Bitcoin: Untitled

△△

by G. R. Secco
ramiro@duck.com
ramirosecco.com

0. Abstract

Initially, this was a personal project with the aim of understanding in detail how Bitcoin, that new system destined to revolutionise the digital industry, works. I was surprised to find that there seemed to be certain aspects to which the answers were incomplete, to say the least. My first instinct was to blame my own ignorance. Gradually, I added new concepts to my toolbox to better interpret those ideas that were eluding me. I studied material from conferences, expert panels and listened to all the gurus revered by the industry. However, I felt that I understood less and less. What puzzled me most about Bitcoin was that it seemed to be in a permanent process of repair.

This is how I got into what seemed like a fictional novel. A story of betrayal and lies that obscured a world that boasted of offering a new paradigm in the way it worked.

Finally, a new way of understanding Bitcoin presented itself to me, and at last, all doubts began to disappear. Along the way, I realised that nothing had truly been misunderstood. Neither had I misinterpreted nor were those original explanations simply mistakes. It could not be a coincidence that thirteen years after the launch of Bitcoin, its very code was literally and figuratively manipulated to represent something that it had not been, was not, and would never be.

The information presented here is more than an academic paper, it is a moral duty, and it is addressed to those willing to listen. Never were the words of a wise old man truer: "*Ignorance is not a right, but an abuse*".

1. Introduction

In 2008, then financial adviser Bernie Madoff admitted to the authorities to running the biggest stock market scam in history. His strategy was simple: pay the agreed-upon dividends using the money from new investors. This fraudulent system is known as a Ponzi scheme. The art of this fraud lies in finding the balance between new investors and dividends paid to existing investors.

In this case, the truth only came out when the 2008 financial crisis erupted, and too many of its investors wanted to withdraw their capital to cover other obligations. If there had been no crisis, it is very likely that Madoff's name would still be associated with honour and prestige today, as it was then.

The truth is that Madoff was reported on multiple occasions. Mathematically, it was impossible to produce his results in the stock markets. The evidence was irrefutable. It is a fascinating case because he defrauded the world's wealthiest people. There was plenty of interest in uncovering possible fraud.

In scams, the common factor is the abuse of trust. Big lies are built brick by brick and necessarily rely on the unwitting complicity of the deceived. The key to Ponzi schemes is balance. Finding the next rung of victims to spread the lie.

It is also essential to distribute internal processes as much as possible. In this way, the information of the operation is blurred between the parties. Each party thinks that the other party has the information they lack. It is part of the handbook of cults, where their leader is the only person with all the necessary knowledge. In this way, they magnify their aura of omniscience while undermining their followers.

Such distributions of power and information can only explain the inability to disclose crime at this level. People are proud of their achievements and ashamed of their shortcomings. The same reflex that prevents us from raising our hand in class to admit that we have a question is present as adults in fulfilling our tasks. Even when we hold a position that involves detecting and investigating, we prefer to avoid any scenario that might expose our shortcomings. This becomes even more evident when we are confronted with an authority figure, be it a spiritual guru or the leader of a corporation. In many cases, we even find both roles in the same people.

In the technology and innovation ecosystem, the universe of those privileged to master an area is often very limited. It requires mastery of particular branches of science within mathematics, physics and electronics, to name a few. Sustaining fraud over time in these areas is virtually impossible. The best way to do this is to dominate the discourse from the outset when the universe of potential perpetrators is almost total. Bitcoin is unique. It is one of the most significant technological developments since the creation of the Internet. Its inventor, the only person with the actual capacity to understand its mechanisms and the true possibilities of this tool, has been banished and vilified by the industry.

Bitcoin has been taken hostage. The cryptocurrency ecosystem is equal parts accomplice and victim. The main losers will always be small investors lured by false prophets. The real culprits will be those of us who abuse our ignorance.

2. The Digital Universe

The world has been in the process of digitalisation of human activities since the birth of the first computers. This way of interacting with our environment and third parties was made possible by a new language enabled after the invention of microprocessors fifty years ago.

2.1 1970: Data Transmission

To understand Bitcoin, it is first necessary to understand how information is transmitted in a network.

In any electronic communication system, information travels through electrical pulses of 0's and 1's. A form of Morse code called binary code. For this communication to be possible, a series of protocols and rules prepare the message for transmission. Headings and descriptions are added, always in binary code. In this way, the various actors in the system can interpret what to do with the message at each stage of delivery. It is then broken down into small packets that are sent individually, and finally, the message is reassembled once it arrives at its destination.

An example of a communication system that we all use is email. Its mechanism is identical to traditional mail but in a digital version. We write down both addresses and put it in a post box to send a parcel. The addressee goes to the post office and, showing their credentials, receives it. Instead of a physical office, in email we use a virtual office: the servers of our email provider. These are nothing more than computers connected to the Internet. We enter two keys to access our email account, one public and one private. This is how we access our mailbox hosted on these servers. The public key is your EmailName@mail.com, while the private key is your password.

Both the traditional mail system and the electronic mail system have their own protocols to ensure that messages reach their destination. Internal mechanisms ensure that all packages are correctly sent and received. These can take the form of barcodes, tickets, among others. The specifics of these processes are unknown to users. We are only interested in getting the message across quickly and safely.

2.2 1990: Internet and the Digital Revolution

In early computers, sharing information between computers was through external disks. The most popular and practical were those whose physical form gave rise to the icon that still universally stands for 'save'. Connecting several computers via cables was also possible, forming a closed 'network'. The Internet is the system that made it possible to connect computers via the telephone line already installed in every home and office in the world. After all, they were simply ordered electrical pulses travelling along wires.

The 1990s saw the birth of the World Wide Web (better known by its acronym "www" or simply "the Web"), an electronic communication protocol that simplified the use of the Internet to such an extent that we still use the same system today. Browsers such as Google Chrome or Mozilla Firefox allow us to use this Web protocol in an orderly fashion. This new way of sharing information, coupled with Microsoft's launch of Windows 95, led to the first major technological revolution. It meant a fundamental change in the way we interact and share ideas. It was a crucial component in accelerating the process of globalisation, breaking down physical borders and fostering a new way of linking us.

Email quickly gained ground as an alternative to postal mail. Search engines soon replaced encyclopaedias and yellow pages. Until then, the world's large companies were producers of physical goods or services. The Internet was a bridge between the tangible and the digital world. There was no doubt about its potential, but it remained to be understood what kind of companies would lead this new revolution. This scenario gave rise to a speculative bubble in the stock markets linked to this type of company known as a dot-com company.

The problem around these tech start-ups was simple: the vast majority did not make money. They sold neither goods nor services but instead represented pure potential. This did not stop the steady flow of money from investors. This increase in demand for shares in such companies had the automatic effect of appreciating their value. Companies multiplied in value solely based on the furore of these investors, who did not want to miss out on the opportunity to have a stake in the companies of the future. These generalised upward movements in equities translated into gains for all. Of course, this only attracted more money and more investors. This further boosted the share price, generating more profits and more investment. This phenomenon, where shares increase in value simply because of confidence that they will continue to grow, is known as a speculative bubble. This dynamic lasted as long as it could. Stock prices must be based on a company's true power to create value, earnings being the most straightforward indicator. In 2000, reality knocked on the door, and stocks experienced a widespread crash. Bubbles can take months or years to be created, but only days to evaporate. The world will remember - and forget - this episode as the dot-com bubble.

In the same year, Napster appeared, a programme that allowed users to share music files for free, unlimited and, of course, illegally. Digital piracy was born. The novel system used for file sharing is known as 'Peer-To-Peer' or 'P2P'. This system establishes a direct connection between the computers of two strangers to share programmes, documents or music. There was no legal way to buy a single song; you had to buy complete albums. In the absence of a service provider acting as an intermediary, there was no practical way to stop this flow of files. It was a scandal. It revolutionised an industry where until then, most of the profits were made from record sales.

While the music industry poured its resources and energies into declaring war on piracy, some took a different view. This person understood that users have no interest in stealing music. On the contrary, they prefer to pay, but only for those songs they are interested in; and do so in a practical and safe way. In 2001, Steve Jobs, founder of Apple, introduced iTunes, which made it possible to download music legally and securely. It changed the music industry forever. Industries adapt or disappear.

