Emirati Journal of Business, Economics and Social Studies
Vol 4 Issue 2 (2025)
Pages (139 - 147)

Available at
www.emiratesscholar.com

Blockchain & Cryptocurrency: New trusted third party or danger for its users?

Houda Zouirchi
Doctor in Economics and Management, La Research Center in Management and Economic Sciences (CReSC), HEC Business school, Rabat, Morocco
houda.zouirchi@hec.ac.ma

ARTICLE HISTORY

Received: 04 November 2025.
Accepted: 30 November 2025.
Published: 09 December 2025.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by three independent reviewers.

HOW TO CITE

Zouirchi, H. (2025). Blockchain & Cryptocurrency: New trusted third party or danger for its users?. Emirati Journal of Business, Economics, & Social Studies, 4(2). https://doi.org/10.54878/hnnach73

ABSTRACT

Purpose: This paper explores whether blockchain and cryptocurrencies serve as a new trusted intermediary or pose risks to users. By examining their fundamental characteristics, it assesses how these technologies impact trust in economic and financial systems. Method: A qualitative analysis is conducted, combining a literature review with case studies of blockchain applications across different industries. The study also draws on theoretical perspectives on trust and digital transformation to evaluate the implications of blockchain adoption. Results: Findings highlight blockchain's potential to enhance trust through decentralization, transparency, and security. However, they also reveal significant risks, including regulatory challenges, cybersecurity threats, and the speculative nature of cryptocurrencies. The study emphasizes the dual nature of blockchain: as a tool for trust-building but also a source of uncertainty and disruption. Originality: While existing research often focuses on either the technological aspects of blockchain or its financial applications, this paper provides a comprehensive perspective by analyzing its role as a trust mechanism. By framing blockchain within the broader concept of "trustnomics," the study offers insights into its long-term implications for business models, governance, and society.

Keywords: *Blockchain, Trust, Cryptocurrency, Innovation, transformation.*

Introduction

Constantly shifting and evolving with the pace of innovations and new technologies, the world as it once was no longer exists. Today, we are witnessing the dawn of a new and global revolution, omnipresent and far-reaching. Its impact is difficult to measure, but its applications are numerous, almost limitless. *Blockchain* technology heralds a technological revolution so complex and fascinating that it echoes the Internet revolution of the 1990s. *Blockchain* gained significant popularity after being featured on the cover of *The Economist* in 2015, with the headline already hinting at a promising future: « *The trust machine* ». Since then, terms like « *blockchain* », « *cryptocurrency* », « *Bitcoin* », « *Ethereum* », and « *Proof of Work* » have traveled around the world, reaching everyone through the media, sparking curiosity and fascination. As for Bitcoin, this virtual currency, belonging to no one and everyone at the same time, without intermediaries or trusted third parties, no bank involvement, and powered by the virtually infallible *blockchain* technology, has reached its peak. Its price has reached the highest value ever recorded. Behind this cryptocurrency and its related concepts and technologies lies the first application of the fascinating *blockchain* technology, which emerged nearly ten years ago, in 2009. Behind it all is a multitude of cryptographic technologies and concepts.

This article aims to popularize and demystify, in both a pedagogical and professional/managerial scope, the functioning of *blockchain* technology used by cryptocurrencies. It addresses the following question: ***« Are blockchain and cryptocurrencies a new trusted payment method or a danger to users? »*** It will first place the emergence of cryptocurrency within its historical context to explain its functioning. It will analyze the issue of this new shared trust within its economic, social, and political environment to define its stakes, potential, and limits. Finally, it will assess the current level of knowledge and adoption through a qualitative and quantitative survey. These technologies have the potential to change the rules of the game, especially the global banking system, creating a new paradigm of trust as we know it today. A new model of trust is emerging, one based on a decentralized and shared system, replacing the current trusted intermediary. The advent of a new world is unfolding before our eyes.

1. Literature Review:

2. Cryptocurrency

Cryptocurrency is a computer protocol that hosts an electronic and universal currency, making it usable across the entire globe. But where did the idea of cryptocurrency come from? Did it truly originate during the 2008 financial crisis?

The concept of cryptocurrency actually dates back to 1982, emerging from the idea of creating a transaction system that protects anonymity and prevents payment traceability. It is easy to understand that it is impossible to track a cash transaction (its amount, date, and the parties involved—the payer and the receiver), unlike credit card payments or bank transfers, which leave traces. This gave rise to the concept of cryptocurrency.

In 1982, a decade before the development of e-commerce, in a document titled « Blind signatures for untraceable payments », David Chaum described the first encrypted system to enable untraceable payments. The author explains how to achieve payments based on cryptography that prevent third parties from knowing who is paying, at what time, and for what amount. In 1990, in another document titled « Untraceable electronic cash » , the same author explains that using credit cards has become an act of faith, as they offer no protection against surveillance or fraud. Thus, the idea of cryptocurrency was conceived well before the 2007 crisis, but it was in 2008 that it materialized with Bitcoin, the forerunner of these new digital currencies based on cryptography.

In 2008, one or more individuals using the pseudonym Satoshi Nakamoto published an article on the « cypherpunk » mailing list, which is referred to as the « White paper » by the Bitcoin community, aimed at describing how the protocol works. Bitcoin allows for near-instant and free exchanges via an electronic wallet. Unlike other currencies issued by central authorities, it does not depend on any higher regulatory entity, whether state or bank-controlled.

This gives it a monopoly over control of the currency, which is why it captivates so many minds. This concept is clearly stated on the official Bitcoin website : « The concept of Bitcoin is based on the fact that no organization can dictate new rules or arbitrarily issue bitcoins » .

1.2. The blockchain protocol:

Blockchain technology can be seen as a sequence of digital documents grouped into successive blocks, each containing the hash of the previous one. Such structures emerged in the 1990s due to the growing need to prove that a given software is indeed the new version of another.

