunities, and you will not be able to catch all of them manually. You will need a program or an AI algorithm to catch them and execute the trades. Just keep the program running and set it up to either trade automatically, or to seek your approval prior to placing the trade.

If you don't do this, there are a number of other traders who are going to do it. The fastest to execute this gets the prize. The guys who trade on web-based portals are certainly not going to be in the running. Because, to take advantage of this, you need extremely low-latency systems and real-time data feeds. Your Bloomberg Terminal can do it, only if you are on a T1 line.

On Balance Volume

The two strategies you've seen so far are really enough to get you started, but here is a third one that goes beyond just buying and selling when and if you 'feel' like it. The logic behind the first one, on the surface, is designed to get you to identify market entry and market exit triggers. On a deeper level it is designed to get you familiarized with the nature of price movements and the use of charts to visualize them. The second strategy was arbitrage, and that was designed to get you to profit off the mispricing of the market. That's on the surface. From a deeper perspective, it is designed to get you to open your mind to the different ways of taking advantage of the markets.

This last of the three strategies is designed to get you to see what the smart money is doing. By using this strategy, you are keeping an eye on where all the money is flocking to. If you can get comfortable with the movement of big money, then you can pretty much ride the trends and

scalp the fluctuations.

To do this you need an OBV indicator. Bloomberg has it preinstalled on the Terminal. Some prominent MT4 for cryptos have it as well. OBV stands for On Balance Volume.

The OBV indicator gives you insight into how much money is flowing into any given position. What happens when you see money pouring into a currency? You know that it is about to take off. One of the things that you don't normally see in the online or web-based trading platforms is the volume of orders that are going in the pipeline. When you watch that with the OBV, what you get is pretty good insight into where the market is going to tip at any given moment.

Conversely, what you can do, among other things, is watch where the market starts to lose steam, and either get out of a position, switch counters, or short the asset. The possibilities of how to read the market and what to do get pretty sophisticated once you start to get comfortable with the OBV. But the two things that you absolutely must keep your eye on is the pending trades and the OBV.

There is also something called the OBV mismatch, and it is a trade of the second order in the sense that you are no longer just looking at the price of things to determine a trade; you are looking at the effect of the activity around it that is measured by the OBV.

If you find that there is a mismatch between two cryptos, then you go to the price that they are trading at and determine if the price of the cryptos are converging or diverging. If you find them converging, then prepare yourself for a sell order. If they are diverging, do the opposite.

Chapter 4: Trading Indicators

Within the next decade, or less, trading in cryptos is going to be dominated by algorithms and artificial intelligence. There is not much to dispute on that. We have already started to see that equities and bonds have started using Quants (Quantitative Analysts). Quants in traditional markets are similar to the technical traders we talked about earlier in the book when it comes to trading cryptos. They essentially trade on statistical and mathematical strategies.

Don't worry, you don't need to be a mathematician to do any of this. What you do need to do is get started now, so that when the time comes, and you want to remain competitive, you will be able to understand what the technical analysis is and how the program you get into will be able to assist you when trading cryptos. Remember that cryptos, more than anything else, naturally lend themselves to program trading.

There are four market zones that you need to be aware of. The first one is the Japanese time zone, which starts at about 8pm EST and ends at 4pm EST. During this time you get fair volume. Then comes the Middle East Market, which opens at about midnight EST and stretches to 8am EST. This overlaps with the European Market and stretches the active tomes to about 10am EST, by which point the US east coast comes online and kicks up the volume, and that stretches all the way to about 8pm EST due to the west coast.

Even though these are 24-hour, 7-day week markets, there are peak times that you need to be aware of. If you are not using an AI to monitor the volumes, then you can just use these times in your program to assume that these are the times – especially the times when there is an overlap that there will be greater volume and better use of statistical and computational strategies. Increased volume plus increased volatility make trading profitable, and that is a function of peak overlap business hours.

Moving Averages

Whether you get a sophisticated system, or you decide to run the numbers by hand, you need to start your technical education with the simplest and most effective tool that you will find. It is called Moving Averages and you will see them denoted in forms like MA-30, MA-5 and so on. MA of course stands for Moving Average. But the number that follows it represents the period that the average is computed for. So MA-30 represents the moving average of prices over the last 30 periods.

Note that I wrote 'periods' and not days. The reason is that the time-scale is up to you. If you are looking at short-term trades, then the time-scale can be as small as 30 seconds or a minute or even 5 minutes. If your investment horizon is in the long-term, then you would use days. You can even use them in conjunction to understand the longer trend and the short-term fluctuations.

For instance, you can use a 30-day moving average to get a feel for the long-term trend, and that would give you y0ur bias. So, for instance if the trend indicated an up-swing, then you would have a bias that the prices are going up, and that you should favor long (long is the term used to indicate buy positions) positions. If the long-term trend is moving downward, then you should have a bias for short positions (short is the term for selling).

Typically, you would use two long-term trends, let's say an MA-35 and an MA-21 (I find that using Fibonacci numbers gives better results). This timescale is measured in days. That will give you the long-term bias. Then you can have the short-term indicators, like the MA3 and MA8. These are measured in minutes. So, I take the price at the end of a minute, three times consecutively, then add them up and divide it by 3. So, let's say at 9:01am the price is 10. At 9.02am the price is at 10.5, and at 9.03am the price is at 10.8. You would take 9, 10.5, and 10.8 and add them up to get 30.3. Divide that by 3 (since it is three periods) and you will get 10.1. As such, the MA3 is 30.1. You will then plot that line and superimpose that plot on the price chart. What you will find is a smoothed out price movement chart. If you then superimpose the MA8,

which is the 8-period average, then you have two similar lines that tend to flow together.

The signal comes when one line crosses the other. When the MA3 is below the MA8, it indicates a falling trend, and when the MA3 is above the MA8 it indicates a rising trend. This is your short-term indicator.

The same happens with your long-term indicator. If the long-term indicator (the one measured in days) shows a longer-term trend, this can form your extended bias. So, if the long-term trend is set to rise, that is your long-bias. Thus, if you have a long-bias that is necessitated by the longer MA, and the short-term trend indicated by the shorter MA, then what you have is a good position to scalp the market in both directions whichever way it goes.

Here is how you do that.

If the long-term MA is a long bias, then you keep your eye on the fact that the market is poised to turn up quickly, and so you start with a footing of a buy position. As soon as the short-term indicator also shows a buy signal, then you jump into the market. The moment the short-term indicator changes to the sell, then you liquidate that position, and enter a new short position. But this second short position needs to be more sensitive. At the first indication of the short-term changing back to the buy, you liquidate that position, reap the profit, and also enter a new buy position. You keep doing this at every opportunity, especially when there is large volume in the market during peak time. This indicator is most effective and accurate when the market is liquid.

This is a good indicator, and in unsophisticated markets is strong enough to be the only indicator that you will need to profit from a market. If you start doing program trades, which you should, then just use the test feature in the app to test the strategy on past price movements and observe the trade signals. I have done this many times while programming the AI version of the trade algorithm and the rapid-fire efficacy – which is to take every trade every time without hesitation. Strict programmatic trading resulted in 81% accuracy of trades and a 27% return in a day. (this was in test mode, not live market). That was the program trade version. In the AI version, we

programmed the engine (AI engine) to run millions of simulations until it found the best interval and the most accurate signal. The results were better than expected, and it is one of the reasons I mentioned earlier that crypto trading will be fully programmatic or AI-driven within the next decade. So you might as well get on board now.

Exponential Moving Average

The EMA has a little more efficiency to it in certain markets, especially the BTC-USD rates. It is exactly the same as the MA that we saw above, with the only difference being that there are weights applied to different periods. The rationale behind this is that the number that are close to the present moment in time should count more toward the average than a number that is much further in the past. This calculation has its advantages and works well in BTC-ETH exchange, and a couple of other crypto-crypto rates. It also works better in markets that are less volatile. Less volatile markets tend to result in indicators that are too sensitive, which then results in a higher incidence of false positives.