2.3 2000: Web 2.0, The Dynamic Internet

The development of the Internet ecosystem and the new forms of interaction between its users gave rise to what is known as Web 2.0. It is the network we know today. It is no longer just about access; it is now possible to create, share and interact across platforms. Smartphones put a computer in everyone's hand.

It is the age of apps. Uber, the transport app that connects drivers and users, was born. Spotify, which takes over from Apple, offers unlimited music access for a fixed price. Netflix had done the same a few years earlier with its catalogue of series and films. This way of making money is known as 'Software as a Service', 100% digital services. Username, password and credit card.

It is also the era of social networking that displaces email as a form of digital social interaction. Facebook, Twitter and Instagram are exploding. YouTube ends the monopoly of TV channels on content creation.

Facebook, a pioneer in the massive expansion of the social networking concept, and Google, the default search engine of the last twenty years, solved the dot-com problem. Like them, they lost money for years. In fact, since they did not charge for their use, they had virtually no income.

The solution they found was to become advertising companies. By collecting information about our habits and preferences, they offered an affordable online advertising service. What had previously been a luxury reserved exclusively for large companies was now available to the world's SMEs. Thus, the concept of 'Consumer as a Service' was born. Nothing is free in life, and the Internet is no exception. If you are not paying for the product, you are the product.

2.4 The Digitalisation of Money

Money is information. Each country transmits this information in its local currency. Whatever the currency, there are two storage methods: physical and digital. Both are interchangeable with each other. When we withdraw money from an ATM, we are converting digital money into physical money.

Physical money requires physical protection and is therefore stored in vaults or safes. In contrast, the digital cash register is kept on computers. Its storage requires special protection to ensure the integrity of the records. Special permissions for access and modification must be established.

The digitisation of money brought the advantage of no longer relying on paper records to store customer information. The massification of the Internet introduced the possibility for banks to offer online access. This meant visualising the availability of funds and conducting transactions from the comfort of one's own home. On the flip side, this ease of access translates into increased risk. Protecting a computer without access to the Internet is not the same as protecting a computer that is open to interactions with the outside world. The more access points, the more vulnerabilities a system has.

Another difficulty of the online banking system is to ensure that transactions are correctly updated in real-time. The most common risk to avoid is that a user tries to make the same transaction twice before recognising double-spending. To do this, the movements must be processed chronologically. While this may sound simple enough, this is a big challenge in computing.

Let's say that from the same account, you are trying to make the same transfer at the same time but from two computers located on opposite sides of the world. The information must travel through the world's wires to reach the bank's nearest servers. They, in turn, must collate all incoming transactions with each other, sort them and execute them all at the same time. It is not a simple task, especially considering the millions of transactions received per second and the ever-present risk of illegitimate access. For these reasons, we use trusted third party agents, such as banks or credit cards, to take care of our electronic money. They set up automatic controls to avoid such situations but must permanently monitor the system. Based on strict and robust IT security systems, such controls are also not free from cyber-attacks.

Complexity in IT security has become a significant distraction and, therefore, a diversion of resources, compromising the efficiency of the core work of the banking system.

2.5 The Financial System

In the banking system, we use accounts to keep track of the balance of money available to each person. With each transaction, the balance increases or decreases. In Bitcoin, on the other hand, each coin has a record of ownership. It would be as if banks had a record of each banknote, with its serial number and the chain of possession since the banknote entered the system.

It may also be helpful to imagine that each bitcoin is a cheque for a value of '1'. To transfer it, the last beneficiary must sign the back (endorsement) and include the new holder's identity.

We must remember that the current financial system must:

a) Confirm funds.
b) Confirming identity.
c) Ensure the integrity of the system.

Given the complexity, each movement of money implies a higher maintenance cost. The higher the volume of transactions, the more sensitive the system is and the more secure it must be at the same time. It is also important to remember that the very spirit of the banks' business is to use part of the deposited funds to make loans - charging interest on the loans - and to make investments with the money.

3. Bitcoin, The Cash Substitute

Bitcoin is a new computer-based instrument that allows the transmission of value in digital form.

The original Bitcoin document or 'White Paper' is entitled: *Bitcoin: A Peer-To-Peer Cash System* [1]. That is a peer-to-peer *cash* transfer system.

It is a new kind of money. A hybrid between e-money and cash. It was conceived to fulfil the function of physical money, but instead of using banknotes, virtual currencies are exchanged. These virtual currencies will be referred to as lowercase *bitcoins* to differentiate them from the capital *Bitcoin* system.

The system is based on a public register where all movements are entered chronologically. The programme operates under a new information storage and distribution system called *Blockchain*. Its maintenance is carried out by a group of people known as *miners*.

These terms and how they work will be explained in later chapters.

To understand what Bitcoin is and how it can change how we interact with money, it is essential to forget everything we think we know or understand about it. Most of the concepts and explanations presented in this document contradict information available on virtually all accessible sites.

3.1 Bitcoin, The Origin

The original White Paper describing the goal and the technology applied to achieve it was published on 31 October 2008. The document bears the signature of Satoshi Nakamoto, a pseudonym chosen by its actual author, who preferred to remain anonymous.

Bitcoin software was launched in January 2009. Satoshi remained an active figure. He interacted online with those who showed interest in the system. In the beginning, it was not too different from any school project. It was most likely going to be an interesting experiment but would fail. After all, he was trying to solve a problem that computer specialists had been trying to solve for more than twenty years. He made adjustments and corrected minor bugs and weaknesses identified in the software. Satoshi, always anonymous, added some of these people as collaborators in the process.

Inevitably, Bitcoin soon attracted users who saw it as an ideal opportunity for illicit activities. This is not a good idea since all movements are permanently recorded in a public register, as we will see below. In addition, identity is eventually required to convert digital currencies into dollars. In 2011, Silk Road [2-3], a marketplace for drugs and other illegal products, was born, using Bitcoin as a payment currency among users. It was then that virtual currency began to gain popularity, and its use spread beyond the small circle of people who knew about the system.

With the number of active users exchanging bitcoins on the rise, so did the exchange rate. Early adopters who had saved coins greeted this with joy and enthusiasm. For his part, Satoshi was wary of this, noting that it could risk attracting an unwanted audience and at the same time gaining bad press. Even in 2010, when Julian Assange's Wikileaks stated that they were considering accepting donations in the virtual currency, Satoshi publicly asked them not to do so as it could destroy the system [4].

Such was his concern that in December 2010, he withdrew from discussion forums and began to delegate the project. In his last act, he grants software licences to Gavin Andresen, an early collaborator.

3.2 Post-Satoshi Bitcoin

The aim was for Bitcoin to fulfil its ultimate goal of being digital cash. To do so, it had to process hundreds of thousands of transactions per minute. The difficulty was that, as their use increased, a considerable number of transactions accumulated together.

In this instance, we need to understand how Bitcoin works because transactions are grouped and recorded in what we call '*blocks*'. Each block is nothing more than an entry in a ledger where all movements of bitcoins are recorded.

Simple intuition tells us that more transactions can be entered per block if the blocks are larger. Satoshi had momentarily limited the size of these blocks after he was warned of possible risks of cyberattacks. These risks were real in the early years when few people sustained the system. Satoshi could not have imagined that this would be at the centre of one of the most significant Bitcoin disputes, which is still raging today.

Andresen, now in charge, had good intentions but made the mistake of taking Bitcoin as a collaborative project. He gave power to more developers and even set up a voting system for miners to approve changes. This was his second mistake. As we will see below, Miners do not make decisions; their work is purely technical. They do not approve transactions; they only dispute a challenge honestly. The system is designed to undergo as few modifications as possible. A monetary transmission system could never work if the game's rules can be changed at any time.

3.3 Bitcoin: Civil War

In 2015, Andresen presented a project to the "community" to gradually increase the size of the blocks. For reasons that will become clear below, he did not have the support of most of the developers he had selected [5-8]. Opponents argued that an increase in block size would mean that the system could only be sustained by large pools of capital, which in practice would lead to a new kind of centralisation of Bitcoin. For this group, the size was kept so that anyone from a standard computer could help maintain the system. Andresen's proposal was discarded, and as of today, the limit still stands.

This same group failed to mention that many of the members had joined a private project called Blockstream.