This is how the role of the timestamping authority became established, which prints its digital seal on a document to certify its origin, creation date, and reference to an older document. Rather than « timestamping » a series of twenty documents consecutively, several individuals managed to find the appropriate formula to group all these documents into one block and seal them together. This timestamping server generates computer proofs of the chronological order of Bitcoin transactions within the system.

It is secure as long as reliable nodes collectively control a majority of the transaction verification network. At least 51% of reliable nodes are required for the network to be invulnerable to attacks. Nowadays, processor power is no longer sufficient to operate the Bitcoin system. Miners, who circulate bitcoins in addition to confirming and securing network transactions, have transitioned from using graphical processing units (GPUs) to programmable logic circuits, and are now utilizing ASIC (Application specific integrated circuit) power, which has been specifically designed for the Bitcoin system. Thus, each new element confirms the previous one. A blockchain is, de facto, identifiable by its unique hash. When this process is repeated, it results in a chain of blocks, known as the blockchain. This well-known certification technique was later developed in the Bell Labs located in the United States and was ultimately adopted in 2008 by Satoshi Nakamoto. Many attempts were made to create purely electronic monetary networks before its actual creation in 2008, all of which failed.

1.2.1. From currency to cryptocurrency:

The author of this remarkable technological advancement is Satoshi Nakamoto. No one knows for sure whether this is a single individual or a group of several people. Satoshi Nakamoto conceived and developed Bitcoin, as well as the Bitcoin Core software, from 2009 to 2010. Before this date, no trace of their identity has been found. The individual claiming to be a 37-year-old Japanese has stated that they had been working on this technology since 2007 and published a document introducing their invention in 2008. In 2009, the first version of the Bitcoin QT software, along with the very first units of currency, was born. In 2011, they posted a final message on the « bitcointalk » forum, which they created on December 12, 2010, to the other Bitcoin contributors. They wrote to Martti Malmi: « I've moved on and will probably not be around in the future ».

For a long time, Satoshi Nakamoto was the only active miner. According to an analysis by Sergio Lerner, the fortune of the creator of this revolutionary protocol could reach one million bitcoins. According to the introductory article that Satoshi Nakamoto published on January 12, 2009, titled « Bitcoin: A Peer-to-Peer electronic cash system » , they pose an essential question: how to eliminate a central regulatory authority while ensuring a high level of trust from users? For Nakamoto, it is necessary to record all transactions in a ledger that self-regulates and monitors itself.

1.2.2. Toward a new paradigm of digital trust?

The true value of a currency lies in the trust that its users place in it. How much trust can we actually place in this new digital currency ? Security aside, the use of a currency is adopted on a large scale only if its users grant it near-total trust. For example, consumers use the dollar because it is difficult to counterfeit, the Federal Reserve does not issue money out of thin air, and it is a currency issued by the largest economic, geopolitical, and military power in the world. However, since the Bretton Woods agreements in 1971, the dollar is no longer convertible into gold and lacks intrinsic value. Similarly, in Europe, the production cost of the most recent five-euro banknote is less than five cents. To establish this trust in digital currency, Satoshi Nakamoto chose mathematics and algorithms. A cryptocurrency like Bitcoin is rare, imperishable, and infinitely divisible.

Its creation follows a very complex mathematical law, characterized by being generated solely within its network. Furthermore, there are several ways to store it : online platforms, external hard drives, DVDs, paper printing, digital storage, etc. As long as the medium is accessible, bitcoins remain accessible as well. Thus, it is essential to establish a crucial fact : Bitcoin is a currency that meets all the requirements related to the trust that a citizen should grant to a currency, with a significant advantage over traditional currencies : no trusted intermediary is established in its rules of operation.

1.2.3 Consumers :

Bitcoin consumers are the true nerve center of the network ; without them, it would merely be a protocol for exchanging information, revolving around complex and unused mathematical algorithms. It is not an easy task to define the exact number of users on the network, simply because each user can create as many addresses as they desire. As of the fourth quarter of 2017, there were approximately 21.5 million *blockchain* wallet users. The average age of Bitcoin users is 31 years, with 85% of them being men, and nearly 70% of them owning fewer than 10 bitcoins (currently, 10 bitcoins represent 63,746.38€), reflecting the relatively recent nature of cryptocurrency purchases. Furthermore, nearly 20% of users of this currency have never used a single bitcoin. These consumers, through their usage, are closely linked to the trust placed in cryptocurrency. The value of Bitcoin, as explained earlier, primarily relies on the law of supply and demand. It is the consumers themselves who define the price of Bitcoin in real-time.

1.3. The blockchain revolution : How does It resemble the Internet revolution?

The Internet is an old military technology dating back to the 1960s, but when the private sector seized it in the 1990s, it became evident that it would change the world . Thousands of entrepreneurs then embarked on projects, with varying degrees of success, and the most visionary built today's digital society. Today, the same phenomenon is occurring : hundreds of projects launch every day with the ambition of changing the world by harnessing this still relatively unknown technology.

This frantic pursuit has led to the « bubble » that doomsayers often describe when talking about the price of Bitcoin. It is likely that the market will experience a severe correction (the question remains as to when society will experience the peak), but like the Internet, cryptographic technology is here to stay. The advancements offered by cryptography represent an upgrade to the Internet. It enables users to regain control over their data.

As of 2018, blockchain technology is poised to become the new Internet. The year 2017 was marked by rollercoaster fluctuations in cryptocurrency prices. « Altcoins » experienced massive growth and attention, largely due to Bitcoin's wild ride of continuous increases and decreases that year. Regardless, Bitcoin succeeded in introducing cryptocurrency and blockchain to the global stage. Whether taxpayers understand it or not, the public has taken notice, along with their money. To this day, trading continues unabated, and new users are on waiting lists. Institutional currency is slowly infiltrating the market, and the influx of capital does not seem to be slowing down anytime soon. In 2017, the rest

of the industry outside of Bitcoin grew six times faster than its predecessor. Today, blockchain is essentially a new form of the Internet, although the two terms are not synonymous. Cryptographic technology will power Web 3.0, the new Internet.

