EAMR

EUROPEAN ACCOUNTING AND MANAGEMENT REVIEW

VOLUME 8, ISSUE 1, ARTICLE 3, 54-82, NOVEMBER 2021

New economic-business paradigm: The cryptocurrency and the tokenization of the economy. Monetary and financial revolution. The Blockchain, as the ultimate evolution of the accounting book.

José Daniel Barquero Cabrero

ESERP-Abertis Observatory, Spain

Mario Rioboo

ESERP-Abertis Observatory, Spain

Received November 23, 2020; accepted November 10, 2021.

ABSTRACT

Since the beginning of the economic revolution in terms of cryptocurrency and tokenization, we have been researching the theoretical aspects and the practical and real implementation aspects. As well as the potential that these have to establish new financial, entrepreneurial, accounting, and many other paradigms. We cover various fields (philosophical, legal, monetary) and areas that may be affected by the emergence and subsequent establishment of this new paradigm. Through comparisons or examples, we try to clarify the common factors that have in common with business success and the development t of these new elements.

KEYWORDS

Cryptocurrency, blockchain, tokenization, cryptoactive.

1. Contextualization and historical conceptualization

In the course of human history, we have located two great advances that have changed the sociological development of humanity and have brought logic, coherence and ease to its social, economic and commercial development, among others. These two inventions that have evolved with society, and which we will always deal with from both the intellectual and sociological point of view, are not purely scientific or technological advances; they are what have made it possible to lay the foundations of concrete characteristics in the relationships of both people, both of their means, and of the civilizations that have been formed throughout the course of human history, establishing that basis in the development of transactions.

After our research, fruit of our analysis, these two elements are: language[1] and money[2]/currency[3], understanding the latter as united terms, in fact, they are gathered as synonyms. Both are associated with different particularities, as well as other brilliant inventions or underlying ideas. Language understood in its broadest sense and money as an index to value the level of wealth. We have not found any other determining element for the development of human activity that has had such an impact.

Both elements have acted as mediators throughout ancient and contemporary history. Understanding language, in its broadest sense, with its meaning and content as language and money as an index to value the level of wealth, being represented in the currency(money), in that is measured. This money directly influences the development and survival of communities. Wealth marks people's destinies, and money is a wealth meter for the population in general and as economic activity develops, in different elements that appear in it.

Perhaps, in recent times, an invention has appeared that can end up displacing them or establishing itself at their level (that of language and currency). This invention is the Internet. According to our analysis, the new element has the potential to deploy new evolutions or advances of the previous ones, as has already happened at the level of

[1] Language: The ability of human beings to express themselves and communicate with others through articulated sound or other sign systems. Language. (RAE Dictionary)

[2] Money: Current currency. Treasury, fortune. (RAE Dictionary)

[3] Currency: Instrument accepted as a unit of account, measure of value and means of payment. (RAE Dictionary)

language and as could happen with currency, deploying it through its networks and making it serve to function in a useful way. However, given the bizarre nature of the invention and the lack of comparability in terms of its impact on society, we cannot yet consider the Internet and everything it represents at the same level. Although it seems to be part of this cast, for what it has represented until now, it has them. As the famous writer, member of the Royal French Academy, Victor Hugo said: "There is nothing more powerful than an idea whose time has come".

However, if we speak of the Internet, of what emerges and for what emerges, we could consider it one of those sub-elements associated with language. Its basis is communication; with that intention, it was born in its origins and in practice it has managed to revolutionize it. For this reason, we must analyse the Internet in everything that has to do with people and the association between them, whether it is directly or indirectly related to language or money.

Richard Buckminster Fuller, American designer, architect, visionary and inventor, said that: "You will never change things by fighting against the existing reality. To change something, you have to build a new model that makes the existing model obsolete". In the same line, the most influential German philosopher of the 20th century, Martin Heidegger (2002), asks how man has to face the technological revolution, with all the advances for humanity that this entails, whether positive or negative. He reflected that it is necessary to understand and to put them in a context of total and abstract mental opening, not only to prepare for the external changes that are coming, that will modernize and change all the society and its rhythms, but to internalize and to accept new paradigms that in another epoch would be totally implausible.

Dr. Enrique López González (2018) raises the importance of the introspective re-evaluation of our relationship with previously internalized and acquired dogmas and thoughts, especially regarding the advance of digitalization in many aspects of our society, making some observations in order to be able to make predictions in the future.

It is necessary to arrive at a meditative modification of thought, above a continuous revolution based exclusively on pragmatism, and that which is calculable or quantifiable. The philosophical current of progressive rationalism[4] suggests to move away momentarily from pragmatism, interiorizing in our conscience new ideas, to later develop them pragmatically.

[4] Rationalism: A doctrine based on the omnipotence and independence of human reason. (RAE Dictionary)

All this is happening all the time and is caused by a dizzying succession of technological and social advances. These evolve and transform modernity itself, at an increasingly significant rate.

There is a tacit acceptance of this idea in the Anglo-Saxon term VUCA[5], coined by Bennet and Lemoine (2014) in their articles in the "Harvard Business Review". The word VUCA combines the four main characteristics of this modernity, and at the same time the most difficult to assume mentally, as it happens with everything that is: Volatile, Uncertain, Complex and Ambiguous.

From the technological and human development analyzed in our study, in the last years it has arisen, fruit of the advances and social demands, the financial and economic "self-management", without damage of failures or mutabilities. It is then when the "Blockchain"[6] rises as a consequence of the new order forged by the Internet. The "Blockchain" is nothing other than the digitalization of the accounting general ledger, an element that has been used since the old age to reflect the economic or financial movements of any entity. Thanks to the accounting ledger, the first city-states were born and it became sustainable to execute the most basic values of control and order to be applied on the management and administration of the economic life of a society. The "Blockchain" eliminates, one of the first problems that the accounting general ledgers had when there were few resources, a palimpsest[7] effect, which makes it possible for them to be modified and mutated. Similarly, the problem of double spending, which is so worrying in terms of digital money, is eliminated.

But what specific advantages and benefits does such digitalization achieve? To begin with, the block chain eliminates the main problem of the analogical or mutable accounting book. Nothing recorded can be rewritten or deleted because technology makes it immutable. Through consensus among users and the rules that everyone assumes when

[5] V.U.C.A: acronym for volatility, uncertainty, complexity and ambiguity.

[6] The blockchain is a data structure in which the information contained is grouped into sets (blocks) to which information is added relating to another block in the previous chain on a timeline, so that, thanks to cryptographic techniques, the information contained in a block can only be repudiated or edited by modifying all subsequent blocks.

[7] Palimpsest: Manuscript in which the primitive text has been deleted, by scraping or other procedure, to rewrite a new text. (RAE Dictionary)

using this technology, the possibility of erasing or rewriting records, as well as the problem of double spending[8], is removed from the equation.