Blockstream proposes different options to solve Bitcoin's limitations due to the block size limit. They have created technical abominations with fancy names like "Lightening Network" or "Liquid". Broadly speaking, their plan is to create a parallel blockchain that bundles and reconciles many transactions but managed and maintained by Blockstream. The commissions would then go to this company instead of going through the "official" intermediaries, the miners. In point 5, we will explain in detail the actual functioning of Bitcoin, and this will become clearer.

Blockstream is one of those technological projects with ambiguous missions and objectives, but which was created to offer systems that facilitate and improve the functioning of Bitcoin. The problem is that this was precisely the task that Bitcoin developers were supposed to be carrying out. This point is key to understanding what is happening in the ecosystem today.

The same individuals in charge of implementing improvements to the system, the same ones who had decided that Bitcoin was a 'community' project, founded a company - for profit - with the same objectives they claimed to be selflessly pursuing. The same group is still trying and failing seven years later. The same group that in 2016 made a change to the original rules they claimed to respect [9]. If centralisation of the system was to be avoided, creating a corporation to broker transactions sounds inconsistent, to say the least.

These people controlled the proposals to be considered, all aspects of Bitcoin communication, and even censored conversations on public forums such as Reddit. Also, consider that its investors include Twitter CEO Jack Dorsey and various personalities and groups related to the financial world. I do not intend to point out that this is a strategy pursued by banks or credit cards to take or keep control of the world of finance. Part of the strategy followed by significant funds is to invest in technology companies that can be profitable. Blockstream is one of the thousands of companies these groups have invested in.

The real corruption lies with the developers of Bitcoin (technically, we are now talking about a deformation of Bitcoin called *BTC*). Both those who are part of Blockstream and those who are not and do not denounce this reality are defrauding the public. In no other organisation would such a blatant conflict of interest be permitted. If they work as developers of an open and public service, they cannot at the same time work for a company whose sole reason for existence is its inability to perform its functions in the first place. This is without getting into the real substantive discussion about who hired them and whose authority. It is also necessary to point out the deceitfulness of personalities such as Jack Dorsey, a solid and vocal promoter of BTC from his position of power, though not so vocal in expressing his potential conflict of interest.

It should be made clear that all this information has been public knowledge for years. The details of investments are not always very transparent, but this is normal when companies are still private. What is striking is how little impact these events have. This is primarily due to a lack of understanding of the whole world of cryptocurrencies. Part of the aim of this paper is to present an accurate picture of the different elements that comprise it.

Finally, it is essential to note that none of these people invented Bitcoin. Nor were they central to its development. The entire functioning of the system explained in this document is derived from the original White Paper written by Satoshi Nakamoto.

3.4 Separation

As we will explain below, a blockchain system like Bitcoin is maintained by miners who keep track of the blocks with the transactions. To do this, miners download a programme that connects to the registry. If a sufficient number of miners maintain the system, the blockchain is operational. In this document, we have focused on the original chain that is Bitcoin, but there can be several chains, each with its own rules.

There is also a phenomenon known as '*Fork'*, where the same chain splits in two. It would be like a fork in the road, where one group starts following one set of rules and the other another. Up to that point, the past is precisely the same; what changes are the rules from that point onwards. A hypothetical parallel would be to imagine that the US splits into two countries and each country keeps the dollar as its currency, but from the date of the split, each country manages its issuance and reserves under its own rules. The result would be two currencies that continue to function but independently of each other, each with its own exchange rate.

Following a significant rule change implemented in 2016 (known as '*SegWit'*, which was, in fact, a type of '*Fork*'), a dissenting group made one such fork. Bitcoin was thus split in two: Bitcoin Core (BTC) and Bitcoin Cash (BCH).

Bitcoin Core, or BTC from now on, is the most widely known Bitcoin. It is the one whose exchange is repeated in the media, and the whole community considers it as 'the' Bitcoin. Misnamed the 'original', it is the same one taken hostage by a group of developers. Bitcoin Cash, meanwhile, forked again, and one of its offshoots is the Bitcoin Satoshi Vision blockchain. The latter, dubbed BSV, seeks to follow the true spirit of Bitcoin as a cheap and efficient exchange instrument. It has another peculiarity that makes it one of the least known and respected currencies on the market: the man behind it is Satoshi Nakamoto himself.

3.5 Satoshi Nakamoto

Anyone with a modicum of knowledge of the world of cryptocurrencies will tell you that his true identity is a mystery; no one knows, and probably no one ever will. You would get the same answer after consulting any specialised media, formal or informal. They are wrong. His real name is Craig S. Wright, an Australian citizen with an extensive background in cybersecurity, auditing and finance. His academic record includes at least two doctorates, some 20 professional degrees, and dozens of certificates. All of them can be consulted on his website [10].

The magazines *Wired* and *Gizmodo* revealed his identity in 2015 [11-12] after receiving anonymous information. Wright admitted to being the mastermind behind Bitcoin but not conforming to the imaginary constructed ideal, so the "community" rejected him. That's right, the same community that modified the original protocol and for years failed to make Bitcoin a practical tool for the exchange of value determined that this person was an impostor. Investors, formal and informal media and "experts" from all over the world agreed with them. It was 2015, and the universe of stakeholders was noticeably small. Seven years later, both influential media outlets and significant investment funds continue to deny his identity.

One reason for claiming that Craig Wright is not Satoshi is that he refuses to use the key associated with Satoshi's accounts for a public demonstration. On the one hand, this is not entirely true, as he did so privately to people like Gavin Andresen and at least one BBC journalist. But the most important thing Wright wants to show is that possession of keys does not necessarily translate into ownership. In the same way that having the keys to a house does not automatically make one its owner. Absolute and irrefutable proof cannot rest on access. Bitcoin does not guarantee ownership and is not a substitute for the actual laws created by the authorities in each country. Bitcoin represents a registry, nothing more. I understand that this may be a convenient position for a hypothetical impostor. Still, one only has to read and listen to Craig Wright enough to come to the unequivocal conclusion that he is the creator of the system. Even before his identity was revealed, Craig appeared at conferences showing a mastery of the system that cannot be matched to this day.

It is also worth noting that Craig Wright does not owe the community, or anyone, an explanation. He did not ask to be recognised as the creator of Bitcoin but was forced to accept it. Bitcoin is a system that should work regardless of who created it. It is a tool for the world.

Unfortunately, the current powerful interests have forced a media circus full of inconsistencies. It is not just a matter of bad intentions; there is a mafia-like apparatus in place committing crimes with impunity.

To understand Craig Wright's dislike of the crypto world, it is vital to understand the depth of the false narrative that has been fabricated around Bitcoin, its history, and its potential.

4. Bitcoin, Digital Cash

The main practical benefit of Bitcoin is the possibility of making micro-payments over the Internet. It's something that sounds simple and low impact, but it has the potential to revolutionise the way we interact with the digital world.

Today the only way to make payments online is through bank transactions or credit cards. The US's average fee paid per transaction to credit cards in 2021 is 2% [13-14]. This figure may represent the profit margin of many companies. At the economic level, such cost savings would significantly affect small and medium-sized enterprises, helping in particular to boost emerging economies.

Take for example a search engine like Google. As we have already explained, its revenues depend on advertising and data mining as it is free. With Bitcoin, Google could charge users pennies on the dollar for each search. Today this is economically unfeasible due to the minimal transaction costs of any credit card. Similar would be the case with YouTube, which could charge minuscule amounts for each playback.

Such a system can also mean the end of spam. Introducing an economic barrier to bulk mailing would no longer be so attractive to fill entire mailboxes with junk content.

Traditional trade can also benefit from a secure and practical tool to buy and sell more fluidly and with lower associated costs that do not add value today.

On an international scale, it can serve as an impetus, especially in providing services abroad, considerably reducing costs and frictions that today limit the development of many economies.

To conceive of these cases, it is a good idea to understand what we are talking about when we talk about Bitcoin and how its virtual currencies operate.

4.1 Conversion to Money and Exchange Rate

Bitcoins are stored in electronic wallets. It is not important how they work. Just imagine them as a mobile phone application that keeps track of our virtual currencies. As it is an open system, any developer can create these applications and users can choose the one that suits them best.