While the advent of the Internet and blockchain are complementary and similar, they do have some distinctions. The Internet has enabled the automation of relationships; in contrast, blockchain facilitates the automation of transactions by removing trusted third parties. The Internet is a decentralized publishing system, while blockchain is a distributed consensus system. The Internet serves as a publishing infrastructure, whereas blockchain functions as a certification infrastructure. The Internet, which emerged in 1994, can be characterized by the following: personal communications, self-publishing, e-commerce, and social networks. By 2015, blockchain emerged with promises of decentralization of trust and value flows without intermediaries.

1.4. The dangers of blockchain and cryptocurrency:

In principle, the elements described above assert that the security of the network and the exchanges between Bitcoin users are guaranteed. However, the dangers associated with blockchain and cryptocurrency are very real.

1.4.1. Network-related risks:

One of the primary sources of risk concerns the mining procedure. When the blockchain operates under the « Proof of Work » mechanism, a validated block rewards the miner who solves the problem with Bitcoin. This is where potential abuses can arise : if a miner discovers the solution first, they have a block called « Be » (a block kept in the chain) that they should communicate to other participants. However, they could keep this block secret and work on validating the next block without revealing « Be » to the rest of the network. This technique is known as « selfish mining ».

Once another « honest » miner finds a block « Bh » (a block not kept in the chain) that follows the blZockchain, the « selfish » miner will almost instantly disclose their block « Be ».

At this point, the network witnesses two blocks validated simultaneously and temporarily stored on the blockchain. Some nodes in the network will be aware of block « Be », while others will know block « Bh ». New blocks will then be added after « Be » and « Bh », creating two separate chains. The simultaneous creation of two blocks leads to what is called a "fork." For instance, if a person named Alice exchanges one Bitcoin with Bastien, and this transaction is recorded in « Be », while simultaneously, Alice exchanges one Bitcoin with Célestin in « Bh », there will be a double-spending issue (Decker, 2013), resulting in one of the users (Bastien or Célestin) being defrauded.

Furthermore, another risk relates to the anonymity of users. It is indeed possible, with appropriate tools, to know in detail an individual's activity. To resolve this issue, it is advisable to group a number of signatures under a single link, thus enhancing anonymity. A composition of signatures can then be recorded on the blockchain.

1.4.2. Volatility risks:

At the same time, Bitcoin faces heavy criticism regarding its volatility, which is higher than that of traditional currencies and gold. With no ties to any reference currency or regulatory authority to monitor its value, the cryptocurrency is traded solely based on supply, demand, and speculation. Highly dependent on new technologies and IT infrastructures, the price of cryptocurrencies is constantly fluctuating. More than just a medium of exchange, Bitcoin is increasingly used as a speculative instrument, with 55% of bitcoins not circulating within the network but serving as investments, thereby influencing its price volatility. For example, Bitcoin fluctuated from 13$ in January 2013 to around 166 $ by mid-August. By mid-2014, it had risen to 600$ per unit.

2. Empirical literature review :

In this section, we will present various previous studies that address issues closely related to our core research question. This overview is essential to confirm the collective findings of the different

studies conducted, which will be summarized in the form of a table :

Author	Study	Methodology	Key findings	Conclusion
Nakamoto, S. (2008)[1]	Bitcoin : A Peer-to-Peer Electronic Cash System.	Theoretical modeling of the Bitcoin system.	Proposal for a decentralized blockchain-based system to eliminate the need for a trusted third party in financial transactions.	Blockchain ensures transparency and security, but trust depends on widespread adoption.
Zohar, A. (2015)[1]	Bitcoin : under the hood	Technical analysis of the Bitcoin protocol and its vulnerabilities.	Highlighting the security vulnerabilities and potential solutions for the Bitcoin protocol.	The underlying technology is robust but requires improvements to ensure user trust.
Catalini, C., & Gans, J. S. (2016)[1]	Some Simple Economics of the Blockchain.	Economic model of blockchain in commercial transactions.	Blockchain reduces verification and audit costs in transactions.	Although blockchain offers economic benefits, the risks of manipulation or attacks must be monitored.
Yermack, D. (2017)[1]	Corporate Governance and Blockchains.	Qualitative analysis of the impact of blockchain on corporate governance.	Blockchain enhances transparency and reduces corruption in corporate governance.	Blockchain can be a new tool for trust in governance, but security risks must be assessed.
Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017)[1]	A Survey on the Security of Blockchain Systems	Literature review and case analysis on the security of blockchain systems.	Security vulnerabilities, particularly 51% attacks, threaten trust in blockchain.	Blockchain offers significant advantages, but security improvements are needed to minimize risks.
Kshetri, N. (2018)[1]	Blockchain's roles in meeting key supply chain management objectives	Empirical study of the use of blockchain in supply chains.	Blockchain improves traceability, transparency, and cost reduction.	Although beneficial, security and privacy issues remain.
Tasca, P., & Tessone, C. J. (2019)[1]	A Taxonomy of Blockchain Technologies : Principles of Identification and	Comparative study of different blockchain technologies.	The various applications of blockchain are classified according to their structure and associated risks.	The impact of blockchain on trust varies across applications, necessitating continuous risk

	Classification			assessment.
Feng, C., Wang, H., & Zhang, Y. (2020)	Cryptocurrency and its impact on global financial systems	Quantitative analysis of the effects of cryptocurrencies on financial markets.	Cryptocurrencies provide new opportunities but are associated with increased volatility and risks of fraud.	Cryptocurrencies can play a disruptive role in financial systems, but they require clear regulations to protect users.