Here is how you do it:

Use a Fibonacci number again to choose the time horizon. Let's say you take 13 periods. Apply a weight of 1.3 to the most recent number, 1.1 to the number before that, 1 to the number before that, and go all the way back to 0.1 for the first number in the sequence. So, let's say the following sequence is the price of the asset over the last 13 periods:

10,9,10,11,12,11,12,13,12,11,13,14,13

Multiply each number by its weight, like this:

10(0.1),9(0.2),10(0.3),11(0.4),12(0.5),11(0.6),12(0.7),13(0.8),12(0.9),11(1.0),13(1.1),14(1.2),13(

Then add up all those numbers

1+1.8+3+4.4+6+6.6+8.4+10.4+10.8+11+14.3+16.9 = 94.6

Then divide 94.6 by the sum of the weights, which is 9.1

So 94.6/9.1 = 10.39

You can play around with the weights of the prices to fine tune it to your favorite counter, but

you now get the picture. In case you were wondering, yes, you use two horizons—EMA 13 and EMA21—and when they cross over, it indicates a trigger to purchase or sell.

When the faster of the two is above, then it is a buy, and when the slower is above it's a sell indication. You can use this in conjunction with the regular moving average for certain counters. In my experience, it seems to work well with the less volatile pairings like Ethereum vs Ripple, or Ripple vs Monero.

ADX Indicators

The final indicator that I want to introduce you to is the ADX. But before we get into that, I want to impress upon you that the way to make money in crypto trading is not so much about identifying the trends of a price movement. It is really about identifying turning points. You make the most return in accurately picking the point where a turn is made in earnest – that means you are able to look over the false positives. In trades you want to get in at the start of a run and keep scalping the mini moves. That's why a 24-hour market works so well, because the market lends itself to constant data analysis. There are no sudden starts and stops – discontinuities that leave risk to accumulate from the close of one session to the open of the next. I have said this in an earlier part of the book. It is statistically more prudent to liquidate and square your positions at the end of your trading day than to leave open positions unattended – especially when you do not have a program or AI engine running your trades.

The ADX is a line chart that is plotted on the price chart. Typical price charts represent the movement of the price in graphical presentation. Charts give you visual cues which are better to work with manually, and conceptualize strategies for. But programs do not see things in chart presentation, they see it in equations, variables and data. But for you and me, the visual representation works well – like seeing the analog needle of your car's speedometer is more effective than seeing digital numbers.

You don't need to know how to exactly calculate the ADX, because it is not something that is of much use unless it is done in real-time to evaluate a trade, and most programs and web trading portals provide it. Instead of showing you the long and tedious calculations, I think it will be time well spent to describe its efficient use.

With the ADX plotting in real-time at the bottom of the chart and the moving averages superimposed on to the price chart, what you get is one statistic backing up another. The ADX shows you the momentum of the counter or the move. It goes between 0 and 100 and that

indicates the percentage of strength. Anything above 80 shows significant momentum in a particular trend, and anything below 30 shows little (or none). When the ADX line breaks 30% you can start to see a momentum build in the price and you can reconfirm this with the overlapping MA. This gives you an assurance of the signals.

If you are thinking that this just sounds like more work for no additional payoff, I couldn't agree with you more. Where this really comes in hand is when you place this as part of a trading program and the program automatically checks the momentum to determine if a trade is viable. So, in the work up to running algorithms to signal your trades, you should get used to using the ADX so that when the time comes you will be able to tweak the parameters to get better results from the trade recommendations.

Chapter 5: Artificial Intelligence and Algorithms

This is going to be a short chapter because it is only intended to introduce you to AI and programmatic trading. It is my strongest belief that you should get into AI trading, or at the very least programmatic trading, as quickly as possible.

Many traders talk about the art of trading and getting a feel for the market before you actually get into programs and algorithms. But I am in it for the money, and so are you, I assume.

In that case, the thing that you want to invest in, in addition to the T1 line and the Bloomberg Terminal, is a comprehensive trading algorithm and an artificial intelligence platform. They may seem like the same thing, but they are not at this juncture.

The algorithm is one where you can pull various data feeds and tell the program what you want it to do, and it will do exactly what you tell it. If there is a mistake in the program, or the logic in the concept is faulty, you will get suboptimal results and you will have to tweak it yourself over time.

AI on the other hand is self-learning. If something is self-learning that means you get to tell it what output you want, and if that output is wrong, it will continue to chew on the data to arrive at predictions that are accurate.

The way we run our AI is to feed it millions of points of data and run specific instructions that it will then look at and make a prediction, it will then look at the subsequent price data and see if its predictions are correct. If they are, the program learns. If it's wrong, it learns that as well, then changes the parameters until it learns so far ahead that its predictions and strategies become highly effective and accurate. That's what you want. That takes time, as the market is constantly evolving.

Within ten years you will get to the point that you can leave that program to do the trading while you hang out with your pals and take on a new expensive hobby. After all, that's the whole point

of AI, and crypto-economics and cryptocurrency trading are ideal markets to run AI.

Conclusion

The idea of this book is to give you an understanding of cryptos, how they work and how they behave in market conditions. It also serves as a launching point for you to get the best trading mindset and the understanding of what you should or shouldn't do to make money in this market. If you are planning to enter small, that's fine, but make sure you have the infrastructure to support your trades. Don't just open a trading account and hit the buy or sell button based on recommendations you find on random websites.

The trading of Cryptocurrencies is in its infancy, and it is the best time to get into it. The convergence of AI and cryptos has made it a huge area of growth and wealth creation. I can't stress this enough, do not waste your time and resources on random accounts and trades. You have to make this a focus and an endeavor. This is serious business and you should bring a serious mindset to the table.

Whether you look at Bitcoin or Altcoins (Altcoins is the term given to all other cryptos that are not Bitcoin) the trading strategies are the same. Their underlying blockchain may differ, but the nature of the exchange and the way to profit from it remains identical.

Within your basket of investment, spend more time looking at Bitcoin and Ethereum, but also have a healthy exposure to the other nine cryptos that we mentioned earlier in the book.

There will be more cryptos entering the market in the next few years, and then after that, you will see a consolidation of several them and the attrition of a large number of tokens and other coins. What you will see is the nature of evolution play out over the next ten years, and you will have a front seat to it if you indeed get into this full-time.

Do not hesitate to invest in the infrastructure and get to know the nature of the market. It will carry the day.

Introduction

You can't fully understand the workings of any cryptocurrency until you understand the blockchain. That is the topic of this book which starts off conceptually – describing the Bitcoin or cryptocurrency that rides on top of it, but slowly and rapidly looking at sufficient detail so that you can get a good foundation in the functional aspect of blockchains.

For those of you who have heard so much (or not at all) about this thing called cryptocurrency, but don't really know what it is, let's start there. A cryptocurrency is a form of currency where you exchange it for goods and services. This exchange of goods and services for a payment of some sort happens online. Happening online does not preclude it from happening in person. We tend to think of them as being mutually exclusive, but, in actual fact, today's technology has made it possible for us to do instant transfers of payment in person using electronic methods and without the need for using cash. Online payments are just as possible when standing face to face with your counterpart, as it is with one sitting in the Arctic, and the other in the Antarctic.

Having sad that, this cryptocurrency is completely independent of any form of central authority and so cross-border transactions are easily accomplished. It takes less than an hour and, in most cases, just 10 minutes to effectively transfer payment from one person to the next. The biggest problem that this kind of system will face, if you think about it, is that there is no enforce of trust. That was the whole point of the trust institutions being erected at the start of civilization. A central authority was needed to make sure that everyone was kept honest and that money would change hands as promised, but the cryptocurrency does away with all that and makes the system trust-neutral. That means we do not need a centralized system to act as the trust institution. We don't need to have anyone print or manage the supply of currency and we do not need any unnecessary printing of currency and waste of paper. Instead, the trust system is kept in what we call a blockchain – which is the topic of this book. We will get to that in more detail shortly, but, for now, we are just getting underway to understand the fundamental overview of

cryptocurrencies.

To get a good grasp of the cryptos, we need to think about the role of money. We use bills – paper notes and metal coins, which we call fiat currency, to market the value of the exchange. If you buy a stick of gum at the newsstand, you exchange that stick of gum with a certain value when you hand the cashier a dollar bill. That dollar bill symbolizes the trust institution's guarantee that you will be able to use that same value when you take that dollar bill and give it to someone else for another purchase you make. This means that the dollar bill moves from The Mint when it was first printed, and goes to the bank and to the customer and, from there, it passes hands constantly until its service life is over and it gets sent back to the treasury and is incinerated. When it is incinerated, another bill takes its place. Nothing new is created and nothing old is destroyed; it merely carries the value of one person's labor and contribution.