The most fascinating thing about the "Blockchain" technology attached to any "token"[9] or "crypto currency"[10], is that within it there are cultural, philosophical, ethical, ideological and pragmatic foundations. Some of its characteristics refer to different fields and subfields within those fields. To give an example, within the economic field, the "blockchain" brings together features of game theory or incentives, accounting, general ledgers or balance transfers, and even of mathematics or cryptography.

There are many other theories and theorems applicable to different fields and issues, which make the valuation of this technology complex. From an analytical point of view, their coherence and logic have very clear functional bases, which, although mutable by consensus, make it inadvisable to try to deceive or modify them at first (according to the protocol, doing so costs more than the hypothetical benefit obtained). It is also determined, after a detailed analysis, that it maintains its own idiosyncrasy, even though it is analyzed from many different ways and perspectives.

The "bitcoin" is the circulating currency or "token", attached to the "Blockchain". To make a comparison, we would say that it is the gasoline that allows the "blockchain" to work and, at the same time, acts as an oil so that its gears maintain their essence and nature. However, it is difficult to define the cause-effect relationship between Bitcoin and Blockchain. Due to the fact that it is the crypto currency with the largest community of users, which moves more capitalization and dominates a high percentage of the market, the technology has been able to reach a higher level of development. The association and conjunction of both technologies (blockchain and bitcoin) established in 2009 by Satoshi Nakamoto[11] (Nakamoto, 2009), is what we know and forms the TCD; Distributed Accounting Technology.

Even though the blockchain technology is not exclusive to Bitcoin, and its nature makes it adaptable to other tokens or crypto-currencies (for example: Ethereum, Ripple or

[8] Double spending is a potential flaw in digital currencies whereby the same digital currency or token can be spent more than once on the same network.

[9] In numismatics, "tokens" or monetiformes are coin-like objects, which are used instead of coins without being so.

[10] A cryptocurrency is a digital medium of exchange.

[11] Satoshi Nakamoto is the name assigned to the person or group of people who created the Bitcoin protocol and its reference software, Bitcoin Core.

Bitcoin Cash), the perfect symbiosis with the Bitcoin network is what places it in a position of superiority and preponderance over other digital currencies. Although a thorough analysis of Bitcoin raises many technical and other questions, the suitability of this union is unquestionable.

2. Paradigm development: Apparition and Ontology

The first time that the concept of *cryptomoney* is mentioned is in 1998, in the Bmoney essay (Wei Dai, 1998) about the anonymity of transactions between people, by the prestigious Doctor in Electronic Engineering Dai Wei. It is in this text where the bases of cryptocurrency are laid as the use of a value directly linked to cryptography as a means of protection, and to currency as a means of payment and deposit of value. Perhaps no one could foresee its rapid development at that time, but that is where the foundations of electronic or virtual currencies are laid.

About 10 years later the first public appearance of crypto currency occurs, which from that moment on becomes a reality. On the mailing list "cryptography", an announcement is made on November 1, 2008, a user under the pseudonym "Satoshi Nakamoto" reveals that he has worked on an electronic money system different from what we know so far, concisely shows us a summary of its properties and possibilities. It can be found in the original article (Nakamoto, 2008), in which both the first specification of the protocol and the Bitcoin proof of concept are compiled, and which has been done by the user, or group of users behind which "Satoshi Nakamoto" is hidden.

However, it's not until two months later, on January 3, 2009, that the Bitcoin peer-to-peer network is generated and launched and the Genesis block is created with it. As we will see later on, we call this block the set of transactions that are registered within the network in 10-minute periods. The first client is published, and the first bitcoins are generated, giving rise to the first existing decentralized e-commerce transaction where operations are not registered or channeled through banks or financial sector companies that track their transactions.

On February 11, 2009, a user, who again answers to the name of "Satoshi Nakamoto", publishes this time in the web portal P2P foundation, the following statement:


Comunicado de «Satoshi Nakamoto».

P2P foundation

The Foundation for Peer to Peer Alternatives

Main My Page Members Videos Forum Groups Blogs Chat

All Discussions My Discussions + Add

Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at

Fuente: P2Pfoundation.

Figure 1: “Satoshi Nakamoto” Notice. Source: P2Pfoundation.

In it, he explains which portal the Bitcoin system will use as its official portal, the article explaining the design, the initial client with which he started the network and, of course, the main features of Bitcoin in all its aspects.

That's how Bitcoin came about, but it won't be until the end of 2010 that the user "Satoshi Nakamoto" will announce that he's leaving the project to focus on other goals, leaving his legacy anonymously to the world, without any intention of notoriety, and disappearing as surreptitiously as he had appeared. Despite the great curiosity about the creator or creators of Bitcoin, their origin and motivations, we only know the data that was collected in the P2P foundation profile, at the time of publication: It would be a 38-year-old man, with Japanese nationality, something that unfortunately we can't verify, and we won't be able to verify, until someone proves that he has the original keys to the original Bitcoin network account.

There are several theories about the identity of "Satoshi Nakamoto". It must be assumed that the creator or creators have extensive knowledge of mathematical algorithms and cryptography, so some speculations point directly to well-known people around these aspects, such as Shinichi Mochizuki, a professor at Kyoto University who specializes in number theory. Some theories point out that its creator could be immersed in illegal businesses and black markets, since by its changing nature through exchange sites (bitcoin for any other currency), cryptocurrency can facilitate that type of business. It cannot be ruled out that the founder "Satoshi Nakamoto", through a message to one of the developers of Bitcoin, will disassociate himself from the project in 2011, in order to devote himself to other issues.

Knowing the origin of Bitcoin and the Distributed Accounting Book Technology, it is necessary to explain what the system it supports consists of and what its main lines of use or action are.

To begin with, we can talk about the DABT as three different things. It is at the same time, an electronic currency, a software and a protocol, but it is necessary that they appear as an integrated system that allows the realization of fleeting transactions between pairs, by means of the "P2P" or "peer-to-peer" network. By the very definition of this type of network and the way Bitcoin operates, it is an autonomous system that offers a number of rewards, allowing payments to be made worldwide with minimal or no transaction costs.

The choice of a technological system based on a "P2P" network, is one of the bases on which the creation of Bitcoin and its protocol is based. Since in this way it does not depend on a monetary authority which is in charge of the emission and control of money, as well as the establishment of self-determined monetary policies. In this way, the bitcoin becomes a currency whose value cannot be manipulated by any government body and, therefore, inflation cannot be created in the system by producing more currency. Since it is the network itself that manages both the issue of bitcoins and the transactions, it is difficult to think that its operation applied to a network of users cannot be a success. The issuance of bitcoins or any other cryptoactive used by the DABT system is not manipulable because it is the network itself that generates currency through so-called "mining", creating bitcoins in a controlled and decentralized way.