All bitcoins in circulation come from rewards previously earned by the miners who maintain the system. In the beginning, with almost no transactions or competition between miners, mining could be done with any computer. As the currency gained traction, more investment was required to perform this task, and therefore miners needed to sell their bitcoins to pay bills and other associated expenses.

This is how the first exchanges came about. In the beginning, they were informal places where there was no real exchange rate. As the market grew and businesses developed around it, the system took on a certain formality. The reality is that one exchange should work like any other. They are fiduciary agents that intermediate an exchange of value. In a properly regulated scenario, they will have to register the identity of users for specific operations and execute transactions following the law that regulates them.

In the short term, Bitcoin is an ideal tool for making small payments. Prices will not be set in Bitcoin but in local currencies, and based on the current exchange rate, conversion and payment will be made in bitcoins. In the case of Google, it could set its prices in dollars and charge the equivalent in bitcoins. Similarly, a trader anywhere in the world can sell his products in his local currency and get paid in virtual currency.

In general, the prices of goods result from a chain of aggregating costs. To measure and determine these costs, the best measure we have is the currencies of each country.

It does not matter what the bitcoin price is. It matters that it fulfils the function of transmitting information.

It is not sensible to think that someone today will store the equivalent of the value of a house in bitcoins in their mobile phone, at least in the medium term—much less attempt to make a purchase of that nature in this way. Today we can access our bank accounts from any computer, but only to give orders to the entity that holds our money.

4.2 Risks

The security of any system depends on the level of assurance required. Therefore, if digital cash is involved, security should be higher or equal to traditional cash.

We will explain later the system that makes Bitcoin extremely secure when it comes to guaranteeing the fidelity of the information displayed.

As mentioned above, bitcoins are stored in electronic wallets. These are nothing more than computer programs that integrate seamlessly into the Bitcoin system. They may be private, but that does not mean anonymous. Like a bank account, identification and registration may be required. The difference is that legal registers can be established where only certain information can be accessed with specific permissions. This is possible today, but the difference is the transparency offered by the Bitcoin system. Each permitted access would generate a public record, ensuring more significant safeguards for the parties.

4.3 Are Transactions Reversible?

In a fraud case, a judge may order that a transaction be returned. Transactions cannot be deleted or manipulated, but they can be reversed. The important thing is that everything that happened is recorded. Specific special permits could be used to enforce the judge's order and would serve to enforce such orders. Of course, this would not be practical for any amount, given the complexity that such a judicial process and its subsequent enforcement would require.

4.4 Will Bitcoin Replace Banks?

No. While it is true that it could be used as an alternative to some banking services, this is not the same as saying that it can replace the function performed by banks. It is unreasonable to imagine a world where we have hundreds of thousands of dollars in a computer in our home.

Moreover, this is a failure to understand the dynamics of the economy and the role of the financial system in the economy's health. That the current system is perverted in many of its original functions does not mean that dismantling it is wise, let alone feasible.

Financial intermediaries also play a crucial role in preventing money laundering. To do this, they must follow the provisions known as KYC (know your customer) and AML (anti-money laundering). This cannot be fully automated, but instead, responsibilities must be assigned. There are regulations at the country level on specific controls and procedures to be followed in executing these processes.

Bitcoin is a reinforcement of the whole system. Banks can become banks again. Know their customers. Attracting the funds of those with the capacity to save and offering loans, and investing in projects that create value.

4.5 Can Other Information Be Transmitted?

Yes, Bitcoin is a computer program. At its lowest level of complexity, it moves digital currencies. These digital currencies may represent other assets or other forms of information. Entire programs can also be written that use the information transfer system to perform their functions.

5. Blockchain: The Technology

In accounting, movements are recorded in what is known as Accounting Ledgers. The main one is the General Ledger. It records economic events in chronological order. Unlike a simple cash register, which records receipts and disbursements, ledgers also record assets, rights and obligations. This correctly ordered and displayed information is used by companies to measure their economic health and its evolution over time.

A particularity of the accounting system is that it is not possible to edit records once they have been entered. If, for example, a sale is recorded in error, correcting it means recording the same transaction but in reverse. This step is known as "reverse entry". To ensure compliance with this rule, accounting standards mandate that a value from the previous sheet must be entered on each sheet. In this way, all sheets are connected. Attempting to change a single number would mean that all subsequent sheets would have to be changed.

Bitcoin is inspired by the General Ledger and introduces a similar record in a digital and public format. This system is called *Blockchain*. Instead of pages, we use blocks. The rest is the same principle. Blocks are recorded in a row, one after the other, chained by a value associated with the previous block. Any attempt at tampering automatically breaks the chain link.

To simplify understanding, we can imagine that each block is a new transaction, so the blockchain is a chain where each added link corresponds to a movement of coins. In reality, each block can contain any number of transactions together, as long as they are valid.

5.1 Identity and Public/Private Keys

One of the strengths of the system is that all transactions are public. Anyone can see the movements, but not the identity of the people. The General Ledger, with all movements, is available to any interested party. This not only ensures transparency but also makes any attempt to destroy it impossible.

In the traditional banking system, accounts are used, and information is transferred in encrypted form so that only those with access can decrypt its contents. In Bitcoin, transactions are public, and information is not encrypted. For this reason, an alternative system must be used to validate the identity of the parties, protect their privacy and at the same time provide security guarantees.

This is where cryptography comes into play. Instead of an account number, a code called a *public key* is used. To receive bitcoins, it is enough to share the public key. An excellent way to imagine this system is to think of these keys as slots to deposit envelopes with values. An essential aspect of this system is that an infinite number of such slots or public keys are available with one particular feature: they are all opened with the same key, the *private key*. We can imagine this as a physical master key that allows us to open each of our safe deposit boxes. This is why we say that public keys are derived from the private key.

In section 2.5, we said that the way bitcoins are shared could be compared to the cheque endorsement system. This is because that is effectively what the private key does. In practice, it functions as a digital signature. Cryptography only confirms that the 'signature' is correct. It verifies that the private key is the one associated with the public key that was used to deposit the funds. When we use our virtual currencies, we forward the values to other safe deposit boxes.

This complex key mechanism should not be understood by any user. The fundamental idea is not that we know our keys or risk entering a wrong digit and losing our money. It is designed to work automatically with e-wallets produced by private developers. They create a codename, such as @Craig_22, and our signature is a password. We, as users, should only care about getting transactions done.

In this instance, it is essential to note that the use of public keys does not mean that it is impossible to establish identity registers. In particular, e-wallets can be created to establish identity controls, irrespective of the keys used. Bitcoin allows that the @Craig_22 account is associated with a registered individual and can transfer funds to the @Amazon account, which is also registered. Amazon does not need to know the user's gender, age, marital status, or other personal information. It would also not have to report transactions above specific amounts, as this information could be automatically shared with the authorities. You can comply with all legal requirements and at the same time have a deserved level of privacy.

It remains to be explained how to resolve the chronological order of the transactions. For this purpose, a "game" is implemented in which people compete for a prize. This competition is called '*Proof of Work*', and those who participate in it are known as '*miners*' or '*nodes*'.

5.2 Proof of Work, the Support

Bitcoin is, after all, a computer program. Like any programme, it has a set of rules or protocols. In the absence of a formal organisation behind it, the protocol includes a system of incentives set up as a form of 'reward' for those who keep it running. To win a prize, all you have to do is add a block to the system. The catch is that there can only be one winner per block. This is because, as we said before, blocks have to be aggregated one after the other to ensure orderly transactions and avoid fraud.

Those who participate by adding blocks and collecting rewards are known as *miners*. Any individual or group of people can be a miner. They have to download a computer program that proposes a competition between them to do so. It is this competition or gaming that enables the maintenance of the system.

5.3 The Game

The miners are the ones who keep the system running. To do so, they need computers and an Internet connection. Their task is to compete in a game that solves puzzles to win bitcoins as a reward.

To understand the competition, it is easier to imagine a manual process where only a telephone, pencil and paper are available.

In this hypothetical case, we work for the office in charge of recording transactions. Our task is to be alert on the phone where transactions are received. When we receive one, we write it down on a piece of paper.