If you think deeply about it, the ubiquitous paper currency is convenient to use in person, but fails when we can't shred it up and transmit it across broadband to pay for an online purchase. It is more important that we start leaning towards the use of a currency that lends itself to electronic transmission.

There are two things that you need to consider when you come into electronic transmission. The first is that it gives you an opportunity to re-engineer the outdated and expensive trust institutions, and the second is using the centralized systems creates a little bit of a problem as it places too much value in a centralized location. Think about the hacking and theft of online assets. When you put all your assets in one location, any breach will compromise all that. The centralized model, even in data storage, is not that preferred these days.

As an example of the online world and looking to decentralized systems, look at the world of cloud storage. It is increasingly trending towards the use of decentralized and fragmented storage solutions that provide safety and reliability, while protecting against targeted cyber-attacks (i.e. hacking and DDOS attacks) or physical attacks – like property destruction.

In fragmented distributed storage, a single file is broken into smaller pieces, and each piece is then encrypted and sent to multiple locations. There are also duplicates kept at other locations as well. When the user wants to retrieve it, his app pulls all the files from the locations and brings them back and decrypts them. This way, when a server is attacked, the data stays safe.

That is not an example of a blockchain, but the distributed files storage systems use of blockchains to keep track of the data. The example was more to illustrate the value of decentralized systems over centralized ones.

In cryptocurrencies, there is no physical manifestation of value (like the dollar bill); instead, the value is taken from each person's word or promise. It is a messaging system that keeps track of this intent to pay and then transacts that payment. It is called a distributed ledger because it is like a massive ledger with millions of people all paying each other by their word alone, and without a single piece of paper.

That ledger is part of the blockchain and it keeps a record of every transaction in the system, and everyone has total access to that ledger to understand the records if those payments are valid, to confirm ownership of assets, and to facilitate the transfer of value.

The blockchain is the engine that drives all this. On top of the blockchain, everything is just a messaging system. Within the blockchain, the algorithm is sophisticated and, more importantly, the strength of the system is not predicated on the power of the coding, but on the structure of the system. That makes it virtually unhackable from a system's perspective. There are certain security issues but, so far, the system itself has been robust. As we go through the rest of this book, we will discover the genius of the messaging system and the blockchain that supports it underneath. To do this, we will look at the cryptography involved, the common vernacular and definitions of cryptocurrencies and blockchains, the blocks that make up the blockchain, and the proof of work in the mining process.

The bulk of this gives us the full handle we need to form a solid foundation in cryptocurrencies.

Remember, the currency is only as robust as the blockchain under it, and the same goes to your understanding of it.

Chapter 1: Fundamentals Of Cryptocurrencies

To understand the ecosystem, and before we reintroduce the concept of messaging intent to transfer value, we will look at the ecosystem of a blockchain and the basis of a coin or token in the world of cryptocurrencies. The definition may seem alien, but it is fairly easy once you get through the basics. The terms are not listed in alphabetical order, but in the order that will best serve you in layering on the understanding of the subject matter.

Nodes

Nodes are a good place to start. They are the points in a network and are typically considered the computer or terminal in each netw0rk, but they are actually, and more specifically, the instance of the Application that is running the Bitcoin protocol – which is called Bitcoind. Each node has a particular address and starts off by getting online, then downloading and installing Bitcoind, if you want to be part of the Bitcoin network. Other cryptos have other blockchain versions and instances and have different apps that create this on your computer.

There are approximately 12,000 nodes in the Bitcoin system, and this can be visualized on a map. You can find that here: https://bitnodes.earn.com/. The nodes form the network that is decentralized and each node can talk to another node if it wants to and, over the life of the network, every node would have talked to every other node. This is essentially a P2P network that we will describe next.

There are two kinds of nodes. The first is a lite node and that node just keeps track of the transaction that node has taken part in, and the other is the regular node that keeps track of all the transactions in the entire ecosystem.

P2P

P2P stands for Peer-to-Peer and it is a network that people, through their computers and devices, can become a part of it. P2P initially was popular for its file-sharing features during the days of Napster. The content was deemed an infringement of copyright, but the technology and the concept was quite sound. It just didn't go anywhere until the advent of cryptocurrencies.

There is no need to do any major programming as the app will usually do everything that is necessary. You just have to load it up, install it, and the app will open up a port – typically port 8332. From there, it connects to other nodes in the network and communicates pre-determined information. It doesn't allow anything in the rest of your computer to be seen or shared. The P2P format is just for a way for individual computers to come together and become a network without any centralized server. In the typical internet infrastructure, there is a client-server relationship. All the data sits in the server, and the client engage the server and ask for the information. The information is centralized and, if in the event of a hack, a DDOS (Distributed Denial of Service) attack that disables the server, or even physical acts of terrorism on the server farm, all will be lost. In the distributed system, an attack cannot disable the entire system because each node is not dependent on the other node. If one node goes down, there are still numerous nodes left to fill the gap in any way. In the Bitcoin ecosystem, the nodes broadcast information to each other. It is the way to spread information across the network. If one node gets hacked or DDOS'd, the other nodes can still provide reliable copies of the information. The advantages of a P2P network versus a centralized server architecture can be appreciated, especially in blockchains. When you add blockchains to a P2P network, you get a system that is robust and impenetrable, yet easily deployable across a global landscape.

Ledger

A ledger only seems to invoke the notion of a great big book that stores all the information of each person's account, its current balance and the transactions relevant to that account. If that is your notion then, you are almost 100% correct. The ledger is an electronic record of all transaction, from the transaction of the very first coin, to the very last transaction. Every single one of those transactions can be traced back to the very beginning, and those transactions can be mapped.

So, in essence, this ledger is a live document and the updates are transmitted across the node that keeps a copy of their ledger on the computer that hosts the app. That ledger has grown to a fairly large file at this point. Each time a person starts up a new node, they typically have to download the entire ledger from the first transaction all the way to the most recent, and then keep its ears open to update the ledger as and when a transaction is complete.

The value of this distributed ledger is priceless and inexpensive. Each person who is a member of the network, and who uses the network, bears the cost of his own computer and it is incidental to his own use of the computer, so the cost of the distributed system becomes fragmented and inconsequential. This is the first benefit of such a system. As opposed to the public cost of maintaining a centralized infrastructure to print, regulate, enforce and defend the currency, cryptos are relatively uncomplicated and market-driven.

The node's responsibility goes more than just maintaining the ledger, it is also tasked with reviewing the transaction that is transmitted to it, and to figure out if an address has the funds it needs to spend it, or not spend it twice.

Gossip Protocol

The nodes in the network communicate on an algorithm with the Bitcoind called the gossip protocol. When a block is completed, that block needs to be transmitted to the ledgers contained in each node, and that block has a certain identification number. One node will ask another node if it has that block, and if that node doesn't, then it will transfer that block for this new node to save. That node will then randomly select another block and find out if that node has the new information. It also does another thing. Once it has told the node its information, it asks that node if it has other new information and compares it to what it already has. If the information from the other node is not within its ledger, then it will take that information as well. That way there is a two-way exchange of information.

Each node contacts six other nodes (in most cases that is true, but you can adjust your Bitcoind app to contact more nodes if you like). In most cases, nodes just contact six others at random. The node they choose is randomly selected and so, each time it opens a communication to a node, it is a different set of nodes. This keeps the system safe by not allowing predictability of who the node contacts are.

If each contact six, then theoretically, it will only take six hops from any new piece of information originating from a node to reach all existing nodes. Think about it like this – the first node passes it to six nodes and each of them pass it to six more. That makes 36 nodes that are now up-to-date on that information which was broadcast by the first node. Those 36 then broadcast to six more which makes it 216. That's three jumps so far. From there, it becomes 1,296, and then 7,776 on the fifth hop. On the sixth hop, it becomes 46,656, but there are only 12,000 nodes at this point which means that it only takes a little over five hops to disseminate all the information of every transaction to the entire ecosystem. That happens in just a few seconds and everyone is up-to-date. The gossip protocol is extremely effective and can be used in larger ecosystems effectively.

Consensus Methods

This consensus algorithm is a feature contained with the blockchain's algorithm. It is a core function in that it keeps the system in check and avoids the forking of the blockchain. It can be said that the consensus algorithm is related to the gossip protocol because it tells the next node what it knows, and also checks to see if that node has anything to add. It tries to build a consensus of what is right and what is not. An occasion that requires the execution of the consensus protocol hardly happens, but if it does, the protocol staves of a forking in the chain.