Source: Prepared by us

This table highlights the evolution of studies on blockchain and cryptocurrencies, starting from the initial research on Bitcoin and its technical foundations to recent analyses on applications and risks in various sectors.

3. Methodology:

3.1. Presentation of the data collection tool:

The research methods for this article will include qualitative interviews and quantitative studies through questionnaires. The qualitative interviews were conducted with a range of professionals (miners, investors, journalists, entrepreneurs, etc.), while the quantitative study is exclusively aimed at individuals. This was carried out with a sample of approximately 120 participants using the « Google Forms » platform. The recruitment criteria considered include : investment amount, involvement, experience, professionalism, and occupation.

Professionals were selected based on their roles in the cryptocurrency and blockchain technology sectors, either directly or indirectly. They provided insights related to trust, technological adoption, and skepticism towards cryptocurrency. These professionals contributed their expertise in this technological field.

For the questionnaire directed at individuals, the article sought out « techies » - people highly interested in this technology - as well as engaged investors. The questionnaire was structured around their motivations. Additionally, individuals who did not intend to invest or had the intention to use a cryptocurrency in the future were also targeted. The primary motivation was to determine their risk level and skepticism.

3.2. Justifications and list of interviewees:

3.2.1. The qualitative interview:

In the field of qualitative studies, individual interviews are the most commonly used technique due to their ease of implementation. The qualitative interview is particularly suitable for this article as it allows for an understanding of the motivations and barriers related to Bitcoin. The goal is to gain a better understanding of cryptocurrencies—especially Bitcoin—and blockchain, as well as their uses, motivations, barriers, and risks, both from the taxpayer's perspective and from a managerial standpoint. The individual interviews conducted ensured the spontaneity and freedom of response of the interviewee. The flexibility of the exchange allowed for very personalized follow-ups, which were particularly useful for constructing precise client typologies or validating an existing concept. However, this method has the drawback of low responsiveness.

Generally, considerable analysis time is required to obtain actionable results. This method demands thorough preparation for the exchange, the involvement of an experienced professional, rigorous analysis, and satisfactory, conclusive results. The qualitative interviews conducted for this article lasted between 45 and 90 minutes to gather all the necessary information. In some cases, the interviews were conducted face-to-face, while others were conducted via email or telephone. The interview was directive, very detailed, covering several themes, and before concluding, all discussed themes were verified.

The quality of the data collected strongly depended on the involvement and experience of

the interviewee (author, researcher, cryptocurrency specialist, investor, miner, etc.). As the interviewer, it was my duty to provide positive attention and active listening to the subject while wisely employing rephrasing techniques. The aim is to encourage responses rather than simply providing information, ensuring a sincere, realistic, and unbiased testimony. Managing silences and reflective phases of the interviewee, as well as the ability to interpret non-verbal language, are other key elements.

Regarding the analysis of the interview, it was necessary to transcribe them. The verbatim statements (excerpts from the respondents' discourse) were translated into complete sentences to understand their context and ensure better comprehension for the readers of this article. Subsequently, content analysis was performed by working with the verbatim statements, as well as through inventories (of words, themes, verbs, etc.) and structuring the information by themes or types of individuals.

To achieve this, five interviews were conducted : Lucas Martin, Investment Advisor at Coin Capital ; Thomas Dupont, Cryptocurrency Journalist at Capital ; a blockchain miner who preferred to remain anonymous ; Camille Robert, Finance Researcher, Lecturer at CNAM (National Conservatory of Arts and Crafts), and author of several works in the field such as The Revolution of Bitcoin and Complementary Currencies (Eyrolles, 2013) ; and Émilie Lefebvre, Doctor of Scientific and Technical Information.

3.2.2. The choice of the quantitative questionnaire:

The population analysis model includes both Bitcoin users and non-users, both professional and individual. Several factors come into play. Alongside classical sociodemographic variables such as age group, family situation, and gender, we find: the intention to use or not use cryptocurrency or blockchain technology, personal or professional experiences with cryptocurrency (positive or unsuccessful), attitudes that are more or less favorable toward this blockchain revolution, and the degree of knowledge about it. The originality of this model lies in highlighting the complex relationships between these variables on one hand and, on the other hand, the representations and attitudes toward the technological emergence of cryptocurrencies and blockchain, as well as the intention to use them.

Here is the analysis model used here, which incorporates these various elements: environment and information: use of blockchain and cryptocurrencies, modes of information (social circle, media, Internet); cognition and attitudes: direct or vicarious learning (substituting), attitude and knowledge regarding this « new » technology; sociodemographic factors: age, gender, profession, family situation, education level or socio-professional category, geographic location; conative variable: intention to use/invest in the technology.

4. Collection and analysis of responses:

4.1. The quantitative field study:

For the completion of this article, it was crucial to establish a quantitative field study, specifically through the use of an online questionnaire. Here are the results divided into three parts : the habits of the population, their relationship with trust in this technology, and finally, the typical profile of the investor. This questionnaire gathered 125 unique responses.

4.1.1. The habits of the population and their knowledge:

Before studying a complex technology, it is essential to understand its consumers and users and to determine their level of knowledge in order to filter and refine the analysis of the responses. The cryptocurrency most commonly recognized by respondents is Bitcoin, with 98% of responses, closely followed by Ethereum (63.2%), Bitcoin Cash and Litecoin (56%), and NEO (47%). Respondents believe that cryptocurrencies are used by "geeks" (76%), exchange platforms (75.2%), individuals (71.2%), criminals (53.6%), and banking institutions (43.2%). For them, cryptocurrencies are primarily used for investment transactions (66.6%), the Dark Web (50%), and speculation. Thus, for the majority of respondents, Bitcoin and blockchain are familiar

concepts; for others, to a lesser extent, they are new notions.