On the other hand, the use of cryptography in the protocols means that there is a great guarantee of security for the transactions. There is no surveillance or supervision by any

authority, as is the case with the rest of the existing currencies prior to Bitcoin. By using these cryptographic elements, double spending can be prevented and fraudulent payments avoided, since, if the latter happens, the system will reject it and the rest of the network nodes would equally reject the user's transaction.

In addition to the new technical aspects, the system of cryptocurrencies that Bitcoin opened the way to is new, due to a peculiarity that did not exist until now. A coin with the implications and volume of use and acceptance that bitcoin has, including the DABT protocols, works without an authority to regulate the issuance of coins or an authority that can decide whether to accept or deny transactions.

It is the users who assume that by using the Bitcoin network, they implicitly take command and make those decisions globally and among all users, collaborating to make the system work without anyone being able to manage it at their sole will.

We can understand this new nature and its philosophy through examples, to put them in context, even though we haven't yet gone deeper into the system or the protocol.

1st example: A user, let's call him Carlos, makes a payment of 351 BTC to another user whom we will call Miguel. How do we protect a network in a situation where Carlos could try to trick the system, to try to make a transaction again with those 351BTC, which now belong to Miguel? Well, so that Carlos doesn't try to use those 351BTCs again to pay Lucia (a third user and Bitcoin client), what the network does is publish the transactions. When they become public, if the user tries to spend again with those particular 351 BTCs, the system will notice and through the network, the rest of the users will reject it, which will make any attempt to reuse those 351 BTCs impossible.

2nd example: As we mentioned before, it is the Bitcoin users themselves who make up the network. Therefore, Bitcoin users collaborate directly with the network and, as long as each one of them collaborates, Bitcoin will reward them by obtaining bitcoins, (this process, known as mining, will be discussed in the corresponding block). This may tempt users to cheat the system to increase their bitcoin harvest, but because of the very structure of the system design, it is up to the users to validate this reward once it has occurred. Therefore, if the user decided to use fraudulent means to acquire new bitcoins, increasing the amount of bitcoins received, the action would be quickly rejected by the rest of the users, making it impossible again to manipulate the system.

Figure 2. Box about the practical explanation of the nature of Bitcoin. Source: Own elaboration for doctoral thesis at UOLS.

As far as we can see in this couple of practical examples, it is the nodes and bitcoin users themselves who are in charge of validating the operations, not a central authority. To feed itself, the network depends on the honesty of the network itself and not on the impositions that come from the monetary policies that a government institution decides to apply. From this we can deduce that, as long as more than ½ of the percentage of Bitcoin users in the network's computation are considered to be honest, the network will follow the evolution that they understand and assume to be correct. Bitcoin users have real power over the network, since the network is so vast it is literally impossible for a single person, or several of them, to claim more than half of the existing Bitcoins. The system marks the weighting of the user's influence on the Bitcoin network or any other cryptography using the DABT.

If we look at its nature and at the examples given above, we can sense that something really interesting is happening and that it has a projection and potential that goes beyond economics.

"Even under government pressure, Bitcoin could evolve as a sort of parallel society cohesive of countless fully voluntary agreements among Bitcoin network users" (Gonzalez Otero 2013).

Following the appearance of Bitcoin, a totally new economic and social framework appears on the scene. Nothing like this has ever existed before. If Bitcoin were adopted, or a later system that could be better adapted or that included substantial improvements over Bitcoin (like other existing systems already, with more advanced protocols), government bodies and financial authorities would not be able to control the evolution of money directly as they have been doing up to now, through the implementation of their monetary policies. They could influence it indirectly through regularization, regulation and subsequent legislation, but they could not control its behavior. As we will see later, the legislative framework in which an electronic or virtual currency such as the Bitcoin can be moved is cumbersome. Since it is international, and not national, it is more difficult for a regularization to take place or for effective legislation to be carried out.

But more important than legislation, since it is a totally new scene in the world economic order, are the effects of the global and generalized use and acceptance of this currency, which would turn the scenario into a complete unknown with unpredictable results.

3. Legal context for the regulator and its financing models.

We will analyze different concepts that will allow us to understand the contractual situation observed in different matters related to the situation of the regulation of cryptocurrencies and cryptoactives, mainly in relation to their possession and control.

3.1. Financing models - The ICOs.

There are three main ways to obtain cryptocurrencies, which determine the type of product, the development policy of the product and the ways or methods through which it will be financed.

Through airdrops[12]. In this case, the delivery of some coins is requested free of charge, which the developers of the same give, voluntarily and for free, to promote their new creation. It is the most virtuous way to acquire digital coins or cryptoactives, because the developer is particularly involved in the success of the coin and, on the other hand, it is the way with the least risk of all.

By means of hard forks[13]. The duplicities of the blockchain that give rise to new cryptocurrencies. If a chain is separated, because the developers or supporters of the network do not agree on its development, an investor who had crypto currencies in the first chain or original chain would have exactly the same crypto currencies in both chains. This is because where there was only one blockchain, it is doubled (there are two blockchains), and at the same time, the main blockchain is divided in two. And the inverter will have the same amount of crypto currencies in one than in the other.

By means of an ICO (Initial Coin Offer). Many of the financial fears and warnings from the regulators came in the wake of the ICO fever of 2017. According to Carlos Kuchkovsky, CTO of BBVA's New Digital Business, 2017 was the year of the ICO explosion. They experienced both great successes and a series of frauds, scams and outright failures, which were mainly what alerted the supervisor and forced him to warn and remind him of the nature of this type of (financial) cryptoactives.

Investing via ICO has its advantages and disadvantages. The main advantage, and at the same time the main objective of the investor, is to obtain a return on the cryptocurrency

[12] Airdrop: Process of distributing tokens, usually for free.

[13] Hard fork: type of P2P network protocol update that supports a crypto-currency, which implies radical changes in the consensus rules, and makes incompatible the software of the non updated nodes with the one executed by the updated nodes. Its making technically impossible for the first ones to validate data blocks created by the second ones.

or cryptoactive (by increasing its value or by the benefits that the idea or project linked to it can pay back). The main drawback is the risk of theft of cryptocurrency or its failure as a means of profit (a risk inherent in all cryptocurrency, such as the same physical money in circulation or bank money). It should also be taken into account that the more the value of a cryptocurrency increases, the more capital is acquired by the first investors. It can increase the price and "inflate" it artificially, due to its dominant position over the property (when we can strangle supply and demand, the market is under our control), its in turn generates lack of liquidity and low supply

It is quite possible that, in the future, the ICOs will allow the creation of new projects without the need for bureaucracies, placing us on the margin or in parallel with the traditional financial system. This would theoretically encourage innovation and at the same time the will of the market itself and the actors in it.