Firstly, it must meet two formal requirements:

1- Contains the value of the previous block. ✓

2- The correct private key correctly validated the transaction. ✓

Once these requirements have been met, we take the paper to the Registry for registration. The official in charge then tears the paper into a thousand pieces. The game consists of reassembling the paper hash. The challenge is made particularly difficult because we must do it in absolute darkness. The only way to win is to try combinations and submit them to the Registry until you get the right one. But the challenge is even more remarkable when you consider that anyone can carry a sheet of paper and play simultaneously.

It should be noted that each miner may be trying to process different transactions, so the puzzles may differ from one another.

The first to solve their puzzle receives confirmation from the official and wins the prize. The other players must run to find a new paper containing the new value of the now last block and start again.

The game is known as *proof of work*. The objective of this is to confirm, as the name implies, that the miner has invested time and resources in solving the puzzle. The actual process is similar but uses computers instead of physical papers. These computers do not solve equations or complex mathematical problems. They simply play a number guessing game. It is this arbitrariness that makes it impossible for a miner to cheat. To increase the chances of winning, more computers are needed to try more numbers. There is no referee or judge other than the rules themselves, which oblige the players to play fair.

5.4 The Rules

Each miner keeps their own copy of the General Ledger (hereinafter referred to as the "Ledger").

To become an official miner and earn the right to write blocks in the Ledger, we must first agree to receive and transmit transactions. In other words, miners must be in constant communication with each other and the rest of the world. It is in their interest to do so anyway; otherwise, they cannot be updated on the latest block and upcoming incoming transactions. In addition, each miner wants to publish his solved puzzles before the others, so it is in his interest to maximise communication with each other. In the above example, we would have to be on the phone all the time, calling other miners sharing both the transactions received and the puzzles solved. This requires a strong Internet connection to maximise the efficiency of this task. This is another implicit strength within the system. A miner cannot hide in the middle of a rainforest to do his job.

The next obligation is to accept and add to your copy of the correct blocks. It is not acceptable to reject puzzles that meet the requirements.

The last rule is that the Ledger with the most blocks is taken as valid. If a miner wants to cheat and ignore the transactions of his colleagues, nobody cares because his Ledger is no longer a reference for others. It can indeed happen that two miners receive two different blocks and, in good faith, enter the one they believe to be correct in their records. The rules then state that the game continues to be played, each with their own Ledger. We said that the rule states that the Ledger with the most blocks is valid. In this way, after a short time of continuing to play, the system itself decides in favour of the Ledger that more miners continued.

At the genesis of Bitcoin, 21 million bitcoins were created for distribution to miners. All bitcoins in circulation today are the fruit of rewards received by miners. Being a miner implies accepting the game's rules, so legally it can be considered a unilateral contract. An excellent example to understand this type of contract is a newspaper advertisement offering a reward in exchange for finding a lost pet. Anyone can accept the contract and, if the animal is found, they are entitled to collect the reward offered.

5.5 Traps

As explained above, the miners use computers for the puzzles. Computers have no way to solve the problem logically or intelligently. The only way to maximise the chances of winning is to use more computers, which only test more answers.

It is important to note that more computers are being used, not better ones. For this reason, miners today form what are called *farms*. These farms are nothing more than sheds full of computers testing solutions all day long. This translates into hundreds of thousands of dollars in equipment, electrical power and personnel.

Attempting to force bogus transactions is impossible for two reasons. Firstly, they must have the digital signature that does the cryptographic validation. Secondly, we need to think about the implicit economics of the system. A malicious miner, who enters an inappropriate block, should win in absolutely all of the puzzles presented consistently to continue to have the most blocks. This is statistically impossible and would also violate the rules of the game. This means breaking a contract and doing so in full view of the world. Let us remember that to keep a Ledger, its results must be constantly transmitted. Imagine a giant shed full of computers transmitting data across the universe. It would be very easy to identify, exclude and subsequently take legal action against their owners. It does not seem like a good strategy considering the amount of money invested in such facilities.

In short, the system favours playing by the rules and discourages cheating. The specialisation of miners reinforces security, forcing them to invest resources to play. The fact that the resources are no more than useless computers serves as a mechanism to reinforce security, as not being part of the game would mean throwing away all the money invested. Thus, miners are economically incentivised to comply with the rules.

5.6 Miners = Nodes

One term worth explaining is *node*. It is a repeated and manipulated concept in the crypto world and lends itself to confusion.

In computing, a node is a communication point in a network. To be a node, one must therefore receive and send information. In other words, it serves as a connector between points, hence the term node.

This definition has led to any computer connected to the Bitcoin network being considered a node. BTC even encourages all users to do so by downloading and maintaining the entire Blockchain, claiming that they play an essential role in maintaining the network.

Bitcoin does not work like that. While a person can download the software and maintain a communication channel, the miners maintain the system. As explained above, being a miner necessarily involves 'listening' and transmitting new transactions. They are financially incentivised to do so. That means they invest thousands of dollars in the best equipment in the world to receive and send information. They are the actual nodes of the system. It is unfeasible for a person with a computer to establish better communication between users than a miner. It would be like supporting a city's electricity connection using an extension cord. Even if they had the best equipment, they would repeat what they got from the miners, so they would not add any value.

Ultimately, the actual nodes of the system are the miners. BTC is trying to maintain this myth so that the authorities believe that the system cannot be stopped.

5.7 Other Cryptocurrencies

Since Bitcoin is a programme, it can be imitated. This led to the birth of other digital currencies with their respective blockchains. Broadly speaking, they are variants of

Bitcoin but with different rules. Some seek to make the information more anonymous. Others seek to be able to share information more quickly. Many of them are used to represent ownership or powers within new projects.

Most of these alternative currencies claim to solve Bitcoin's limitations. In all cases, however, they include discretion on the part of their proponents to make modifications to internal protocols. Nor are they transparent about the people who are actually in charge of these projects.

It should be made clear that Bitcoin is not technically a cryptocurrency. It uses cryptography, as do many security systems. But information travels and is presented in a transparent and readable form.

The second most popular blockchain after Bitcoin is Ethereum. It was created with the novelty of being able to execute computer programs, something it was believed Bitcoin could not do. A then-ignorant Craig Wright had denied this in 2015, later confirmed as true by the entire industry.

One of the unique features of Ethereum is that it supports the creation and distribution of other currencies by computer developers. Many of these currencies are launched as a way to finance projects. Its value is often sustained by speculation rather than its actual economic contributions in most cases.

Ethereum, in its early years, also used *Proof of Work* to keep its Blockchain running. It is now transitioning to what is known as '*Proof of Stake'*. This means that, instead of computational power, miners must leave funds in the digital currency in a sort of escrow. The system then relies on those miners with more extensive deposits. In this way, those with the most resources contribute the most blocks to the chain and therefore generate the most commissions. This system is considered more environmentally friendly as it eliminates the need to invest in computing power and energy. It only requires funds. What this alternative system promotes is an opportunity for miners to be anonymous. This can be achieved by distributing large amounts of capital to small anonymous users. Moreover, this type of system does not seek efficiency. Bitcoin miners invest money but, because of the game's competitive nature, they must also make sure they are better than others. They provide a service that serves as an indirect security mechanism. With the '*Proof of Stake'* system, money makes money just by being deposited. This is not how the economy works, and it only leads to a further concentration of wealth.

Another type of coin that has emerged is the so-called '*stablecoins*'. The spirit of such currencies is to offer a virtual currency where each unit corresponds to a real unit of money that is deposited in a bank. In other words, for every virtual dollar, there is a dollar effectively backing that value. The problem with some of these well-known currencies is that there is no de facto backing. Those who operate them are not accountable for the actual deposits, becoming de facto issuers of money without any backing. Even more seriously, they use these unbacked but theoretically backed virtual currencies to manipulate the markets for other currencies, creating the false illusion of liquidity.

6. Debunking Myths and Lies

Satoshi Nakamoto is a popular myth. He is a legend whose exploits are passed down in the crypto-universe from generation to generation. All the stories and visions of absolutely all the projects are underpinned by the vision of this wise man who chose to retire and leave his creation in the hands of the community.

Satoshi is seen as part of an 'anarcho-cybernetic' movement. He represents the rejection by the middle and lower social classes of the financial system and its closeness to the governments of the day. This rejection was significantly strengthened in the US after the 2008 financial crisis.