Of the 125 individuals surveyed, half believe that one of the limitations of Bitcoin lies in the difficulty of regulating this dematerialized system. The other half, however, suggests that the Internet does not make it impossible to regulate the Bitcoin and cryptocurrency system. Furthermore, nearly 90% of respondents think that Bitcoin and cryptocurrencies will continue to develop and their use will become more widespread.

For a large majority (73%), cryptocurrencies present a real advantage over the current banking system. Cryptocurrencies provide traceability and transparency, which in many areas could multiply exchanges and facilitate business, trade, the effectiveness of development aid, and even fundraising for humanitarian organizations, as suggested by the UN press release in August 2017 encouraging member states to work on developing blockchain technologies. Some respondents see this as an opportunity for individuals to break free from the traditional model and thus benefit from a form of freedom.

4.1.2. Between reluctance and trust:

The use of Bitcoin and cryptocurrencies as a real alternative to the current banking system is divisive : half of the respondents believe in it, while the other half do not. However, one in four respondents considers Bitcoin a means to bypass the current banking system, if not to replace it. While some tend to think that the population needs the traditional banking system to access cryptological services, others believe that transfers made in cryptocurrencies are easier to trace than so-called national or international money, which the population uses for "under-the-table" payments, including for the purchase of illicit products. The risk of criminals seizing it is significant, as the end of Silk Road clearly demonstrated.

Conversely, some argue that these are two fundamentally different systems. One is centralized, the other is not ; one is inflationary, the other deflationary. The current economic system is based on debt ; as soon as the state stops borrowing, the system collapses. Thus, with the help of cryptocurrencies, such a system becomes unthinkable. However, banks are not about to disappear ; they will have to play by new rules to adapt to an ecosystem that is changing increasingly rapidly. Cryptocurrencies and blockchain are here, and they cannot be ignored given the significant stakes for states. Indeed, they allow for improvements and economies of scale that will enable banks to achieve notable efficiency gains. As Herman Gref, president of Sberbank, a Russian giant, pointed out : « Protectionism is just the first reaction of the state. That said, institutional money and states [...] will eventually find a place for cryptocurrencies within the economy ».

Furthermore, for more than two-thirds of respondents, a convergence between the current fiat system and cryptocurrencies is conceivable. Indeed, decentralization allows for regaining control over currency. Society is witnessing the birth of a new economy based on the trust of a network rather than an authority. A century ago, church and state were separated ; today, it is the turn of currency and state. Other respondents raise an essential point and suggest that Bitcoin is a currency with too volatile a price. Thus, the current banking system is well established, and it will be a challenging task to ask taxpayers to use a new currency based on a technology they do not master and do not understand. For the respondents, Bitcoin is more of a safe haven that could replace gold over time. Indeed, the ecosystem surrounding Bitcoin is too significant for it to disappear. Regarding the future of this disruptive technology, the majority of respondents (89.6%) are confident. They believe that the network will continue to expand and evolve, and especially to secure itself. Today, the Bitcoin network, in terms of computational capacity, is 300 times larger than the five most powerful computers in the world.

Thus, every attack on the blockchain, every threat from politicians or the media, will serve to secure and improve the network. Bitcoin is currently the most resilient cryptocurrency. Despite its various weaknesses, it will remain the first cryptocurrency

offered to humanity, in the sense that its governance model and any potential improvements are relatively democratic and that no one can control it–neither corporations, states, nor hackers. One of them specifies : « Bitcoin Core is completely autonomous and will function until the last node of the network (computer) disconnects. Bitcoin is unstoppable and accessible to anyone who has internet access ».

4.1.3. Profile of investors and non-investors:

To capture the typical profiles of informed cryptocurrency investors, a persona was created to understand their behavior. In this regard, more than half of the survey respondents have already invested in a cryptocurrency. To facilitate the creation of this persona, cross-tabulations were conducted, and here are some of them