3.2. Between regularization and warning.

Since this is a completely new and deregulated concept, it is difficult to define and establish the legal framework in which Bitocoin or another cryptocurrency operates. As we have already commented, in order to standardize Bitcoin or another international currency, it would be necessary to standardize the regulation of the currency in a joint manner. Since just one server operating in a country that can escape the control of the network's transactions is enough for the network itself to continue operating without dependence or state control (all the nodes of the network would have to be intervened in order to manipulate it, since if only one node were to escape that control, it could invalidate all the operations).

With the intention of preventing legal loopholes, the "Financial Crimes Enforcement Network of the Department of the Treasury" made the decision to write a guide for the correct use and legitimization of virtual currencies in the USA (US, 2014). Bitcoin is included in it because of its decentralized system of behavior, and therefore the use of bitcoin in the US is legal. The guide also defines the obligations to which the user is subject and must comply. This was the first attempt at regulation of any crypto currency, which took place in the US.

In its early days, Bitcoin was barely regulated. Beyond any mention or creation of guidelines for its use, little or nothing was done for regulation. In a report (ECB, 2012), for the first time an international financial authority, the ECB, acknowledged that it was

studying and monitoring Bitcoin's movements and stressed that it posed a risk only to those agents who entered its network. However, at that time, Bitcoin was not considered a potential danger to the economy, as it has been later by government bodies in different countries.

In that ECB report, a tour of the virtual currencies and what they meant for the economy was made, analyzing technical aspects (monetary, fiscal and other more basic aspects). It also included a record of Bitcoin's vulnerabilities and the attacks it had received, as well as its uses on the network and aspects of its protocol. Reference was also made to the bad press and criticism it was receiving and the legal risks that the currency posed. Finally, the risks of price stability and how this could affect financial product were mentioned.

For its part, in 2009 the Central Bank of China banned trading in the first virtual currency that deserved its attention, the Q-coins, considering it potentially dangerous because of its hidden nature. Later, during 2013, it declared that it prohibited the trade of bitcoins because through its high volatility it exposed its clients to a risk that the country could not and did not want to assume. As a result of the lack of regulation, the Chinese government rejected their use both as a means of payment and as a currency, classifying operations carried out with bitcoins from its territory as illegal, as it considered that they were motivated by evasion.

The US Treasury Department, recognizing the existence of crypto-currencies and their recent acceptance and use by an increasing number of users, assumed that virtual currencies are indeed unregulated. But it did recognize the houses that are used when we establish an exchange between currencies (or a purchase of crypto-currencies if it prefers to be so defined), as an integrated element in the regulation.

As we have already mentioned, the main difference that Bitcoin or any other cryptocurrency has, with the rest of the physical currencies, is that it is not a currency regulated by a central authority that can set financial and monetary policies on its own economy and that is the one that responds and supports. However, this may not be enough to be able to solve global monetary problems in the event of a crisis, as we have seen throughout this paper. In the case of Bitcoin, this is not necessary because it works only because of the value attributed to it and granted by the members of the network. If this and other cryptocurrencies do not have the intrinsic value of trust that money generates because they are regulated by a government authority. It is not because anyone supports them or is interested in their adoption, but simply because they do not need it.

This trust and value are granted by the customers thanks to the complex system of computer protocols to which it is linked to the cryptoactive and which guarantee its security, something similar to what happened with gold and which we analyze and compare in this chapter of the paper.

In the year 2015, in the middle of one of its diastoles, Bitcoin and cryptocurrencies caught the attention of the notary's office. In February 2016, after studying and analyzing their case, the Centralised Body for the Prevention of Money Laundering in Spain launched several alert groups, to emphasize and remind notaries of the risk inherent in the use of crypto-currencies to incorporate a company, to make capital increases or simply to carry out transactions. Since then, the Spanish notary's office has followed the evolution of this technology in order to achieve its regulation to minimize its risks.

However, in the middle of the year 2019, we observe that the general forecasts to carry out this are not at all encouraging. On the one hand, we have the problem of what this technology means for different branches and sectors (including the notarial sector). If blockchain technology were to be imposed, the work of notaries would probably be in danger, unless it was supported by the route of state protectionism.

The danger lies in the fact that the individuals who are part of the network, set up an alternative and contemporaneous system with the "official" professional. It is would be based on blockchain and which would make the notary's work useless or unimportant, reducing its prestige and use value. As a matter of pragmatism, nobody would go to register something in a notarial way, being able to do it from home with an internet connection and at an infracentesimal cost, needing only the acceptance of the other individual. At that point the figure of the notary, who is both intermediary and arbitrator, could be forced to disappear.

With this example, we want to put on record the double standard or dualism that can exist when judging or valuing such technology, when it is exercised in a free, public and open way. Anyone can select it as their daily technology and somehow have some freedom to do things outside of state control. Therefore, every sector and segment regulated by the state will look with suspicion at a technology that in some way may make it obsolete or unnecessary, turning its functions into something archaic, analogical or symbolic.

In addition to the notarial sector, there are many other sectors affected by similar dichotomies, such as the financial sector, the registry, some aspects of the legal sector and public administration, and a long etc. These sectors will have to adapt to the new

technological situation, or exclude this new situation from their sectors, with the difficulties and dangers that this entails.

What is most worrying today, due to the reduced nature of their areas of influence and the number of people who are already introduced and operating in the crypto-currency sector (less than 0.01% of the world's population). It is the massive influx of "unwary private savers" who, unlike finance professionals, may not know or assess risks properly, while specialized users know and assume them as part of their profession and daily work.

Due to all these exceptional characteristics, together with the novelty of this type of product, idea or market, the actions of the different supervisory and regulatory institutions to date show different attitudes and a good level of legal or conceptual coordination and communication, at international level, is not yet apparent.

On the one hand, cryptocurrencies have been banned in countries such as China, Russia, Iceland, India, Bolivia, Bangladesh, Sweden, Thailand, Vietnam and others. Many others are trying to place them fiscally and legally within the different typologies that these countries have for their financial products/assets that are regulated and typified. This, far from appearing to be an adaptation to the circumstances or "simulate" a regulation, what it does is a sort of comparison with other different products. So that they can be integrated into the same legal framework; however, due to the exceptional nature of cryptocurrencies this would only increase the confusion about their use and their circumstantial situation in each country in which we want to analyse their supervision.

To exemplify the situation previously described, let us take the following samples in such different points of the international geography.

In Australia, the ATO (Autralian Taxation Office), considers that it is not a detrimental means to transactions, but classifies or qualifies it as a means of barter, and is subject to the regimes and levies of the related Australian tax law.