Bitcoin is, for many, a religion, and Satoshi, its messiah. He is presented as the answer to the evils of the modern world and unbridled capitalism. The story is so powerful that it has captured millions of people hoping to be part of a financial revolution. For these people, Bitcoin means taking back control over personal finances. 'Your money, your keys' goes the crypto motto. In this view, banks are unnecessary agents. Parasites seeking to perpetuate their status as middlemen.

In addition to the revolutionary romanticism they arouse, they base their narrative on technical lies about how the system works. The main one is about its decentralised system status, which, they say, makes it impossible to stop. It is also intended as a substitute for gold as there are a limited number of bitcoins. In turn, the concept of Decentralised Finance, or *DeFi*, was invented and solidified as a counterpoint to the financial system traditionally identified with Wall Street.

Some of these concepts and ideas are detailed below. The best lies always have a component of truth, and this case is no exception. Incredibly, they have managed to get away with it for so many years.

6.1 Decentralisation

Decentralisation is one of the most repeated words in the crypto world. This concept, in itself, can be interpreted in different ways. The community uses it in the sense that the system runs on thousands of computers simultaneously. Thus, the programme is not maintained on a centralised server or by a single manager and is, therefore, a decentralised system.

As we have already explained, the technology behind Bitcoin has been misrepresented. It wants to impose the idea that any computer running the software is helping to support the system. This is a lie. Only miners participate in it. They are dispersed, but it is an illusion to think that the system is entirely decentralised. In practice, miners pool their computational power in what are known as 'pools'. This had already been predicted by Satoshi in one of his first posts in 2009, stating that as the system grows, maintenance would be carried out by "farms with specialised servers" *[15]*.

Today BTC, the famous Bitcoin, has less than thirty such pools. As we said before, they need a vast infrastructure: contracts with electricity companies, municipal permits, internet connection, etc. Like all organisations, they are subject to the laws of each country. If you wanted to stop BTC, BSV, Ethereum, or any cryptocurrency really, you would just stop the operations of those miners, and the system would collapse immediately.

We can also visualise centralisation as the bottlenecks in a sector. In the case of Bitcoin, in addition to all the factors necessary for its operation, we have two more intermediary agents: exchanges and e-wallets. They, in turn, depend on the regulated banking system. This makes it clear how a properly regulated system could be created.

There is real decentralisation because there is no financial entity controlling funds or issuance.

6.2 Regulation

Bitcoin is and will be regulated. There is no mystery to this. In reality, Bitcoin should be seen as an asset that can also be used as an exchange currency. If we think about it, everything that can be paid for with cash today has a lower level of traceability than Bitcoin.

It is sufficient to understand that to acquire bitcoins, it is necessary to use a foreign exchange like any foreign currency. The laws of each country will govern these exchanges. There is no further discussion. Those exchanges with physical offices will operate as any exchange does. Any digital exchanges that may exist must be duly registered to be able to receive transactions either via bank drafts or credit cards.

The same can be said of e-wallets. Like any software, it is subject to national regulations.

What happens if someone avoids these requirements and clandestinely buys bitcoins using an unregistered wallet? Such a person is likely to experience a severe inconvenience when going to any real shop to pay for their goods. Their plans would be even more absurd if significant figures were involved. It would be significantly wiser to hold such securities in cash and avoid headaches.

Of course, it would be ridiculous not to take advantage of the technology that Bitcoin presents to establish personal records where the privacy of individuals is maintained while ensuring that all parties comply with all obligations. The most sensible approach would be to start legislating slowly from small amounts where all parties can familiarise themselves with their use in a safe way. The developer ecosystem also needs time and space to offer solutions that are scalable and secure. The same can be said of regulators.

The maximum value of payments that can be made integrated into each country's tax and regulatory systems can be gradually increased. The role of governments is to create registers or tools to facilitate compliance with all obligations in a practical and straightforward way.

On the other side, most of the interest groups within BTC promote non-regulation by holding the lie that it is impossible to regulate and exists beyond the control of any authority or power.

Miners only run one programme. They do not vote or make decisions. The integrity of the system depends on following the rules of the game. They must be identifiable to sanction those who try to break the rules. It is unreasonable to think that a miner would dare overrule a court order in any serious country. Nor would it be for a miner to decide to invest the money needed to set up operations in a country without a reliable legal framework.

Miners, exchanges and wallets are businesses, and as such, have to respect the laws and regulations of each country. Many of these players go to great lengths to maintain the myths in the community. They have no interest in facing regulations as that would imply taking responsibility. The truth is that liability is part of the social contract when someone provides a good or service.

Nowadays, most legal changes and systems that directly or indirectly allow cryptocurrencies to be held require formal documentation of personal identity according to the volume being handled. They do this to comply with international regulations.

6.3 Decentralised Finance

Decentralised Finance or *DeFi* refers to a financial system without intermediaries. The logic is that banks and the financial system, in general, have become agents whose intermediation results in an abuse of control over our resources. It is a financial system without authorities, where individuals can both raise finance for their projects and act as investors. While it sounds romantic and has a significant component of valid criticism of the current system, both systems are simplified.

On the one hand, listed companies must submit and publish their audited financial statements. Indeed, many investors do not do the relevant analysis, but the solution does not seem to be to eliminate any kind of requirements either. They are supposed to fulfil a protective function towards stakeholders.

Furthermore, they omit that there are already other venues where projects can be submitted for funding. These venues often involve giving up percentages for a service that does not seem to add much value. An efficient financial system should intercede between the parties to provide clear rules and prevent fraud and illegal activities. A system that claims to be 100% decentralised is nothing more than a platform to transfer money and receive a voucher or share without further guarantees.

This does not mean that the financial system does not need reform. The rules are unclear, and too many intermediaries who add no value profit exclusively from other people's capital and risk. Bitcoin is a tool that promotes transparency and, therefore, honest systems. It is illogical to demonise banks and, at the same time, sell the illusion that a system without controls will be fairer and nobler. Banks are made up of people; they are not independent entities that appeared on Earth.

6.4 Money as an Illusion

The crypto movement wants to convince investors, economists, politicians and users that money is an illusion. The rationale is that the US dollar is not backed by gold, unlike in the past.

While that is true, the dollar does have the backing of the Federal Reserve. Everywhere in that country and almost everywhere globally, the dollar is accepted as a valuable currency. Moreover, the rest of the world's currencies are also not backed by gold or any other commodity. However, this does not mean that they have no value or that it is simply a social convention. People all over the world accept money in exchange for our working hours. The sum of the money paid for these hours defines the final price of the goods and services produced. Money is, therefore, a source of information. It helps to translate work and goods so that they can be exchanged effectively.

On the other hand, Bitcoin is not accepted in almost any trade in the world. We cannot pay salaries, goods or services with Bitcoin. The only illusion is to believe that we will magically generate wealth by inventing new ways of measuring money.

The financial system can and must be improved. The management of public finance and inflation are problems that concern many countries and need to be monitored much more closely. The solution to the lack of control cannot be less control. The deficits of so many economies and their irresponsible management of the resulting debt generated simply reflect the hypocrisy and double standards prevailing in the political universe. No business or personal environment would allow such levels of financial malpractice.

It is necessary to understand that the crypto movement is not about crazy or stupid people. It has to do with people who feel permanently cheated and see their meagre savings reduced year by year because of inflation. At the same time, countries embark on investments they cannot afford using euphemisms such as *trusts* or *funds* so as not to use the ever-feared *debt*. At the same time, the intellectually weakened media accepts to be part of this circus while the people accept with resignation.

Better control and greater accountability are needed. You don't magically get that just by wishing for it.

6.5 Digital Gold

This is one of the fundamental pieces of the pyramid scheme operating mainly in the context of BTC.

By convention, only 21 million bitcoins can exist. This makes Bitcoin a finite asset, just like gold. In addition, both serve the function of preserving value over time and are easily interchangeable. The reasoning is completed by explaining that, since the actual supply is known and, given the impossibility of generating more coins, their price will reliably reflect their value.

A finite good may have no value in itself, as in the case of a painting, and yet be socially accepted as valuable. That is not the same as saying that every finite good will be valuable just because, at one point in time, many people consider it valuable.

Moreover, this idea is entirely at odds with the concept of Bitcoin as digital cash. While money has a value-preserving function, equating it with a commodity such as gold only turns it into a speculative asset. In this view, demand only exists because its price increases. In other words, demand becomes an end in itself.