Figure 1: Investment according to gender

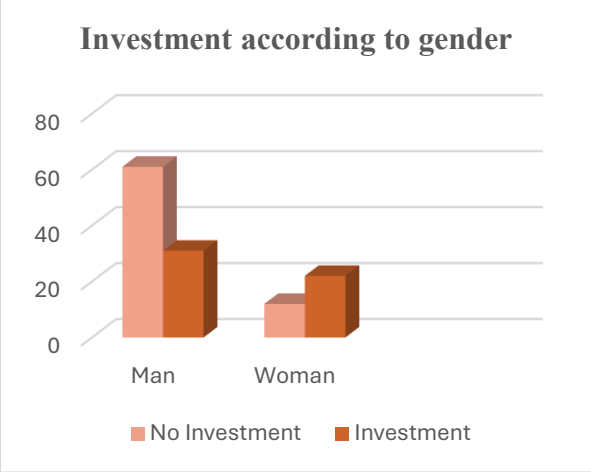


Figure 2: Investment according to socio-professional category

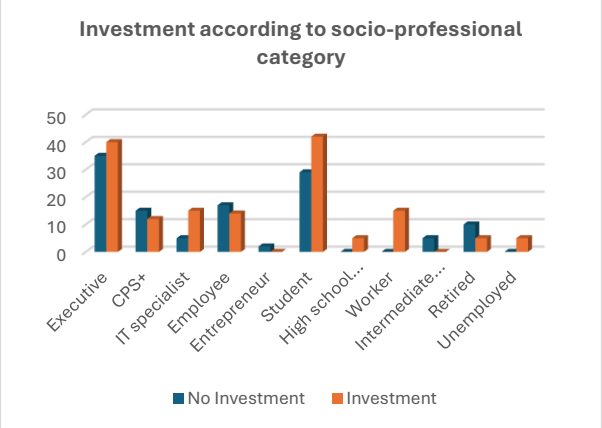


Figure 3: Investment according to family situation

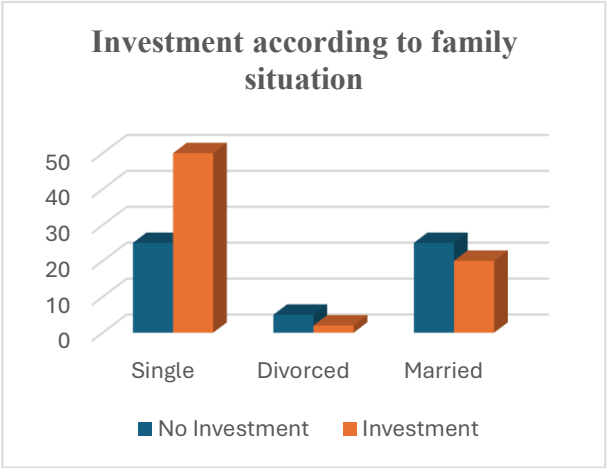
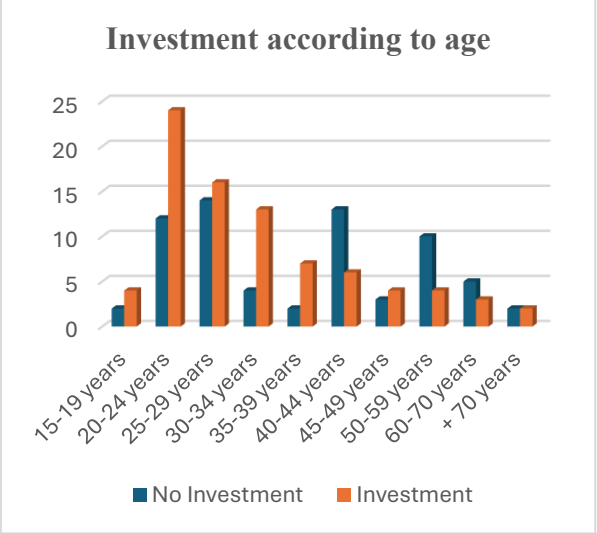


Figure 4: Investment according to age



Source: Prepared by us

Thus, after processing the questionnaire and creating several cross-tabulations in the form of pivot tables using Excel, it was established that the typical profile of a cryptocurrency investor is a man aged between 20 and 24 years, who is either a student or an executive, and who is single.

4.2. The qualitative interviews:

Various stakeholders encountered after the completion of this article contributed to furthering the reasoning articulated around trust in blockchain technology and cryptocurrencies.

4.2.1. A complex protocol with a future:

Through the first step of this field analysis, it was established that cryptocurrencies and the blockchain protocol are complex concepts. Many express both positive and negative opinions about them. Thus, it seemed essential to seek clarification on certain points from professional interlocutors and specialists in the field.

For Lucas Martin, cryptocurrencies and blockchain allow anyone around the world to freely express their creativity, particularly in terms of new projects, reshaping their relationship with trust. But what are their purposes ? What is the primary goal of this technological revolution ? Two crucial aspects should be noted. According to Thomas Dupont, from a technical standpoint, a cryptocurrency transaction allows for electronic payments without intermediaries. Proponents of cryptocurrencies, especially Bitcoin, believe that this technology frees them from the arbitrary decisions of central banks. They can be justified in this belief, as movements in interest rates or monetary easing are never subject to citizen votes, even though these decisions significantly impact their economic fate.

Thus, the blockchain is merely a digital ledger on which the vast majority of cryptocurrencies rely. It is reputed to be tamper-proof, as what is inscribed on it cannot be erased or altered. While it is called revolutionary, it is actually the entire ecosystem that functions alongside it that creates a system with tremendous potential. During our interview, Thomas Dupont wanted to highlight the point regarding the proof-of-work mechanism, which he characterizes as nearly impervious to fraud but very energy-intensive. This is what allows transactions to be validated before they are inserted into the blockchain.

Therefore, the democratic nature of money stems from its innovative character. This is indeed a public blockchain open to all humanity ; it was not created by a corporation or a state but for a universal purpose and is not controlled by anyone. « There is truly an equal relationship between nations », notes Lucas Martin, « everyone can appropriate it around the world ». Anyone who wishes can engage in payments regardless of international restrictions.

Mr. T.K. (pseudonym), a blockchain miner, emphasized the crucial importance of mining. « However, I have noticed that, unlike trading where you must make good moves (i.e., buy low and sell high), mining is a different philosophy ». Thus, in the mining world, a miner is an integral part of the universe and plays an indispensable role in the proper functioning of the blockchain. Without miners, neither the blockchain nor cryptocurrencies can exist.

4.2.2. Is Bitcoin really a currency?

The Bitcoin protocol was born during the global economic crisis of 2009. At that time, and still today, states were forced to dig deeper into their deficits and increase their debt. To address this, nations heavily solicited central banks to buy back their debts. Bitcoin then emerged as a safe haven, allowing individuals to secure their capital during times of crisis. This cryptocurrency was hailed by a majority of tech enthusiasts who believed in its promising future. However, is Bitcoin truly considered a currency ?

On this subject, economists agree that a currency is considered as such when it serves as a medium of exchange, a store of value, and a unit of account. In this sense, Bitcoin is a simple and rapid means of exchange. However, its extreme volatility does not allow it to be regarded as a store of value or as a unit of account.

The question of Bitcoin's classification is crucial. The stakes are both legal and tax-related, and the rules vary depending on the country. Furthermore, states face a challenge in classifying the capital gains made from cryptocurrencies. While some ideas have been raised, nothing has been decided yet. Jean-Paul Pinte highlighted that the classification of a cryptocurrency like Bitcoin can be double-edged : it can be regarded either as a currency or as a capital gain on movable assets, with the former definition being more advantageous for taxpayers, as it is not taxed at 19% beyond 5,000 euros, unlike capital gains on movable assets.