In Canada, the CRA (Canada Revenue Agency) considers them to be the same as the ATO as a barter medium, however, with the specifics of Canadian legislation. Transactions in crypto currencies are considered to be barter transactions. The income generated from each transaction is collected as business income. Exchanges in crypto-currency are also subject to anti-money laundering laws and therefore have to be compulsorily registered with Fintrac (Financial Transactions Analysis Centre).

In the United States, the country that together with China and Japan has been studying the classification and regulation of Bitcoin and cryptocurrencies for the longest time, has

been classified as a money service business (MSB), currently regulated and present in the US derivatives markets.

On the other hand, the EU has not agreed on specific regulation and legislation between its member states. The ESMA (European Securities and Markets Authority) has issued communications and warnings on investments in cryptosystems and ICOs, but this is only considered information for institutions, individuals and companies. Some European countries have already developed their own view on cryptocurrencies: some issue favourable opinions by their regulators and others have banned them. A third group is distant and indifferent, although some of them issue warnings and alarms. This is the case in Spain and the Press releases (CNMV, 2018a) and Considerations (CNMV, 2018b) issued by the Bank of Spain and the CNMV (National Chamber of the Securities Market) on the use and possible risks derived from their characteristics as financial products not regulated by the supervisor.

Special mention should be made of Japan, which has regulated and authorized Bitcoin as a legal means of payment, although not all other crypto-currencies; and Venezuela, which apart from being in the final part of the process to legalize and use Bitcoin as a legal means of payment, has published and publicized in different media (El Pais, 2018) the launch of its own currency, "Petro", as the state's crypto-currency, backed in its value by the country's crude oil reserves[14].

It must be said, however, that Petro took a long time to have its Blockchain operational and it does not seem that it will have it fully operational in the short term. Given the Venezuelan government's silence on this matter, we understand that, before putting this idea into practice, someone suggested that there might be certain incongruities and inconsistencies with the objectives and red lines that the “socialist” government cannot or is not willing to overcome. But they nevertheless went ahead with their idea, design and the ontology that defines it in their founding document.

[14] https://www.petro.gob.ve/files/petro-whitepaper.pdf

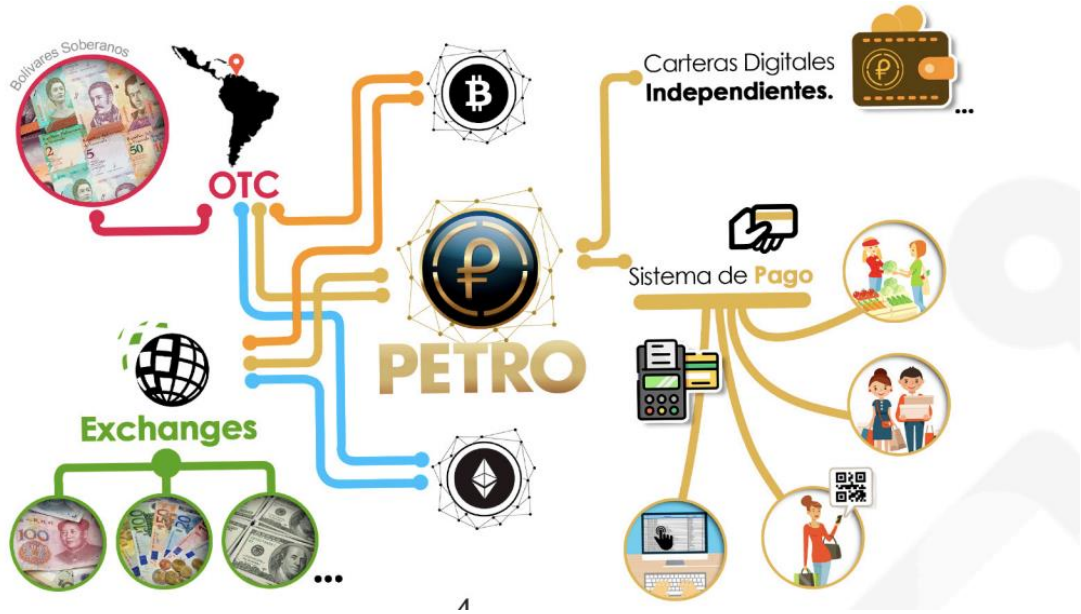


Figure 3. Diagram of "Petro" operation. Source: https://www.petro.gob.ve/files/petro-whitepaper.pdf

The problem of Petro, which they designed and made known and one day without further ado disappeared from public life, is easy to understand on a theoretical level. It is unthinkable that the wealth of this country could support the currency due to an infinite number of factors: hyperinflation, warnings and threats from other supervisors and regulators, political disunity, inconsistency between their wealth data and the data from the WTO (World Trade Organization). However, the main factor, and one that is directly opposite to the objectives and economic policy of the Venezuelan government, is that, as has been explained by Petro, it is a cryptocurrency that is backed by the value of a barrel of Venezuelan crude, from the reserves held by the government itself. This would not be at all strange, since different cryptocurrencies (or in this case it would be more correct to call them cryptoactive) such as Xaurum or DigixDao, from the Ethereum network, are backed by gold.

In the specific case of Petro, if this support were effective, it would in practice mean the privatization of the existing crude oil reserves in Venezuela. It is something that the "socialist" government could not afford in any way or with any conditional element. It goes against its founding ideals and all the policies and ideological values shown so far, is to privatize and cede to foreign capital, the policy on the country's natural resources. That is why, even though it has had an effective launch and acceptance among the first group of pensioners and public officials with whom it has been tested with two donations of half a petro per user ($40 at the price to which they have it subject). In practice, it is

only a sort of parallel government currency (as opposed to the bolivar which is their official currency) to try to curb the highest inflation in the world. They only change the monetary platform, because the acceptance of the use of the cryptocurrency must continue to depend on the trust of the economic agents on a voluntary basis, otherwise it can only be effective at the local level. The post-Chavez regime in Venezuela has turned it into a practical laboratory at the social and economic level. The problems of general lack of supply that the country is experiencing also condition and increase the technical and operational inconveniences.

The governments' greatest fear of cryptocurrency, according to our research, is related to pseudo-anonymity and complete anonymity. To that effect, cryptocurrencies and their underlying technologies have already proven to move huge amounts of money with tiny commissions and with little or no trace. This would end the problem that many professionals, individuals and entities have to move capital or send money between countries, since the Internet is decentralized and its operation is global, unless a government regulates Internet access (as happens in China or North Korea).

The problem, again, is in the first idea itself. if these movements were to escape state control they could destabilize both the GDP of the countries and the tax collections and levies applicable to current financial movements. This is something that states will clearly try to legislate against and prevent from happening, as they would lose control over the country's taxes and sovereign monetary and financial policy, which would affect the administration of the country.