The consensus algorithm takes information from the node population, attaching it to the previous block that it has in its version of memory. In the event that someone tries to make their own block (or alter a block to include an unsanctioned transaction), the few nodes around the offending node may accept the block for a few moments. The moment they receive word of the other block that has really been accepted by the general network population, and that information gets to them, they will now realize that there are two blocks in the system vying for the same space in the chain.

Because two blocks can't occupy the same spot in the chain, the nodes that receive conflicting information will await the next confirmation. They will then look at the block that was used, and they will also use that block. Eventually, the block that has the longest chain survives.

For any block to be confirmed, it has to have the consensus of 50% + 1 of the nodes in the network. The only way the node in the network will accept the newly minted block is if it is part of the longest chain. That is the only way the nodes (or rather the algorithm in the nodes) will reach a consensus. If there is a discrepancy as we mentioned earlier, then the nodes will wait until the next block is attached and then the next block, and then the next one, until it starts to see the pattern of blocks that are slowly increasing. It will then erase from its memory the offending block. The entire network will reflect the appropriate transactions in the block at that point.

This is why you should wait for at least three confirmations to ship your product. It is not until there are a few confirmations built on top of the block that contains your transaction that you can be confident that the payment is legitimate.

Messages

A transaction is when Mr. A sends Mr. B a message saying that he is sending him 1BTC. Remember that's all it takes because it is a message. Once the message is sent, the system materializes the intention of the sender. The first thing the node does is check if the sender has the right to spend that 1BTC. Basically, it checks to see if the balance is sufficient to cover the intended amount to be sent over. If the amount is sufficient, then the node conducts 16 points of verification that is found in the logarithm and, if that all checks out, then the node broadcasts that transaction.

These are the list of checks that it conducts:

- Each transaction, which is a message, must be less than the maximum block size of 1 MB.
- Transaction sizes must be greater than, or equal to 100 bytes.
- The value of each transaction must not be less than 0 and not more than 21 million BTC.
- There can be no hash inputs that are equal to 0.
- The complete data structure is correct.
- The locking script must match the standard format.
- The lock time must be less than the maximum allowed number.
- The number of signatures must be less than the signature limit.
- Unlocking script can only push numbers onto the stack.
- With each input, the output must exist and not have been spent.
- All input and outputs must have values.
- The full transaction's syntax must be correct.

But that transaction doesn’t go to the rest of the nodes. It is then placed in a queue and sent to what are called miners. Miners need to take this transaction after the node verifies it and place it in what is called a block. We will look at what a block is a little farther down. In most cases, once the transaction is done, it is considered complete, but it is always best to wait for confirmation that the payment is complete. Confirmation is done by the mining process. Mining is done by miners and is described in the chapter on Mining.

Account Balance

The account balance that you see in the software does not have some kind of recording of the amount you send and receive, meaning it doesn’t record your activities while you send and receive. Instead, it looks at the blockchain to get the data it needs. The wallet scours the blockchain for every transaction that that address was a part of. If there were no transactions, then the account balance would show zero. The point of this is that you can log on to any Bitcoind node and enter the address you are looking for and it will always show you the current balance in that account. You don’t even need a Bitcoind app for that; in fact, you can even go to the Bitcoin website and look up an address and you would see the available balance and the transaction history of that account. When you open up your wallet, you would have to enter the address you are interested in messaging from, or accepting funds and look at the balance. If you want to move that balance, then you would have to provide the private key and move it from there.

Genesis Block and New Coins

Most of you would have heard of this thing called the Genesis Block. As you can imagine, it is the block that first started out and it was the block that transactions from the coins that the developer awarded himself. Since there was nothing to mine at the time and the coins had to come first, the initial transactions were done by the developer, and when he mined those blocks, he got more coins. It started from there and, eventually, as more people caught on, more miners were needed to put the transactions in blocks. You will see how this works in the Mining chapter.

New coins are added to the network every ten minutes, or thereabouts. The exact time is not fixed, but it is fairly accurate. The reason is that the coins are not released randomly. The miners have to solve a puzzle in order to get the reward – that reward is in the form of new coins. The miner then sells those coins and gets whatever he agrees for in return. In most cases, the miners go to the exchange markets and exchange them for fiats because their mining equipment and computational power and energy usages are paid in hard currency. That does two things. First, it allows new participants to come in because there is always a seller among the miners, and new entrants have a way to get new coins. The second is that it increases the supply of coins in a predictable way. That keeps the inflation of BTC at a predictable and falling rate over time. The maximum number of coins that will ever be released is 21,000,000 and that amount will be reached in the next few years.

There are no other ways of creating new coins and, once the system reaches its limit, those are all the coins that can be in the market.

To avoid a supply problem, you have to realize that the coins are not limited by their denomination. Each Bitcoin can be divided into 100,000,000 (one hundred million) parts. Each part is called a Satoshi. In the event that the limit is reached and the coins are so successful and prevalent that a million more users come on board, then the market price will adjust in a certain

way that it would be common place to transact in Satoshis than it would be to transact in Bitcoins.

It is a reverse inflation question that is resolved by the management of the denomination. For instance, you now pay about 10,000 USD for 1 BTC. For some people, that's more than they need and they just want to buy a little at a time to pay for the ISP service – for instance. That ISP is charging $10, payable in BTC, which would be 0.001 BTC. If I purchased 1 BTC for this, it would last me 1,000 months. So, what's the point? Instead, I can buy 100,000 Satoshis or 0.001 BTC for $10 and use that to pay my ISP, but that example is not to tell you to pay your ISP with BTC; no, it is about showing you that you can break a BTC into its smallest component. When you do that when the supply of BTC stops, the fiat value of something can be expressed in Satoshis rather than in BTC, so, instead of having only twenty one million units of BTC to work with, you can have 2.1 trillion Satoshis. That would be enough to supply the world for some time to come.

Chapter 2: Cryptography

There is a significant amount of mathematics that goes into the entire Bitcoin ecosystem - from hashing, to cryptography, and even probability, and that is then merged with the powers of computing. The outcomes are a structurally-secure platform that can handle the demands of a robust online currency and still be run semi-autonomously without the need for central authorities, and yet be trust-neutral.

To understand the power of the blockchain better, it is best that we dive in headfirst into the cryptography that drives the whole thing. After all, that is what it is called crypto – for cryptography.

Hashes, Hashing and SHA 256

To understand the cryptography, the first thing we need to look at is the SHA 256. This is a 256 bit Secure Hashing Algorithm. Without getting too much in the way the algorithm works, you can easily go to an online hashing website and enter whatever you want and get the hash for it.

Try it.

Go to https://passwordsgenerator.net/sha256-hash-generator/

Place this sentence in the box: The Cow Jumped Over The Moon

In return, you will get this:

3474A5E82F8FED7D5C9FBDC181ED562815C7C95F2D0C6B2D10C502ECB2A39043

Now, place the same sentence, but just alter the first alphabet and change it to lower case, like this:

the Cow Jumped Over The Moon

Note that only the first alphabet has changed, and even then by only altering the case and, when the sentence is put into the box and hashed, this is the outcome:

E7EEA2B7CE4F32A53337A15D85F5F2B5A6A8E65CEE6283117C8432C58FF68E70

For such a small difference in the change of the original sentence, the change in the output is starkly different. This is one of the reasons you cannot reverse engineer the original phrase; hence, it makes it a secure hashing algorithm.

If you haven't guessed it, hashing just means to change any sentence and put it into the seemingly random character string. Here is another example. If you take the entire Introduction chapter from this book, which is over a thousand words, it gives us this:

821EA5FEFA1E48DE85E30E13378A616CECD188D2CD609A2B315472ED4C474DFA

It still gives us a similarly-looking string of characters, but you will never be able to reverse engineer this string to return to the content of the Introduction by just the hash. This makes it extremely secure.

Private Keys

The key to the entire thing as far as a user is concerned is the secrecy of his private key. Users have private keys that can authorize payments when one sends a message from an address. The private key is the core of everything. If you lose your private key to the address, then you should transfer your money out and get a new address. The secrecy of the key is of paramount importance.