It is established : Bitcoin is considered by many as an international and universal currency ; no one truly controls it, and it belongs to everyone.

However, it cannot be categorized alongside national currencies. Moreover, it is important to clarify that it is a deflationary currency. In other words, as time passes and the currency is adopted, individuals will be able to purchase more with the same amount of money.

4.2.3. Major barriers:

Investing in Bitcoin can be dangerous, but this holds true for any investment. Lucas Martin does not hesitate to emphasize the golden rule of any investment : « One should not invest more than they can afford to lose ». This makes even more sense for cryptocurrencies when we know that the only risk of loss in Bitcoin is one's own investment, and nothing more.

However, there are other significant risks, such as environmental risks, particularly the excessive energy consumption associated with cryptocurrencies. But regarding this consumption, Camille Robert, is optimistic about the future, citing technological advancements that will drastically reduce the energy requirements for operating the network.

It is also essential to remember one key point : Bitcoin currently holds a mediocre market capitalization estimated at $6.4 billions, while the dollar is capitalized at 1$ trillion.

As a relatively new currency, Bitcoin still has a long way to go before it can be considered a renowned international currency or a reference currency. Its future remains uncertain and depends on future revolutions in payment methods before it can create a disruption that would forever change trust, much like the intention of Satoshi Nakamoto in 2009.

4.3. Recommandation : Bitcoin, an uncertain yet promising future

Although Bitcoin frequently makes headlines due to its fluctuating price, it has yet to achieve widespread adoption of its protocol. Currently, its market capitalization hovers around 125$ billions, which is just a drop in the bucket in the global finance landscape. The number of users ranges between 20 and 30 millions, which is also relatively low. But what about its development? It is in a state of failure. Its primary function—facilitating peer-to-peer payments on the Internet—is being sidetracked by its users. Investors primarily buy Bitcoin in hopes that its value will increase, storing it away rather than utilizing it. This behavior has been noted by many economists who argue that Bitcoin is gradually becoming a store of value, akin to gold. Like gold, Bitcoin is limited in quantity on Earth (a maximum of 21 millions units, each divisible into 100 million parts). This scarcity adds to its value.

Every year, the Bitcoin community celebrates May 22, 2010, the date when a user successfully exchanged 10,000 bitcoins for a real good. This significant day in the history of cryptocurrency is now the subject of sarcasm. Nevertheless, thanks to Laszlo Hanyecz, Bitcoin transitioned from a mere experimental protocol to a potential currency, and perhaps nothing would have transpired as it has if he hadn't spent his 10,000 bitcoins. Users should spend it rather than hoard it if they truly believe in it.

Regardless, Bitcoin has a bright future ahead. Gregory Raymond state : « To those who think Bitcoin is dead, I invite them to the next financial crisis ». Indeed, it is highly probable that Bitcoin will gain recognition during one of those events that Wall Street is known for, which occur every 10 to 20 years. Its collapse triggered a domino effect that led to a significant financial shock worldwide. In Europe, there was a long-held belief that the euro would not survive. If Bitcoin had existed during the collapse of Lehman Brothers in 2008, it would likely have attracted many individuals frightened by the solvency issues of states. Just three years into its existence, Bitcoin already showcased a glimpse of its potential : its price surged tenfold in early 2013 amid threats from the Cypriot government contemplating seizing part of the population's savings.

One possibility for accelerating its adoption would be if a tech giant allowed it for payment transactions. Numerous rumors circulate regarding Amazon and Facebook, but it is more likely that these companies will launch their own cryptocurrencies to be used for purchasing goods or services on their respective platforms. Such an

announcement would still significantly impact Bitcoin, as Amazon coins would need the original cryptocurrency to ensure liquidity in the markets. If that day were to come, the protocol must be capable of handling a larger volume of transactions. Currently, it struggles to support more than 300,000 transactions per day. This issue is taken very seriously, and several developer teams are working on implementing Lightning, an upgrade designed to multiply the number of transactions Bitcoin can process. Its future on a larger scale depends on their success.

In the shorter term, Bitcoin and Ethereum will benefit from the rise of ICOs—new types of fundraising that require cryptocurrencies to invest in startups. This new economy exploded in 2017, raising 5.6$ billion globally, and promises to continue its momentum following regulatory actions initiated in most countries.

On a negative note, it is always possible that Bitcoin will lose its appeal and revert to being an experiment reserved for a handful of libertarian tech enthusiasts. However, regardless of what happens, its creation will not have been in vain. The technology brought forth by Bitcoin has already led to significant revolutions. The blockchain is now being used by major companies such as Carrefour, Crédit Agricole, SNCF, and Axa, to name a few in France. For these companies, this represents substantial productivity gains as they no longer require human certification to validate certain actions that previously needed it. Gradually, blockchain will integrate into most of our computer systems, suggesting it represents the new era of the Internet, shared with artificial intelligence. What will Bitcoin look like in 50 years ? This protocol may be defined as a grand philosophical experiment that has somewhat been overtaken by events. The blockchain will likely be to transactions what the Internet has been to information. Regardless of its future, Bitcoin has already made its mark in the economic history of the world.

4.4. Critical approach and relevance of the topic and methodology:

Upon reflection and after the completion of this article, it becomes apparent that the complexity of such a subject is significant. Being a nascent and recent technology, few academic works or research articles have been published on the topic. Due to its innovative nature, many skeptics have written about it in the press, making it often difficult to distinguish between fact and fiction, and between mere opinion and genuine knowledge.