4. Success model Vs Failure model

Next, we will establish as a result of our research and analysis, a comparison in what we understand as two different models of starting up a project, related to cryptocurrency. In this case, with two different cryptoactives, we have gone to two tokens, individuals, with a clear financial vocation and in which the willingness to invest was the key to success and the correct development of the token and cryptoactives themselves.

The first, TaaS: this is what we would call an Erc-20 token, a token that is marketed and supported by the Smart Contract network and the Ethereum blockchain, the second, Bitconnect: it’s a cryptoactive, with its own blockchain, its own token (BCC) and its own platform for change.

4.1. Success model (TaaS- Token as a Service)

TaaS is a type of cryptoactive, which was born through an ICO, as one of the first tokens of the Ethereum network, mounted on its contract network. The possession and holding of this token gives you the right to receive a percentage of the benefit obtained in a four-month period by the investment fund. It is the first large operational investment fund created in the world of cryptocurrency and operated exclusively with cryptoactives for cryptoactives.

Incorporated from Singapore, in February 2017, Token-as-a-Service (TaaS) is a closed-ended, cryptoactive and "tokenized" investment fund that actively contributes to the development of the blockchain ecosystem. The owners of the TAAS token take advantage of the booming blockchain markets without having to deal with the obstacles, risks and technical barriers associated with the ownership, transfer and trade of cryptosystems and tokens.

TaaS concluded its sale of tokens (ICO) on the 27th of April 2017, which lasted one month. The results were independently verified by a world-renowned accounting firm, Grant Thornton: the sale attracted 3,942 participants who contributed $7,569,371.61 or equivalent (other cryptocurrencies).

As a result of the sale, we observed that 8,146,000.78 tokens were distributed, while the rest of the 101 million tokens initially put up for sale were burned. The price of the tokens (including bonuses) during the sale varied from $0.8 to $1 / TAAS. The maximum price that was paid for a TaaS token at the ICO was $1, which is the value we will take as a reference, in this article.

The TAAS tokens are based, according to our study, on a smart Ethereum profit-sharing contract, which offers token owners 50% of the quarterly profit. The 25% of the capital gains is retained to increase the capital fund without requiring additional token sales. With its consequent capital increases accompanied by more disbursements, the system or idea with which TaaS is born, is to be viable and to be able to grow as an independent platform without external interferences. And the 25% of the remaining profits are the remuneration assigned to the fund managers.

The main premise is that the gradual increase in the net asset value increases the value of the token over time and, therefore, the token is explicitly linked to the performance of its parent structure. The best feature of TaaS is its transparency, audited by the well-known auditing firm Grant Thornton, which offers a guarantee of transparency that ensures its

viability and legality, as well as a system of annual reports, in which they unravel and explain each movement made for the knowledge of their investors and token holders. This guarantees the proper flow of information and the veracity of their operations and results. In the 4 quarters, under our monitoring, that the platform (the investment fund) was in operation and distributed dividends, its benefits, audited and already delivered, have been the following:

TaaS Dividend: Saturday, May 12, 2018
Total Benefit: $266,937.27
Total Payment: $133,468.63
Payment per token TAAS: $0.01638456 USD
Payment by token TAAS: 0.00002400 ETH

TaaS Dividend: Saturday, February 3, 2018
Total Benefit: $22,201,139.77
Total Payment: $11,100,569.89
Payment by token TAAS: $1.36270000 USD
Payment by token TAAS: 0.00122619 ETH

TaaS Dividend: Saturday, November 4, 2018
Total Benefit: $5,470,784.75
Total Payment: $2,735,392.37
Payment per token TAAS: $0.33579577 USD
Payment by token TAAS: 0.00108020 ETH

TaaS Dividend: Monday, August 7, 2017
Total Benefit: $4,623,111.61
Total Payment: $2,311,555.81
Payment per token TAAS: $0.28376572 USD
Payment by token TAAS: 0.00140665 ETH

Investing at the time when it was more expensive to acquire the token in the ICO, only with the dividends. We would already be obtaining a benefit of double the investment (2

$), despite these dividends, and the future dividends obtained would have to be added to the intrinsic value of the token. In July 2018, with a value of more than $2, represents, if we decided to sell today, an accumulated profit of $2 in dividends and $1 in profit, adding value to the token price, i.e. a 300% return in one year. Although these figures are excellent, at certain moments they exceeded the token's price, profits and returns of more than 1200%, as can be seen in the graph below.

Graph 1. Chart on the evolution of capitalization and price of TaaS token. Source: coinmarketcap.com

Any additional information you want to expand, can be found publicly in the Annual Report that the TaaS Foundation makes in collaboration with Grant Thornton.

The decision-makers recently decided to terminate the TaaS' project. By means of a publication in their usual communication channel, they explained the cessation of activities, as well as the liquidation of the remaining funds available to the company as equity. After auditing the remaining funds, they amounted to 10.77 million dollars, which were distributed proportionally among the token holders.

4.2. Failure model (Bitconnect)

In our analysis, and based on the following model, we will use the example of Bitconnect, a cryptocurrency/cryptoactive, which was placed in the market with a total market capitalization of 2.6 billion dollars, in early January 2018, and always present in the TOP20 ranking of crypto-currencies with the highest capitalization during 2017, to show how a scam, in this case a pyramid scheme or Ponzi scheme, develops.

This is what Bitconnect proposed:

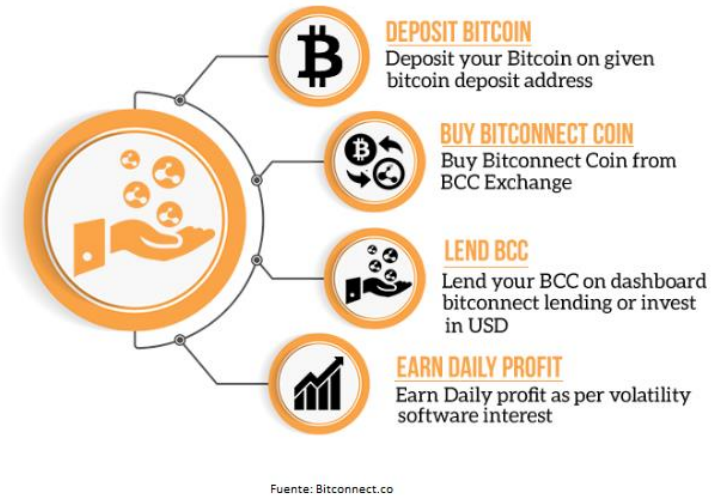


Figure 4. Publicity on the scheme of its theoretical financial functioning. Source: Bitconnect.co

Bitconnect marketed itself as a crypto, with its currency/token the BCC, coupled with its blockchain and exchange platform for its community. Open source and with its own platform, it offered different methods and forms of investment, especially related to the conservation and possession of its cryptocurrency and to carry out transactions in BCC.