Private keys are generated first. It is a random number that is chosen from a robust random number generator between 1 and $2^{97.}$ It is impossible to guess any number, or to end up using it more than once. To be able to guess that number will take more energy than there is in our sun, so the number is fairly secure.

Once a random number generator gets this number, it can then be converted to a public key and that public key is then converted to an address. Now that you know that the hash only works one way, you will also know that the Bitcoin address that is given to anyone to send the message to the money cannot be reverse engineered. This is the way the private keys are kept secure and this is the way that the entire Bitcoin infrastructure is managed.

Just for fun, if you take a simple number, your birthday perhaps, and take a hash of that, so let's say your date of birth is 1.1.1911, so you put in 01011911 in the hash generator, this is what you get:

FA372F9E71529403A63AFFB4E5C04E466E63D567CB054F1CBFCFD5B7FCD36E50

Now, imagine that is the string you want to use as your private key. To convert that to your public key, it requires another mathematical operation. We will look at this in the next section.

Public Keys

With the private key in hand, you can now generate the corresponding public key. To generate the public key, there is an asymmetric mathematical function that takes one number (the private key) and plots it on an elliptic curve then generates the public key from the resulting line that intersects the curve. So, in essence, the public key is derived from the private key, but you cannot reverse engineer the private key from the public key. You must always keep the private key confidential and, if possible, try not to keep it on your computer in case it is hacked or has catastrophic failure. If you can, place it in a cold wallet – something that does not connect to the Internet. Use it only when you need to spend the money in a particular address.

Bitcoin Address

Your Bitcoin address is where someone who is paying you sends you the transaction message, but, remember, this is not a bank account, but more like an email address. They are merely sending you a message. Inside that message, you can write anything you want in addition to the message that specifically includes an amount of the funds to be transferred. Remember the other nodes will check this. If there is insufficient value to transfer, then the message will not be included in the block or unsuccessful.

This Bitcoin address is mathematically linked to both the public key and the private key, by extension. It is merely the SHA256 hash of the public key.

So, now what you have are three numbers that constitute the core of the Bitcoin network as it pertains to you, the sender, or to you as the receiver.

You use the Bitcoin address to send and receive funds, you then use the public key to show that you have the right to send the message from the address and you use the private key as the password to prove to the system that you indeed have the authority to manage the account and dispatch the message.

To put it simply, when you put in your private key, the app automatically looks to see if it corresponds to the public key. If it does, then your message will be authentic and that would result in the message being permitted to pass through the network.

The five things that you need to prepare you for the upcoming blockchain overview is the hashing algorithm used in all things related to Bitcoin – the SHA256; you then need to understand how private keys are generated and what you need to do to keep yourself secure so that no one can guess them and no one can brute force them. You then need to understand the role of public keys and how Bitcoin addresses are generated. You have all that. With that, you can now go on to the next layer of the issue which are blocks and transactions.

Chapter 3: Blocks and Transactions

Before we get into miners and mining, we need to make a quick stop at trying to understand blocks and transactions. It is important to know and understand that Bitcoin transactions are not typical remittances that we think of, but rather they are messages of an indication to give someone (the recipient) the value (in Bitcoin) that you (the sender) already possess. I repeat this often in this book because there is a large body of misunderstood and ill-described material out in the ether. Many people still think that cryptocurrency is a physical coin because they see these images online that show a conventional coin embossed with the Bitcoin logo and the circuit board etching and think it is some form of an electric coin. None of this is true and you have to really understand the concept of the message and the transactions that is driven by it.

It is the ultimate contract where man's word is literally his value – when the message is sent – it is as good as gold. That's the point of Bitcoin.

Ok, so we already know that transactions are messages that go from sender to receiver and that message transfers a certain amount that the sender has to the receiver's address. But where does that value come from? How does it get injected into the electronic network and the Bitcoin network in particular?

Your currency should be convenient for your habits of exchange. If you go to the marketplace in the town's square, then carrying wads of cash fifty years ago was appropriate. Today, the town square has become the global square and the marketplace has become accessible via the Internet but the value carriers only lend themselves to physical exchanges.

But where does the sender get it from? Well, the sender has only three ways of having a coin in his address. He either mined it, bought it, or someone paid him for a product or service. He cannot just create it out of thin air – and that is an important point to make for two reasons. First, for those of you who are thinking that you could just make a string of numbers up, you can't, and I will explain why in a moment. Second, you can't just spend it twice either – well, that is

another way of making your own coin, and you can't do that either. The system is very adept at preventing that from happening and it's not just the code that is in the system but the fact that it is a distributed system. I am a pentester, and I have tried, as an exercise, to penetrate the Bitcoin nodes in my basement from a remote computer. I can't ever seem to break the system, and that is a good thing for many reasons. It means that the only weak link in the whole chain is the person holding the private key. In that way, it is like pasting your ATM pin number on your card so you won't forget it. If you can keep your private key safe, you are not going to lose your coins.

This brings us back to creating coins out of thin air – you can't. The whole purpose of the blocks in the blockchain, and the mining that is required, is threefold:

1. To allow miners to expend something of value in the real world so that something of value can be created in the electronic world.
2. To give each coin or token legitimacy by giving it the credibility of past use. The more it is used, the more subsequent users know that that coin has the ability to be a legitimate carrier of value – that chain of blocks replaces the centralized need for a trust institution to legitimize the carrier of value the way governments do for paper currency.
3. Finally, it precludes forgery so that not one, but every participant is able to validate and store the credibility and legitimacy of the coin. This obviates the need, again, for a centralized system.

To get a more internalized understanding of this, it would serve you well to look at the philosophical and historical evolution of the mechanisms of exchange. We can't go through the full details and full history of the evolution of money, but we will do the best we can to give the current issue context.

Philosophy of Equity and Exchange

This is the crux of the whole Bitcoin value transfer system and this is where you need to disengage your mind from what you and I are so used to. We are used to the printed piece of paper with Jackson, Franklin and Washington printed on them to be something of value on its own. We forget that fiat currency only represents a value. It is in paper form because it's a lot easier to fold and put in your money clip or wallet. That makes it easy to carry around. Imagine having to carry around a cart full of gold to make your transactions. That dollar bill merely carries the value of something that you did in the past to get it that value. You may have labored at the office, or profited at your business, and your contribution of value resulted in the conversion of that dollar. That dollar on its own is a piece of paper. It has value because you worked for it and the sovereign government of the land you live in has printed these (supposedly) unforgeable mediums of exchange as a public good.

That fiat currency – the dollar bill, or gold coin, is just a vessel of value. The actual value itself is not that thing that carries it. You went to work, got paid, took that money and bought bread. Money served as the medium of value that could easily move between getting paid by your employer, to being used as the medium to purchase products so that it made transactions more convenient. Otherwise, you would have to go to the baker and barter him with your skill to get a loaf of bread – what a headache.

So, what we have established painstakingly is that value is different from its carrier. Now that we know that, then we can willingly make the carrier more relevant to the venue and method of interaction. We used physical paper when we traded physically. Now we trade electronically, so something electronic is appropriate. We already mentioned this part and you get that, but here is the point of all this. You see, printed fiats have one thing going for them and that is that the government that printed them places their weight behind the piece of paper and says that they stand behind it – and that gives the people the assurances that they need that the paper can hold

the value that the people put in it.

Make no mistake, the value of the currency does not come from the institutions of trust that the government represents, the value comes from the labor and contribution that people put in to it; whereas, once the government provided security for it, they also ended up giving it value because the fiat was backed by the total output of the country and managed by the supply of the printed bill. In cryptocurrencies, none of that exists and so the only way you can give the currency value and give it credibility and give people the confidence to use it is if it has a track record. By that, I don't just mean that Bitcoin in general and as a whole needs to get credibility, I mean the value and utility of each Satoshi and Bitcoin needs to have the credibility. In fact, to make it plausible and serve as a carrier, that carrier must have a credible starting point and usage over time to develop a history of its use. Without that history, and without that credible starting point, that coin has no value since it does not have the backing of a sovereign body.

I know it's been a pretty philosophical and long trip to get from the start of this discussion to this point – but it is necessary to describe the weight of the blockchain. You would be remiss to undervalue the prominence of the blockchain in the future of human interaction, and it would be easy to dismiss it if you did not understand the philosophical aspect of the blockchain.

Because human exchange is about the exchange of value, and value can only be created by expenditure of effort, it would be impossible to transition from the physical world to the electronic one without the correct procedure and without effort.