Bitcoin as digital gold is just another attempt to increase its value and at the same time make investors reluctant to part with it. The actual market for BTC and cryptocurrencies is much less liquid than other markets, and this is how they want to hide this reality.

6.6 Governance

Bitcoin was designed to be as simple as possible to avoid manipulation. The spirit is that there should be no controlling agent, but that legal controls and regulation should be carried out by companies and agents designed to rely on this technology. What is done and what rules dominate the space is for each authority to determine.

Most cryptocurrencies and blockchains often refer to the individual's control over their money and the freedom this represents. Coincidentally, there is often very little information about who actually makes decisions in them. It would have you believe that the consensus of the 'community' is used to propose and implement action plans. The truth is that the vast majority of them are projects that end up providing enormous profit to their promoters regardless of their purpose. Along the way, the longed-for transparency is conspicuous by its absence.

7. Real Potential

Bitcoin, as conceived, is a unique tool and will change the way we interact with the digital world. The exchange of cash electronically is the first and most basic use. Its future will depend on our ability to innovate and implement new ideas.

As an example, here are some of the possibilities to be accomplished in such a system.

7.1 Automated Administration

Bitcoin is a ledger. With proper programming, many of the processes linked to accounting records can be automated.

The current accounting system is complex and inefficient. This has led to the confusion of accounting with a tax assessment system. For the vast majority of sole proprietorships and SMEs, the costs of accountants are equal to or higher than the costs of taxes.

Bitcoin represents the first real alternative to an automated administration and payment system. With an automated system, taxes can be settled and updated automatically. Let us remember that any business activity that does not generate added value is a waste of resources.

Counters can become counters again. Study flows and ratios and advise your clients based on objective metrics. States can also stop spending resources on processing vast amounts of ultra-processed information. With Bitcoin as a system, one can better understand and study the different economic dynamics that make up each sector and their interaction with each other. This means better tools for all actors to make better decisions.

7.2 Automatic Taxes

As a corollary to the previous point, the possibility of a system of automatic tax assessment and payment follows. Central Administrations in the different countries can create instruments whereby taxes can be directly withheld by the system and transferred to the state coffers.

Value Added Tax (VAT) is the simplest example to imagine. Whenever a transaction of a taxable good is made, the system can directly send the merchant his share, and the VAT amount can go directly to an account related to the tax address.

In practice, this is the end of withholding agents, which today do not add value to the process.

7.3 Entering into Contracts

Contracts are agreements between the parties. Formal agreements usually require compliance with specific guidelines that notaries verify. Many of these formal aspects can be considerably reduced with information stored on a blockchain.

Today, digitisation has led to the transfer of many formal requirements to computers. This has led to a redundancy in processes. Moreover, this information is often inaccessible and, therefore, simply lost among millions of poorly catalogued files. This is inefficient because it does not improve processes but, on the contrary, increases their complexity in exchange for hardly any greater guarantees.

While there is a concept of digital signatures for signing contracts in many countries, Bitcoin would allow this to be done in a faster and more convenient way. From car leasing to more complex contracts, third parties still need to be involved. For example, in such cases, a registered notary could use his particular keys to state that a process has complied with all formalities.

7.4 Digital Intellectual Property

One of the most exciting concepts developed in recent years is digital property, popularly known in the community as *NFTs*. Its name stands for Non-Fungible Tokens.

Instead of exchanging currencies, these are transactions in which ownership of a digital file, such as an image, is exchanged. These images must be unique and therefore subject to copyright. Like a work of art, they can be sold or just shared. The blockchain itself stores all movement and transaction history.

In principle, it may sound like a resource with no real-world applications beyond trading disembodied goods. The truth is that this type of virtual contract can open up a wide range of monetisable options.

Nowadays, whenever a media outlet wants to use a stock image for a story, it can go to an image bank and pay for the use of a photo. With this technology, spaces can be created where photographers can directly upload their images and impose their conditions for using these images by third parties. Owners could also set up the option to charge for each use of the photograph or image. But it would also be possible to set a variable rate based on the number of times the news item is shown. There are endless options, and it doesn't just cover photography. Memes and stickers could also be traded for pennies, allowing artists and creatives to generate value honestly and fairly.

8. Bitcoin and the Environment

One of the most common concerns about Bitcoin and other cryptocurrencies relates to the impact mining has on the environment.

Recall that miner farms are computers permanently connected to power grids. The damage then depends, primarily, on the type of electricity generation used in each case. It is not valid to add up the total consumption of all miners and assume an environmental impact on that basis. Many miners were initially attracted to countries or regions where energy is cheap, which is often associated with non-renewable sources such as coal. This is a problem, of course, but it is a problem for every industry on the planet.

The number of miners will increase with the use and adoption of technology. This will undoubtedly lead to an increase in the absolute value of Kilowatts consumed. Simply analysing this number is nonsense, as it does not consider the Kilowatts saved in current inefficiencies in different sectors that Bitcoin solves.

An analogous case, but little talked about, is the famous "*clouds*", servers specially designed to guarantee remote access. There is no company in the world that does not use these systems in its activities. People also use them directly or indirectly every day. These clouds are permanently connected computers sending and receiving data. Their total electricity consumption is enormous. When analysing its actual environmental footprint, the savings in hard disks, storage units and centralised servers should be examined first. Subsequently, we should make a complete analysis of all the components behind the production, distribution and sale of each. Then, study the current consumption of these clouds, applying pro and con corrections for and against efficiencies and inefficiencies due to centralisation, creation of new applications and expansion of pre-existing markets, among others. Then we may have a simplified idea of a possible impact, which in practice will translate into more and better mitigation measures, which in theory we were already doing anyway. Whatever the outcome of such a study, the conclusion will never be to dismantle the installed infrastructure and return to the past.

The truth is that it is challenging, if not impossible, to calculate the real impact of each industry on the environment. While generalisations are helpful as they serve as an average, actual traceability is a much more complex puzzle than we want to admit. Most environmental studies and reports often differ significantly from each other. This is because the parameters for assessing such impacts often differ in the technical rigour applied and the proper understanding of the different actors involved in a product chain. Moreover, the lack of suitable and scalable alternatives to replace such mechanisms is often overlooked. It is not my intention to go too deeply into these aspects. A frank analysis starts with the actual costs of generating, conserving and distributing energy in all its options and can never be summarised in a few simple lines.

Having said that, BSV is infinitely more environmentally friendly than BTC. Recall that the latter has a limit on the size of its blocks. This results in a reduced number of transactions per mined block, contributing significantly to the system's inefficiency. Bitcoin is efficient, not the Bitcoin we all know, BTC. That is why it is essential to understand what is happening in this sector.

9. The Future of Bitcoin

It is common to label new technologies with the ability to make significant changes as "disruptive". The truth is that the vast majority often fail to deliver on these promises. It is always a risk to venture into the future, especially when it comes to technology. Expectations are often not met due to unforeseen constraints, and, at the same time, unforeseen implementations often slip into the real world.

One of the main constraints usually ignored when analysing such technologies is often the ability to scale the production of the tools necessary for their full development. Every year we see outstanding presentations of humanoid robots doing all sorts of tricks and stunts. Still, the closest thing we have to an actual implementation in real life is an automatic hoover with wheels but no eyes and no brain.

Bitcoin is an information system. The essential infrastructure it needs to operate has already been in place for years, and that is the Internet.

It has the strength of being infinitely scalable. This is due to the permeability to be part of the mining and therefore contribute to the maintenance of the system. As their use increases, the more attractive it will be for new miners to join the market. Moreover, we must remember that they compete with each other, so efficiency is intrinsic to the system.

Most likely, Bitcoin, or BSV, will eventually overlay this cloud of misinformation and begin to be used in the short term to make minuscule payments. For example, newspapers and portals will be able to charge pennies on the dollar to read a specific news item, which can be done at the push of a button. It is also very likely that content creators, such as YouTubers, will start accepting tips in this currency. We tend to make the mistake of thinking of them as rich young people and the reality for most of them is far from this. Today, to reward them for something they do for free, we have to join a site, enter our details, credit card and, in most cases, commit to a monthly payment. With Bitcoin, we can simply send three dollars to the person responsible for a YouTube video, just as today we can leave a banknote in the hat of a musician practising his art in the streets. This is not taking away from the credit card market but opening up a market that did not exist before. The primary beneficiaries will be those in other parts of the world for whom $3 can change their lives.