Furthermore, the choice of the problem was very broad. This article focuses on trust, which requires addressing nearly all aspects of the topic, including its origins, explanations of technical terms, the functioning of blockchain, cryptocurrency in general, as well as other cryptocurrencies. This writing also discusses the adoption of new technology and compares it to the revolution of the Internet. Regrettably, some sections had to be cut and condensed, even though they would have been interesting for a lay reader who is entirely new to the subject. Thus, after reading this work, beginners likely did not grasp everything there is to know about the topic. The limited page count was a significant constraint on the completion of this article.

In terms of the methodology applied to the fieldwork, it proved to be conclusive. The quantitative field study, which was reserved for individuals, allowed participants to express their opinions, although their responses were sometimes too subjective. The qualitative interviews were relevant, despite the difficulty in finding qualified interlocutors who were available to answer the questions.

Conclusion:

It is established that trust, certainty, and transparency in transactions are key factors for business and commercial success. When people engaged in bartering, they knew whom they were dealing with ; trust inherently existed, and it was up to each individual to decide whether to trust their counterpart. As commerce developed, everything became more complex, and institutions evolved into neutral authorities in which both parties held a certain degree of trust. In this regard, Douglass C. North, Nobel Prize winner in economics, wrote that these institutions

were specifically created to « create order and reduce uncertainty in exchanges » .

Nonetheless, even if reduced, uncertainty remains. Today, with the promise of blockchain technology, the potential to strengthen trust in business without any intermediaries becomes possible. In this way, Bitcoin allows for bypassing banks and states, aligning with the culture of Internet pioneers who distrust governments, censorship, and denounce mass surveillance society. Born from this culture, Bitcoin thus becomes a new potential third-party trust. The decentralized digital scarcity, a true innovation, and the most striking promise of blockchain technology is certainly the potential to restore trust and transparency in transactions based on reputation without mediation by third parties whose interests may not align with ours.

However, as with any technological advancement, dangers exist, and users must be aware of them before adopting it. Environmental issues and its use for illicit purposes pose an obvious threat to its uncontrolled proliferation, raising the question of how states will intervene, if at all, to limit it.

So, does Bitcoin, in its current state, have a future ? This disruptive revolution has its detractors and skeptics, much like the Internet or social networks did in their time, which have now become the norm for everyone. Given the speed at which technological revolutions are adopted, it is highly likely that Bitcoin, or at least the principle of blockchain, will quickly become part of everyday life, raising the question of its regulation by governmental bodies and, more broadly, the role of the state in the new economy based on peer-to-peer.

Bibliography:

Buterin, V. (2013). *Ethereum white paper*. GitHub Repository, 1(22-23), 5-7.

Catalini, C., & Gans, J. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research. https://doi.org/10.3386/w22952

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology - Proceedings of Crypto '82* (pp. 199-203). Springer. https://doi.org/10.1007/978-1-4757-0602-4_18

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. In *Lecture notes in computer science* (pp. 319-327). Springer. https://doi.org/10.1007/0-387-34799-2_25

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in Cryptology - Crypto '82* (pp. 199-203). Springer.

Ducrée, J. (2022). *Satoshi Nakamoto and the origins of Bitcoin: The profile of a 1-in-a-billion genius*. arXiv. https://doi.org/10.48550/arXiv.2206.10257

Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841-853. https://doi.org/10.1016/j.future.2017.08.020Niel, X., & Roux, D. (2012). *Les 100 mots de l'internet* (3rd ed.). Presses Universitaires de France. https://doi.org/10.3917/puf.niel.2012.01Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. *Ledger, 4*. https://doi.org/10.5195/ledger.2019.140

Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Technology Law Journal, 30*(4), 1127-1170.

Wright, C. S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3440802

Yermack, D. (2016). Corporate governance and blockchains. *Review of Finance*. https://doi.org/10.1093/rof/rfw074

Zohar, A. (2015). Bitcoin. *Communications of the ACM, 58*(9), 104-113. https://doi.org/10.1145/2701411

References:

Chaum, D. (1983). Blind signatures for untraceable payments. *In* Springer eBooks (pp. 199-203). https://doi.org/10.1007/978-1-4757-0602-4_18

Chaum, D. (1983). Blind signatures for untraceable payments. *In* Advances in Cryptology - Crypto '82 (pp. 199-203). Springer-Verlag.

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. *Lecture Notes in Computer Science*, 319-327. https://doi.org/10.1007/0-387-34799-2_25

Cypherpunks. (n.d.). An informal group of individuals promoting privacy through cryptography.

Buterin, V. (2013). *Ethereum white paper*. GitHub Repository, 1(22-23), 5-7.

Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Technology Law Journal, 30*(4), 1127-1170.

Wright, C. S. (2008b). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802

Ducrée, J. (2022). Satoshi Nakamoto and the origins of Bitcoin – The profile of a 1-in-a-billion genius. *arXiv*, 1-152. https://doi.org/10.48550/arXiv.2206.10257Niel, X., & Roux, D. (2012). *Les 100 mots de l'internet* (3rd ed.). Presses Universitaires de France. https://doi.org/10.3917/puf.niel.2012.01

Altcoins. (n.d.). Definition: Any cryptocurrency other than Bitcoin or Ethereum.

Wright, C. S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802

Zohar, A. (2015). Bitcoin. *Communications of the ACM, 58*(9), 104-113. https://doi.org/10.1145/2701411Catalini, C., & Gans, J. (2016). Some simple economics of the blockchain. https://doi.org/10.3386/w22952Yermack, D. (2016). Corporate governance and blockchains. *Review of Finance*, rfw074. https://doi.org/10.1093/rof/rfw074

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841-853. https://doi.org/10.1016/j.future.2017.08.020

Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. *Ledger, 4.* https://doi.org/10.5195/ledger.2019.140Regulation Review. (2010). Douglass North: Neo-institutional heterodoxy versus neoliberalism? https://journals.openedition.org/regulation/7719