Transactions

As I mentioned, each transaction transfers a certain amount of coin from a person who has it, to a person who is about to receive it. A person without a coin in their account can't send any, but a person with a fresh, brand new address can receive any amount. There are no limitations to creating as many addresses as possible. Remember, the number of addresses you can open is equivalent to the number of private keys you can generate. There are 2^{97} possible private keys that you can generate and while that may look small, here is what that actually looks like:

1.5845633×10^{29} - to make that more evident – that's:

158,456,330,000,000,000,000,000,000,000.

To put that into perspective, earth has 7.5×10^{15} grains of sand. That means if each grain of sand was an earth-like planet that had the same number of grains of sand contained within it, then the number of private keys you could generate would all the grains of sand combined. Get it… ok, it's a lot. Trust me on that one.

The reason we take the trouble to make it a point to stress this is that the chance of a collision is remote, in statistical terms, and this just means that if you keep the pick of your private key perfectly random, the chances of you finding a private key that hasn't been taken yet is very close to zero.

Those odds dramatically change if you pick a number that you like – your birthday for instance, or your anniversary and then try to convert that to a hash and then use that to create the public key and a Bitcoin address; what you will find is that it's probably already taken. The collision rate goes up significantly the moment you do not let the private key be randomly picked by a truly random number generator. You can find one here: https://www.random.org/strings/

Once you pick a random number, you can write that number down somewhere and then, my suggestion is that you run it through a SHA256 convertor like we did earlier and that will give you the hash of that number. You can then take that as your private key and generate the public key from there and then get a Bitcoin address from there.

All that is comparatively a lot of work, because if you have a Bitcoind on your computer, it is going to generate an account, and a public and private key for you as many times as you want. By the way, you can download that here: https://bitcoin.org/en/download. It will be as easy as pie and you should just stick to doing it that way. I have mentioned the process so you understand how it's done and that will give you an understanding of how the blockchain works as well under it.

Now that we took that minor detour, let's get back to our topic of transactions. When you conduct a transaction, it is a message telling the world that you, Mr. A, are sending Mr. B, X BTC. Remember, you are not just telling Mr. B, so be careful of the text message that you include in the message. Once you send that message to the world, all nodes are listening. Remember the gossip protocol as it starts to work at this point and the message gets into the queue and the nodes go into action to verify that your message can be a message. Assuming all goes well, the transaction is righteous and it gets confirmed and the recipient is now the legal owner of the coin.

The coin takes on life because of transactions, and the transactions have value because of the coin. There are two aspects of value when it comes to a coin. The first is that no coin comes free – putting aside the initial coins that were released to the developer to get the ball rolling, but, even then, one could convincingly argue that the coins were reward for the sweat equity that was put into the development of the protocol and the algorithm that was built on top of it.

From the very first transaction until today, every coin starts its life with a certain intrinsic value. That value is defined as the value that miners put in to do the computation necessary to create the

block. Why we need the block, and how that is important, we will talk about in this chapter, but in the next section.

The second part of the value that can be assigned to the coin is the value of net demand. If net demand is positive, then the intrinsic value that the coins have will gain a premium. If the net demand is negative, then the coins will erode from their intrinsic value and eventually grind to a halt and be worth nothing.

As with anything in commerce, the value of one thing can exist in a vacuum, but to know and transmit that value, it has to be expressed in terms of another commodity or item of value. In the case of Bitcoin and other cryptocurrency, there is a vibrant exchange market that gives you an accurate determination of value in almost any other fiat currency of value. In US dollar terms, the value of BTC (Bitcoin)has risen from mere pennies per BTC to $5, then on to $50 and on to $500, and all the way up to almost $20,000. Yes, that was twenty-thousand dollars. It wasn't a typo.

Old school economists can't fathom why something that has no tangible link – like how the dollar is linked to the sovereign wealth of a country, can end up being worth so much. The reason is not because it is a secret currency or that it has some nefarious advantage; what they don't get is that it is the appropriate innovation for the colliding of two socio-economic phenomena – online commerce, and distrust of centralized authority.

The value of the Bitcoin has been defined by the Fiat currency put in the physical world. Some people think that that makes BTC untenable as a major currency in the future, but that doesn't matter, because Bitcoin in itself is not designed to displace sovereign currency.

The things to remember about transactions are this:

1. Transactions are messages that are broadcast to the entire network and are carried across the nodes by the gossip protocol.

2. All transactions are irreversible, so don’t make a mistake.

3. Each transaction is automatically given an irrevocable transaction ID, regardless of size. A transaction ID looks like this (example): 447aebdb9e8c42dd3b617e5e5785634205a96af9d1500ae5b7af03127e186e0a. If you click on it, it will take you to the blockchain.org and give you the information of that transaction.

4. Each TXID (transaction ID) will list out the address that sent the payment and the address that received it. Details about TXIDs are presented next.

Transaction ID

That transaction ID is then placed in a pool - assuming that the nodes have considered the transaction to be legit. Once the transaction is in a pool, all the transaction IDs plus the header information (typical things like date and time stamp, block number and something called a nonce) is placed in the block and hashed.

Hashes and hashing were described and discussed in Chapter 2. Once they are hashed, the block returns a unique string of alphanumeric characters. You saw within that section that even the smallest change, like altering one character in the entire text by changing it from a lower case to an upper case, renders the hash absolutely and unmistakably different and thus changes to it can't be made if you do not want to disrupt all that is built around it. Even if a person were to hack a system and sneak in a transaction retroactively, the hash wouldn't match and the nonce wouldn't work and the block will fail but, if somehow a malicious actor was determined enough to mine the block and get the proper nonce for the block, the problem is the hash for the original block was placed in the subsequent block and hashed out. Remember that each block includes the hash of the last block among other things so if you want to alter a transaction six blocks deep, then when you go to hash that block, the hash that is supposed to appear in the next block will change, and that alters the next block. If you want to go ahead and alter that block as well, you would have to put in a huge amount of hashing power just to get one transaction changed. After two to three blocks, the benefit becomes unworthy of the effort.

But mining is not so simple because within the transaction IDs, time and date stamp and previous block number, there is that thing we call nonce. Remember that? Well, the nonce is a really a random number, and that random number is used to control the resulting hash.

Why does the system need to control the outcome of that hash? They do that so that there are opportunities for the miners to do the puzzle that process the hashes until it gets the format it is looking for. The first miner to get the hash gets the reward. Once the block is hashed, it is placed

in sequence and the next block is processed and it will include the block hash of the previous block.

Do you see the genius of the system?

Blocks

Ok, so this is where it gets interesting. If you have been looking deeply at transactions, you must be considering how on earth you pass on the value of something without it being subjected to forgery and manipulation. Well, that's what blocks are for.

Each transaction is about 100 kb in size and can vary upwards from there, as long as it is not over the 1 MB limit. As multiple transactions are accumulated, the nodes shuttle them into a queue so that a miner can take them and lock them up in blocks.

This is where it gets confusing for most people, so pay attention.

A group of transactions is called a block, but it does not stop there. These transactions are accumulated and if you look at this block, for instance, block number 520763, you can see in blockchain.info when you search for blocks by number, it will tell you all the transactions that are listed by TXID.

When a block is constructed, it is done so by the miners and that will be discussed a little more in that chapter. When the miners put it together, they typically take them as they are, but it is not uncommon for miners to choose which transactions they want to include and which they do not. There is an incentive for them by choosing the ones that have the highest fees. You see Bitcoin has a standard fee, but senders are more than welcome to increase the amount they are paying to expedite the confirmation times. So depending on this amount, the miners would prioritize the transactions and load them up into a block, and then they get started with the puzzle-solving which is to mine the block. You will see that part in the mining chapter.

Once these blocks are mined, they will be given a block number and they will be layered sequentially. Each block has its own unique composition and unique transaction ID sets. They will never be duplicated and no transaction is part of more than one block. Each block is then stitched mathematically to the block that preceded it and the subsequent block will be stitched

mathematically to this present block.

We will show you all of this in the mining chapter.

But the point to make here is that because the TXIDs are unique for every transaction, the number just can't be used again, and the fact that the number will never be repeated makes it impossible for anyone to alter the transaction by using the same transaction ID. If you add to that, that once the TXID is placed in a block, and the block is tied to the previous block, then it is impossible to undo anything that happened in the last block because that would alter all the subsequent blocks after that.