However, without more information and more tangible data than the images, the first thing they ask you to start obtaining your interests and your benefits, without any data of proven success, is that you enter your bitcoins. At the time of the birth of Bitconnect (January 2017), the bitcoin is around $900 per unit. This is more than twice as much as in January of the previous year (2016). Therefore, it already has a proven track record and plausible success: after a long period of decline, its price has taken off again.

According to what you can see in the images extracted from their website (still active), shown below, the returns they offered were beyond all logic and how strange it really was that, unlike our previous model of proven success, there was no reference to how they would obtain that benefit. In fact, the opacity was a shadow that hovered over their existence from birth.

Duration	Interest
1st 6 months Jan 2017 to June 2017	60% (10%per month)
2nd 6 months July 2017 to Dec 2017	50% (8%per month)
3rd 6 months Jan 2018 to June 2018	40% (7%per month)
4th 6 months July 2018 to Dec 2018	30% (5%per month)
5th 6 months Jan 2019 to June 2019	20% (3%per month)
6th 6 months July 2019 to Dec 2019	10% (1.4%per month)

Fuente: Bitconnect.co

Figure 5. Advertising the interests that a Bitconnect token would bring. Source: Bitconnect.co

Another example of the interest and "guaranteed benefits" they promised financially as a claim:

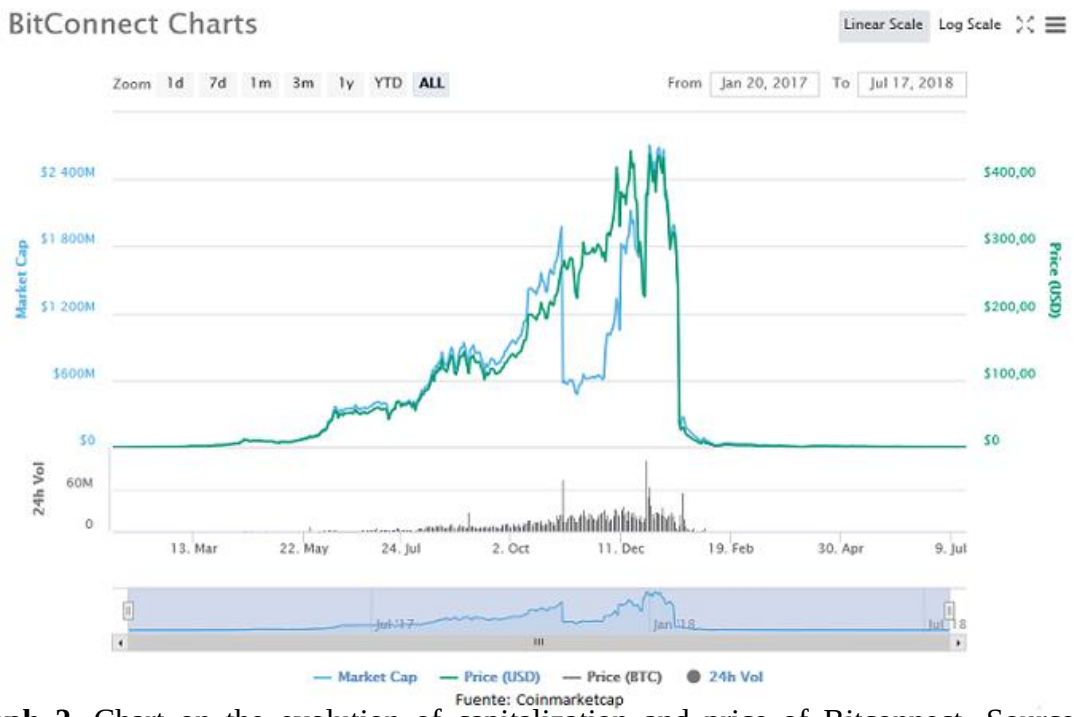
Lending Amount	Interest (Accrued Daily)	Capital Back
$100 - $1000	Volatility Software Interest (up to 40 % Per Month)	After 299 Days
$1010 - $5000	Volatility Software Interest + 0.10% Daily (up to 40 % Per Month)	After 239 Days
$5010 - $10000	Volatility Software Interest + 0.20% Daily (up to 40 % Per Month)	After 179 Days
$10010 - $100000	Volatility Software Interest + 0.25% Daily (up to 40 % Per Month)	After 120 Days

Fuente: Bitconnect.co

Figure 6. Advertising the benefits of token ownership. Source: Bitconnect.co

In January 2018, based on our investigations and follow-up, we detected, in response to several requests from different regulators, contrary rulings and various rumors that placed Bitconnect as an example of a pyramid scheme. In this case, several regulators warned consumers and required Bitconnect to cease its activities in its area of law immediately. The ruling of the U.S. Court in Texas was devastating. Its price plummeted, and the cryptoactive sank, in a succession of falls with a cumulative value of 98% of the value set on January 7th at $420 per unit. At the end of the month, its value was reduced to $7 per unit. In March, the value of its quotation, without any doubt a pyramidal fraud, already ends up at cents, which is the value it is trading today, with a zero volume of trading and only exchanged in a single marginal exchange house (of very little use and volume) that still supports and allows exchanges between the token (BCC) and other crypto currencies.

Here we can see the graph we have recovered, of the dollar quotation and the total market capitalization of Bitconnect since its market launch and its beginnings, until July 2018.



Graph 2. Chart on the evolution of capitalization and price of Bitconnect. Source: coinmarketcap.com

The main thing we can extract from the Texas court ruling, in order to recognize and point out a Ponzi system and its generic "modus operandi", would be the following:

"BitConnect has disclosed virtually nothing about its principals, financial condition, or strategies for earning profits for investors. It has not provided a physical address in England.

Despite providing no information on how it will make money for investors – including the algorithms behind the Trading Bot – BitConnect is touting its investments as a "safe way to earn a high rate of return."

Investing in cryptocurrencies, however, carries significant risk because of regulatory and legal actions, competition from other cryptocurrencies, and the extreme volatility in the price of many cryptocurrencies."

[…]

"The company operates websites and deploys online advertising to recruit sales agents, which it calls "affiliates." The company provides marketing material to affiliates, including online presentations, and pays them commissions for referrals that result in investments in BitConnect programs.

Sales agents for BitConnect are targeting Texas residents, as well as residents of other states, through websites, social media, and online marketplaces like Craigslist[15].
The sales agents are not, however, registered as agents of BitConnect to sell securities in Texas.".