When in doubt, it is always advisable to study the technical implementations in the pornographic industry, a pioneer in all technological innovations: VHS, Webcams, Pay-Per-View, Live streaming, to name a few. As is currently also the case with legal cannabis businesses, they have always had difficulties getting paid and making formal payments, so it will not be long before this type of tool can function in a regulated and secure way.

Mistakes will be made along the way. There will always be malicious actors willing to execute fraud and deception. It is, therefore, natural that their initial uses are for insignificant quantities. This also takes the pressure off governments to develop robust and functional monitoring systems. It would be a waste of time and resources to try to generate mechanisms to control a few dollars. With the development of technology, knowledge, and its materialisation in real life, we will be able to advance in the different uses of Bitcoin as a supplement to cash.

Hundreds of programs and applications are already being developed, from video games to databases, which we will use in the future without even being aware that they work using the Bitcoin blockchain as part of their structure.

In this context, it is most likely that in the future, we will use a single virtual currency, Bitcoin, and a single blockchain area for programming other applications, including Bitcoin. This is not out of necessity but practicality. Using several blockchains would mean developing extra support to interact with each other. That would be a waste of resources. For the same reason, most computers use Windows, Linux or Mac. It would not be feasible that every computer program we interact with should be developed to support twenty different systems. Nor would it be to try to create patches to adapt them. Of course, it is possible, but it would not make sense. A standard protocol that works and is scalable does make sense.

10. Conclusion

At the time of the writing of this document, BTC was trading at around $70,000 per coin, while BSV was less than $200. The substantial difference between the two is that the latter works, and the former does not. There must have been no other time in history when disinformation has been so influential in manipulating prices. The truth is that its price is irrelevant and shows a lack of understanding of the tool that Bitcoin really is. Its application in the real world is what should matter about any technology. Citizens will be its end-users. Ordinary people. Not investors and financial speculators. As such, we cannot allow a set of Illuminati under a media umbrella to use and abuse their position to create a fictitious market and at the same time increase their power with ill-gotten dollars.

Dr Craig Wright is Satoshi Nakamoto, and no serious person who claims to have studied Bitcoin and listened to his words can deny it. His name has been cruelly tarnished and with it his integrity, and that of his family. A person whose only crime was to provide a tool to improve the world. He does not need this document to defend his work or his legacy. We, the individuals, do have a moral obligation to speak out against injustice. In assuming our role as witnesses to what is happening and denouncing the real culprits. Otherwise, no technology will rescue our society from ourselves. It is time to stop delegating moral responsibilities to third parties and do the right thing simply because it is right.

All truth passes through three stages.
First, it is ridiculed.
Second, it is violently opposed.
Third, it is accepted as self-evident.

Arthur Schopenhauer

Author's Endnotes

This work was carried out personally with the motivation to bring clarity to a truly complex subject due to the diversity of disciplines it encompasses. My professional background is in Economics and accounting. My income comes from my private activity as founder and director of Tajes 5, a company that is not related to the technological or financial world. As of the original date of publication, 22 November 2021, I hold no securities in Bitcoin or any of its variants. Nor do I have any vested interest in any company or organisation in the sector, nor any links with people who may have such an interest.

It is always a good idea to go to the source. In addition to reading the original White Paper, I recommend listening to Craig Wright directly in the following interview. As he explains, he has Asperger's, a syndrome on the autism spectrum. This makes it difficult for him to interact with people.

1) Bitcoin's Most Hated Man - Craig Wright, By Patrick Bet-David, Valuetainment, YouTube, https://www.youtube.com/watch?v=0JvDauIX5lg, 16 July 2020.

To better understand how Bitcoin works graphically:

2) But how does bitcoin actually work, By 3Blue1Brown, YouTube, https://www.youtube.com/watch?v=bBC-nXj3Ng4, 07 July 2017.

To learn more about the chronology of events since the launch of Bitcoin I recommend:

3a) The Most Elusive Identity On The Internet - Pt. 1 (Ft. Nexpo), By Barely Sociable, YouTube, https://www.youtube.com/watch?v=_Kav2K1DVWo, 18 January 2020.

3b) The Most Elusive Identity On The Internet - Pt. 2, By Barely Sociable, YouTube, https://www.youtube.com/watch?v=fMWnaR5uJxQ, 07 February 2020.

3c) Bitcoin - Unmasking Satoshi Nakamoto, By Barely Sociable, YouTube, https://www.youtube.com/watch?v=XfcvX0P1b5g, 11 May 2020.

4) Why I Believe Craig Wright is Satoshi, By Kevin Healy, YouTube, https://www.youtube.com/watch?v=3MJSEGnpgB8, 29 April 2021.

To delve deeper into all the concepts and technical aspects behind Bitcoin, the following channel contains 70 hours of interviews with Craig Wright by Ryan X. Charles. In them, they review the original role of Bitcoin and all the events that led to the current state of the industry. Undoubtedly, there is no better material than this to understand everything related to Bitcoin and its history.

5) Theory of Bitcoin - Dr Craig S. Wright & Ryan X. Charles, YouTube, https://www.youtube.com/c/TheoryofBitcoin/videos, 22 June 2020.

To understand a little more about how networks work, I recommend:

6) Networking Course from 0, by NASeros, YouTube, https://www.youtube.com/playlist?list=PLSvxAUzJ-XSfY0KpwV8SHBlyLVcrZkENc, 18 July 2021.

I invite interested parties to pursue their own research and draw their own conclusions. The Internet can be an excellent source of information, but it requires a great deal of mental flexibility when processing and separating facts, speculation and lies. This is especially true in industries that move so much money under the shield of altruism.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, https://craigwright.net/bitcoin-white-paper.pdf, 31 October 2008.

[2] Bitcoin: $1bn seized from Silk Road account by US government, BBC.com, https://www.bbc.com/news/technology-54833130, 5 November 2020.

[3] Hace 10 años nació Silk Road, primer mercado de la dark web que aceptó bitcoin, Por Luis Esparragoza, CriptoNoticias, https://www.criptonoticias.com/comunidad/10-anos-nacio-silk-road-primer-mercado-darkweb-acepto-bitcoin/, 27 January 2021

[4] Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/posts/bitcointalk/523/, 5 December 2010.

[5] Inside the Fight Over Bitcoin's Future, Por Maria Bustillos, The New Yorker, https://www.newyorker.com/business/currency/inside-the-fight-over-bitcoins-future, 25 August 2015.

[6] Bitcoin's forked: chief scientist launches alternative proposal for the currency, Por Alex Hern, The Guardian, https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist, 17 August 2015.

[7] Scaling Bitcoin: The Great Block Size Debate, Por Brian Armstrong, The Coinbase blog, https://blog.coinbase.com/scaling-bitcoin-the-great-block-size-debate-d2cba9021db0, 3 January 2016.

[8] Bitcoin swings as civil war looms, Por Leo Kelion, BBC.com, https://www.bbc.com/news/technology-40654194, 20 July 2017.

[9] Bitcoin's SegWit and Lightning: Need of the hour or not needed at all?, Por Biraajmaan Tamuly, AMBCrypto, https://eng.ambcrypto.com/segwit-and-lightning-need-of-the-hour-or-not-needed-at-all/, 15 December 2019.

[10] Dr Criag S Wright, https://craigwright.net/about/#biography.

[11] Is Bitcoin's Creator this Unknown Australian Genius? Probably Not (Updated), Wired, https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/, 8 December 2015.

[12] This Australian Says He and His Dead Friend Invented Bitcoin, Por Sam Biddle y Andy Cush, Gizmodo, https://gizmodo.com/this-australian-says-he-and-his-dead-friend-invented-bi-1746958692, 8 December 2015.

[13] Credit Card Processing Fees and Costs, Por Joe Resendiz, Value Penguin, https://www.valuepenguin.com/what-credit-card-processing-fees-costs, 9 September 2021.

[14] Average Credit Card Processing Fees and Costs in 2021, Por Lyle Daly, the ascent, 13 April 2021.

[15] Satoshi Nakamoto Institute, https://satoshi.nakamotoinstitute.org/emails/cryptography/2/, 3 November 2011.