Blocks give individual transactions the credibility of existence and confidence of usability. It obviously works because the market price has been consistently above $5000 per Bitcoin – more than the price of gold. Check out the historic price of Bitcoin here: https://charts.bitcoin.com/chart/price#cat-market

We call it a coin to make it easier to explain, but you have seen there really isn't a coin physically present and here is how I can illustrate that to you. You know that 1 BTC can be divided up into 100,000,000 Satoshis. That means if I sell my car to a friend and he pays me 1 BTC for it, I now have 1 BTC in my account. I can then send out 1,000 Satoshis to someone for mowing my lawn, or 1,000,000 Satoshis to my ISP and still have a balance of 98,999,000. If it was physical, how did I just break it up? Ok, so it's not physical.

Now that we understand the nature of blocks, we will see what is in it, how it is formed and how it is stitched together in the next chapter.

In wrapping up this chapter, we have just begun to understand a major component of the blockchain and thereby understand the mechanism under the hood of cryptocurrencies like Bitcoin.

Chapter 4: Miners and Mining

Miners do the mining, so if you know what mining is then you know what miners do. So what is mining? No, it is not taking a pickaxe and chipping away at a cave wall to expose the precious metal in the stone.

Mining is a computational and mathematical process that places these blocks we've talked about in previous chapters in a sequence that cannot be retroactively altered. Once the transaction is in the block, a confirmation is said to be complete. That takes about ten minutes. If you really want the transaction to be solid, in the event it is a large transaction, then wait for six confirmations and you can be dead certain that the transaction is confirmed and without any possibility that the sender will reverse the transaction.

How does this work?

While regular nodes are in charge of going through a checklist and making sure every transaction that is broadcast to them from a neighbor passes all the time on the checklist, the miner is responsible for something just as important. The miner has to legitimize the blocks and tie them together to the preceding block.

This takes a large investment and a tremendous effort and is not as simple as one may think based on the description earlier in this book. In the rest of this chapter, we will go through the other processes and show you how difficult, expressive and how it requires a high level of skill to execute.

To act as a barrier, the Bitcoin system requires that only able parties are invoked in the mining operations of putting together blocks. What is even more brilliant about this system is that the difficulty and complexity scaled up with interest. When Bitcoins first entered the market, almost anyone who wanted to be a miner could – they just needed a regular old PC to do it and they could start mining but, as more and more people got clued on to Bitcoin and wanted to mine, the

processing requirements evolved.

It now takes expensive equipment, and lots of it, to be able to make a return on your effort. There are not mining farms as large as factories and this has precluded the individual from using spare resources on his laptop to participate.

Just keep this at the back of your mind as we start explaining the proof of work and why it’s needed and then we will expand from there to the complexity of the mining process and how that is determined.

Proof of Work

To put it simply (and we will explain this here in greater detail) your Proof of Work (POW) is the way the system knows that effort has gone into creating the block. This is how it knows that the lock was not just thrown together and that resources of value had to be expended in terms of time, energy and assets that had to be deployed to do the work that comes up with the solution.

The proof of doing the work is contained in the solution to the puzzle. You can guess at it, or you can approach it from a particular direction; you can come at it in any way you want, but the point is that you have to work at it and keep trying until you get it. When you do, and if you are the first one to solve the puzzle, then you get to submit that block as the next in the chain and get your reward for that.

The miner first chooses the transaction he wants to place in the block, and then starts to conduct a hashing operation on it. The transaction IDs are placed in a Merkle Root and the rest of the information is added. This, as you saw, includes the time, date, previous block’s hash and the nonce.

This is where the puzzle comes in.

Puzzle

The puzzle is to solve the nonce. Let me show you how. Imagine that the information that was to enter the block included the following items, and let me just use random information to mimic a real block.

Received Time

2018-05-02 00:01:47

Miner

SlushTool

Previous Block Hash 00000000000000000003169d3297051de41502f769f2c36f6abffa7db8985ba77

Merkle Root

57c16f1ab60394b5de123835f4f4beaafbc9629429292b0cb238fc228f798f70

If you were to hash the above information, you would get this:

EB603B946FDA9F623C2D8770B60DA775AD7B99EAC082B319116BA39664A6D04E

If you notice, the nonce is not present in the information above, and it is not in the hash result. Now, just to prove a point, I am going to just say that the nonce is 1 and so I am going to add the number 1 to the whole thing and run the hash program again. This is what I get:

E8B3CB25EA9D72236999330B7D2AFA878FDE9AA35D16A6EF42F52D4024972247

You see the hash has changed.

If I change the nonce to 2, this is what I get:

4A03F84264FADC60A1A9A6BD90C1B1DD3033590C7844DED0166379332559AB83

So, you get the point – changing the nonce alters the hash output. What if my constraint was that I want the output hash to be something that starts with the number 0? What do I do then? Well, since I cannot reverse engineer it, I am left with only one way of solving that constraint, and that is to randomly look for numbers that would get me that nonce.

So, let's say we use this constraint as an example – I want to have the hash start with zero. That means I have to keep randomly guessing the nonce until I find the nonce that results in the hash starting with zero. For this example, I had to randomly try it until I found that the nonce of 222128 resulted in the hash being:

0522BF5F28591F9F6D190EEDACFC700B869D3C35EF3DEF5023D57029589AE448

So, this hash satisfies the condition that the hash has to start with the number 0.

It was fairly simple and it took me a few minutes of repeated calculations to get the nonce I needed, but this was a simple constraint. The typical constraint is significantly higher in complexity and difficulty.

You can see it in two ways. First off, you can see the hash of the last block which is included in the current block. It is:

000000000000000003169d3297051de41502f769f2c36f6abffa7db8985ba77

If you notice the hash has 18 zeros up front. That means the algorithm assigned the miner the puzzle and told him he needed to find the nonce that would result in a hash that began with 18 zeros.

That is not always the case. The system alters the number of zeros it wants the miner to find

based on the difficulty it deems appropriate. One zero is fairly easy to obtain, two zeros in sequential order would be less so, and, by the time you get to 10 or 18 zeros, you would have to hash millions of times before you can get to the answer that you are looking at. However, the many zeros the system is going to constrain you with depends on what it deems the difficulty should be for you to be able to find the nonce. The level of difficulty that is needed can be ascertained at any point by looking at the difficulty chart info here: https://blockchain.info/charts/difficulty

To better understand this difficulty measure and place it in context, we need to look at the hash rate and get an understanding of that as well. This brings us to hash rates and mining rigs.

Hash Rate

The current hash rate can be found here: https://blockchain.info/charts/hash-rate. It indicates that the rate has been rising steadily over time and that it currently stands at approximately 31 million terahashes per second (TH/s). That is an extremely high number because 1 terahash already means 10^{12} or 1,000,000,000,000, or one trillion hashes. Can you imagine the computational power that needs to go into computing 1 trillion hashes per second? Now, imagine that multiplied by 30 million. That's the level of hashing that is going on now in the mining world for Bitcoin to keep the currency going.

Every second that goes by, all the miners in the world are collectively calculating 31,000,000,000,000,000,000 – thirty one million trillion hashes every second. The more miners that come online, the more that difficulty number is going to go up. Miners enter the fray to be the first to solve the puzzle and claim the reward which is 12.5 Bitcoins at the moment. In one day, 12.5 Bitcoins are released every ten minutes. That means 75 Bitcoins an hour are up for grabs. At today's market value of almost 10,000 dollars, that's 750,000 a day that can be gained from mining. This is the reason you see miners flood the market because there are significant amounts of revenue up for grabs.

But the system is built in such a way that the more hash power there is, the more difficult the puzzle. This is because the intention of the developers of Bitcoin was to have a predictable interval between the release of new Bitcoins into the population. Remember Bitcoin is released only through miners as a reward for their mining contribution. To keep this consistently at ten minutes (or close to it), the system monitors the hash rate that is online, plus the timing it took the last few puzzles to be solved. You can see that here: https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html

If the system sees that there are so many miners and the hash rate increases to the point that they

are finding solutions faster than 9 minutes or less, then the system changes the nonce constraint and may say we now need there to be 19 zeros and that will add a few more minutes of processing time.

Mining Rig

This is a good time to start talking about mining rigs and how the Bitcoin blockchain is kept alive. While we are on the subject, you should come to realize by now that in the event that there are no more miners, then the entire system comes to a halt because the blocks will stop being attached to the chains.