5. Conclusions

According to our research and assessments, a multitude of reasoning and variations could be correct in the predictive development of our object of study, even contradictory. This is something logical and reasonable from the point of view of the knowledge or understanding of the subject, which the interested party has, all are subject to the generalities of human nature. The interest aroused by this market is produced by people who have a greater degree of knowledge in the subject. Like all new inventions, it is subsequently democratized and becomes accessible and awakens general interest.

From our experience, we liked to stress that we were not very sure who was more radical in their defense of their ideas and theories, but we did see clearly who was playing the role of "victim" and at the same time playing the role of "executioner". In order to justify what was unjustifiable, and to dress or provide logic, coherence and consistency, that which did not meet the conditions for accepting these characteristics.

Although from time to time in the area of contempt, people also enter with little rigour, both in terms of technical knowledge and more general knowledge of economics and sociology. In this article, we compile the main characteristics and various examples that demonstrate why we are faced with a new paradigm, which could revolutionize the economic world in all aspects if it were implemented. For this reason, it deserves both our maximum mental openness to assess and investigate it, and our respect when it is taken into account and studied. Giving answers to the questions that arise: How? When? Why?

We carry out a pioneering research in its genre to investigate. It is something that has just been born. It is something strange but cryptocurrencies are an exciting social scientific experiment, and surely the most important at a sociological level of all those experienced since the birth of the Internet, since it directly affects the entire political economy. The

[15] Craiglist is an American website of classified ads from different sectors (employment, housing, commerce, etc.)

Internet is the greatest sociological invention in history after language and money itself. Nothing has changed and it has meant so much on a sociological level for human beings, only language surpasses it in importance on a historical level because it was the origin of the main tool we have as human beings who are part of a collective mayor. It closes distances, information content travels at the speed of light, makes us all more capable and offers us facilities. A factor that also occurs in the currencies we use; all of them are not personal (common to all).

From an empirical point of view, today, despite the observation of facts and our acquired experience, we can neither deny nor affirm that cryptocurrencies and their adjacent technology are a new paradigm. But we do have enough indications, studies and patterns that make us glimpse the possibility that we are facing a possible change in finance at a global level. The Economist, already awarded in 2015 to Satoshi Nakamoto, with the annual prize for innovation granted by the magazine, for that potential that his invention would have, to change finance at a global level. It is something that could happen, or not. We are faced with a dilemma similar to that of Schrödinger's Cat, until it happens and time passes, we cannot have any certainty.

This research, in one of its lines would point out that Bitcoin and the cryptocurrencies could be a bubble and if this were so, it will end up like all bubbles, but it could also break the money paradigm and establish itself as the new exchange and reserve unit of international value, offering that divergence of potentiality. This would require the confidence of individuals (users and consumers) and the continuous and consistent technological developments necessary to maintain its modernity. In the same way, it could be, as in the dotcom bubble, that it is not Bitcoin, but another cryptocurrency or another cryptoactive that will prevail as the dominant or successful digital currency in the near future. That there are other projects and other companies related to the blockchain that will end up succeeding in the medium or long term.

If we manage to identify that after many advances and years of technological disruption, we are now facing a new paradigm for money. We will have to understand and value that this money is now in a different medium. Following the simile with which we started this research, if money was the message and content and language were the medium, today, we have taken money out of the medium, to digitalize it and adapt it to our personal circumstances and to this new medium through different communication networks and people connected to each other.

What can we deduce from this and from the research work and content of this thesis? Because of our contrasting experience and the analysis of the most important experts who can be called upon thanks to Bitcoin and the other cryptocurrencies based on the blockchain. Today we could do things and make financial, economic and accounting movements that we could not do a few years ago. There wasn't even an idea that was well thought out and structured enough to be put into practice, to be able to execute and carry out, what we can do today and put into practice.

Therefore, we conclude that really and plausibly today. It already provides us with enough progress, enough technological and economic and monetary novelties to be able to say that, despite the fact that we cannot guarantee its successful implementation, or what it represents as a new model, since it is not something trivial. It covers the whole range of transactional operations, providing new solutions and possibilities for action, which did not exist before, that is, re-establishing new economic and financial paradigms, in the highest sense of the word.

Based on our study, analysis and research, we have to conclude and based on what we have described in the thesis through different phases, processes and particularities of these digital currencies and this digitalization of the economy. In the face of the questions: How would governments react? The markets? What options do they have? And the people who make up societies? And will societies themselves, as the guarantors of the well-being and good development of their living organisms, be able to adapt? As we have already seen throughout the article, many aspects must be taken into account when assessing and describing the being of this new object we are dealing with.

The three main possibilities of application of the DABT to glimpse a new model that breaks into any of the previous paradigms. These would be its three possible ways of being established, such as:

- Means of payment and/or monetary unit (which would redefine the economy as we know it)
- New dominant form of enterprise, that a tokenization is applied to the form in the business participation (as we have seen with different examples in this thesis, this would redefine the business science as we know it)
- That the countries assume the tokenization of their own economies, to establish more control or to give more freedom to the economy, propitiating less interventionism (which

would again redefine the economy and would be the replacement of double-entry accounting and financing through the state's external debt).

REFERENCES

$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales | Texas State Securities Board. (2018). Texas State Securities Board. https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales

Becerra, C. (2020, 30 enero). *El petro venezolano: una ilusiÃ³n y una moneda de chocolate*. El País. https://elpais.com/internacional/2020/01/29/america/1580332251_431554.html

Bennett, N. and Lemoine, J. (2014). What VUCA Really Means for You. *Hardvard Business Review*, 92(1/2)

CNMV (2018a). *Comunicado conjunto de la CNMV y del Banco de España sobre "criptomonedas" y "ofertas iniciales de criptomonedas" (ICOs)*. CNMV. https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf

CNMV (2018b). *Consideraciones de la CNMV sobre "criptomonedas" e "ICOs" dirigidas a los profesionales del sector financiero*. CNMV. https://www.cnmv.es/loultimo/comunicadoCNMV_ICO_ES%20final.pdf

ECB (2012). *Virtual currency schemes*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Heidegger, M. (2002). Serenidad. Barcelona: Ediciones del Serbal.

López Gonzaléz, E. (2021). Hic Sunt Leones: The Future of Money. On the digitalization of the economy". Speech at the entrance of the Royal Academy of Economics and Financial Sciences as Corresponding Academician for Castilla y León.

Maduro, N. (2018, 3 mayo). *Nuestra democracia es proteger*. El País. https://elpais.com/elpais/2018/05/01/opinion/1525190756_964649.html

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260

Otero, G. J. M. (2022). *Bitcoin. La moneda del futuro: Que es, como funciona y por que cambiara el mundo (Dinero, Banca y Finanzas)*. Union Editorial.
US (2014). http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

Wei Dai. (1998). *b-money*. http://www.weidai.com/bmoney.txt.