Miners are categorized in two ways these days; one is the independent miner and the other is the pool miner.

When mining first began, anyone could do it on their computer and the CPUs could handle the calculations. Back then, hash rates were in the region of kilohashes per second and the CPUs could handle that even if they did get hot and needed extra cooling. But then, as more miners got into the mix, you guessed it, the difficulty went up and so miners competed to increasing their hash power and so they started using their GPU cards which were significantly more powerful than the CPUs.

The competition become increasingly fierce and so specialized rigs were developed. These rigs could actually do little else. Companies like NVidia, manufacturers of video cards, started targeting this market instead of their usual gaming market, and they started offering more powerful hashing cards. Eventually, that gave way to specialized hashing machines called ASICs. These hashing machines couldn't do anything else except calculate millions of hashes.

When that didn't stop the competition, people started grouping their computers and buying up more hash power to coin, and then try to solve the puzzles that way, but that soon was outstripped as well.

Today, what you find are either large mining farms that have anywhere from 20 ASICS running 24 hours, or factories running hundreds of ASICs, or, on the other hand, you find people just buying the equipment and hooking on to mining pools.

Mining pools are just individual miners that get together and combine their smaller hashing power to become a large pool and become competitive in being able to solve the nonce puzzle.

Once the mining is complete and the hash complies with the constraint, that nonce is then left in the block and the hash is advertised. That hash is then used for the subsequent block and then that block is mined.

By doing it in this way, value moves from the physical world where work is done, to the online world where the coins are transacted. The miners spend considerable fixed and variable costs to mine the blocks and then allow the blocks to be verified, confirmed and added to the earlier block.

Chapter 5: Downside of Blockchain

There are numerous benefits to the blockchain technology and there are numerous uses to it in the form of coin, token and currency among other things. The thing about blockchains is that they are hard to grasp, and the maths behind them tends to make people cringe when they are first introduced to it.

Then you add that to the fact that the programming behind the blockchain can be complex when you get down to the nitty-gritty of it, but my advice to you is to not let it distort your perception of the next new thing in finance.

The system's complexity varies based on who you ask. For me, the system is as simple as it can be. For a recent computer grad, there could be some conceptual challenges, but the guys who are in their mid-careers are the ones that will find it a little strange as it is a completely new paradigm. Don't worry though, as it just takes a little getting used to.

When it comes to transaction costs, it is mostly cost-efficient but, for those of you who think that Bitcoin is absolutely free, you need to think again. There are costs associated with it, but the benefits far outweigh those costs – unless you are trying to make micro payments and then the cost is not worth it if you are on the Bitcoin platform. For that, you should try one of the other new coins.

The biggest downside is that it is facing a steep uphill battle with lawmakers in countries that are advanced in technology and backward in thinking. Countries are used to keeping track on their citizens for one reason or another, and their knee-jerk reaction to Bitcoin has been severe. Tread carefully and be nimble when it comes to investing. Check with your lawyer if you have to, but even if you do not agree with the law, you have to follow it.

Conclusion

Cryptocurrencies are made possible by the distributed ledger that is kept honest by an independent system called the blockchain. The idea of the blockchain is to harness the power of the crowd to automatically verify and remember. These nodes are central to the blockchain network and provide a valuable service.

As far as the blockchain is concerned, it is in its infancy. There is a long way to go before you start to see the real power of the blockchain, but if the start is any indication, it will be safe to say that the short-term benefits of using the blockchain in a lot of other distributed technologies would be extremely beneficial.

Cryptocurrency has got a bad rap from those who do not understand it and those who are threatened by it – be that threat real or perceived. They like to throw Bitcoin and the blockchain into the category of criminal activity. I don't buy that for one second. Privacy is the bedrock of our democracy, but that privacy has been eroded slowly in the name of security and where has that got us? Events like that of advanced psychographic manipulation on social media, and even large scale monitoring by the powers that be.

The blockchain has become the core of a number of diverse technologies; even companies such as IBM have started to dive into it in a big way. Cloud storage companies are looking at blockchain technologies to be able to perfect distributed storage that is virtually impossible to destroy or hack.

Take, for instance, a company that is combining the utility of distributed file storage and the versatility of cryptocurrency and creating a token out of it. I am only bringing that up here because I want to show you how diverse blockchains can be.

The way this works is that the blockchain is created by nodes in the system and all the nodes in the system contribute a percentage of their hard drive to the network. In turn, what they do is

store some of their contents on the network that is kept track of by a blockchain. The blockchain charges those who store data and then takes that data, encrypts it, and breaks it up into small fragments and scatters it across the network. When a user wants to retrieve it, he just has to enter his private key and he gets access to all his data that is brought back to him using BitTorrent technology for downloads.

Those who want to use this service purchase a cryptocurrency or token (like Bitcoin) and then pay that token on a periodic basis for the service to store the data. The person providing the hard-drive space gets a portion of income each time his drive space is used. The person using it automatically depletes his coin reserve as it goes to the administrator of the blockchain and the nodes that are storing the data.

The income for the nodes is almost automatic and on autopilot. They just need to keep their computer on and, as time goes by, the coin that is paid for the storage accumulates over time.

The point of this example is two-fold. The first, to exhibit the flexibility and nature of blockchains, and the second, to introduce the next wave of distributed apps that will be built on blockchains and parallel the token and coin market.

The larger the coin and token market expand, the more that results in the advance of Bitcoin. It somehow seems that the entry point for a number of the cryptocurrencies is the Bitcoin; and the exchange for these tokens and coins has become quite vibrant, and do not show any signs of slowing down.

Your interest in the blockchain and the coin above it, is one probably driven by smart intuition and should be promoted. You should advance your interest in this because it is the start of a new paradigm in commerce and finance.

There are a few other areas that you should look into if you want to take this business seriously. There are issues in cryptocurrency mining that you may want to advance. There is a huge industry out there that is in its nascent stages. On the other hand, if you are more the trading type

and are not to savvy with the technical aspects of things, then maybe cryptocurrency trading could be something that you could get into. Bitcoin trading has tremendous potential because it is a volatile market and program traders love to trade with volatile markets because there are profits to be made in either direction and there is a large amount of arbitrage opportunity as well.

If mining and trading is not your thing, but you are in other areas of technology, you can also think of the ICO option ICOs are Initial Coin Offerings and they are ways to raise capital by issuing crypto-assets.

There are numerous areas that you can get into to take up the opportunity that is present in this vast, new field of cryptocurrencies. You did the absolute right thing by starting with this book to get an idea of the blockchain technology that sits under the crypto-asset that rides on top.

Blockchains will revolutionize the Internet and change the face of it. The signs are already afoot, and what remains are the passage of time and the flow of ideas. The larger institutional edifices are starting to crumble in the face of the blockchain technology and the implementation of it will be nothing short of revolutionary. The movement from centralized architectures to decentralized ones will be in full force within the end of this century, and it will form the backbone of the internet of things. It will also serve as the preferred route of deployment for Artificial Intelligence and, together, AI, blockchains and the Internet of Things will be the way of the future. Welcome to a new world.

About The Author

Martin Quest is an investor in the world of Bitcoin and cryptocurrency. Making every rookie mistake imaginable, he wants to help you mitigate some of the initial pitfalls of this brand-new world.

Disclaimer

"The content within The Crypto Mining Mindset: A Beginner's Guide to Cryptocurrency Mining is intended to be used for informational purposes only. The ideas and strategies contained within this book and of the author should not be copied, amended or reused for financial or personal gains, or without a financial expert's advice."

Thank you for buying this book. I hope that through it, I have helped you learn much about the Art of HODLing, the how to mine cryptos effectively, understand the world of the ICO, create effective crypto trading strategies, and recognize the importance of the blockchain. I wish you all the best in all your efforts and investments. Cheers!

Bonus!

Wouldn't it be nice to know when Amazon's top Kindle books go on Free Promotion? Want more insider info with Crypto?

CLICK HERE FOR INSTANT ACCESS!

Simply as a "Thank you" for choosing this book, I would like to give you access to an exclusive service that will email you notifications when Amazon's Top Kindle Books go on free promotion, as well as offer you an INSIDER GUIDE to more crypto strategies. If you're someone looking to go to the next level in your crypto success, simply click the link above for FREE access!