UNIDAD EDUCATIVA PARTICULAR JAVIER

BACHILLERATO EN CIENCIAS

MONOGRAPH

"Cryptocurrencies the new virtual money"

STUDENT:

Nicolas Ribadeneira

ADVISER: LCDO. Mauro Mackay

THIRD OF BACCALAUREATE - COURSE A

2017 – 2018

Gratitude

I thank God mainly for giving me the understanding and desire to carry out this theme. To my parents, Rosita and Wolfio, who support me day to day, so I can fulfill my goals and who have trained me as a capable and independent person with values such as perseverance and integrity. To my teachers who guided me in the best way for doing a good job, and finally to the people who collaborated with this work through surveys or interviews.

Summary

The author has chosen this topic because he wanted to analyze the social impact of cryptocurrencies and if this type of currency could be used like a local currency in a country. He started searching what is the real definition of a cryptocurrency, how they were created, and how do they work.

Cryptocurrencies aren't controlled by a government institution, so he will find what are the things that make cryptocurrencies a currency that people can trust and change their earnings to that electronic money.

Also, he will find what type of informatic software do they use to manage cryptocurrencies and trade them with different people around the world. The author at first researched how do cryptocurrencies are generated and who are the people in charged of doing it. It will be shown what do people think about cryptocurrencies and if society trust in them and in what percentage.

The word cryptocurrencies take more popularity with the pass of the days, everyone that has a YouTube application in his or her cellphone should have listened to that word, because of publicity that people do in that social network.

People now a days also is viewing an opportunity for earning money in cryptocurrencies, some people think that one day its price will rise again and that's why they are using them as a business opportunity that gives people great earnings.

This investigation work has the purpose of looking forward to the future of the world economy and view its advantages and disadvantages, if it exists a possibility that cryptocurrencies could improve economy in some countries that are going trough serious crisis and it could be a exit for people that need economy help in some countries or even

continents. Finally, to get to a conclusion where every of the previous aspects has their own answers and come to an end.

Index

page

INTRODUCTION

The present task is a research work on the impact generated by cryptocurrencies in the economy since its first appearance and its purpose is to analyze what will be accepted in the future by society and state governments, through surveys that will give us an approximate statistic to the knowledge of the people on the subject.

The cryptocurrencies are a type of decentralized currency that was unveiled in 2008 with the nascent Bitcoin, which from that moment had an unexpected positive increase in its value and now it is debated whether it should be implemented in governments as the local currency of each country and open the way to a new world economy.

Every day more types of cryptocurrencies are created (among them the famous Bitcoin and others such as Ethercoin, Litecoin, Monero, Dash and Maker among the valued ones) and these increase their price according to the number of people who use them, as happens with traditional currencies, the more people use them the more their value increases and vice versa.

Nobody knows with certainty the origin of the first cryptocurrency but it is clear that the inventors of this informatic system knew that they will probably change the economy in a not too distant future.

The cryptocurrencies work thanks to a system called blockchain, which allows any user to exchange this currency with the person you want worldwide.

Those in charge of working in cryptocurrencies are called miners and they have the task of recording every transaction that is made with each cryptocurrency and in this way creating a block in the blockchain. In other words, it is thanks to this system that you cannot exchange ghost cryptocurrencies or perform any illegal transaction or movement, and you could say that they are the "police" of the blockchain.

Chapter I

Introduction to cryptocurrencies

1. Introduction

1.1 What are cryptocurrencies?

Cryptocurrencies are a type of virtual money that can be exchanged and operated like any other traditional currency, since they are decentralized they do not need a mediator such as a government, a bank or any financial institution, but they depend on the supply and demand that society gives to them, as long as people use them, they will last.

Cryptocurrencies are a type of digital money that works independently from a bank, they are based on cryptography (it is the study of information encryption methods to send a message in a safe and private way) and to confirm purchases that are sent or received. One of the main purposes of cryptocurrencies is the freedom of privacy rights in which everyone decides what to do and what not to do with their money without being controlled by your local financial system.

Is very important to know that cryptocurrencies could be changed in an anonymous or not anonymous way, but this action is necessary to be registered in a data base to have the constancy that the cryptocurrency has already used, and it cannot be duplicated, as experts says, "cryptocurrencies are a good way to preserve intimacy of people online…" (Richard

Stallman, n.d). These works under a mechanism called "Peer-2-Peer" (P2P), it is a data base system that keeps a record of all transactions that have been made with that cryptocurrency indicating the amount, date and time of the transaction. This data cannot be changed or altered because if someone wants to do it the P2P system doesn't allows editing the information in every single computer of people that works on it all around the world, if someone changes the information in one computer, it will remain unedited in the rest of databases that other users have. This is to make the entire web transparent and without secrets or cheating.

There are authors that say that:

> The cryptocurrency project produced great uncertainty, not only because the name of its creator was unknown, but also because when encryption through open codes occurred, anyone had access to them, causing other users' protocols that could modify the software and produce a fall on the system. (Almarcha, 2015, p. 26)

Nowadays there are already several types of virtual currencies and it has been shown to the world that they are getting more and more accepted in society, as both large and small companies have been started accepting them as payment methods and their value increases more and more with the passing of days.

It is necessary to understand them as a monetary system, that is, they do not have a value because of the material they are made of or because of their physical usefulness. The way in which a currency defines its value is in accordance with its importance in the market, while more people are interested in buying its value will go up and vice versa, as well as in an auction.

Winklevoss brothers, owners of the 1% of all the bit coins said that:

> Our first impression was that this could be great or a completely cero. Immediately we were captivated by the elegancy and the big challenge of bitcoin, and when we started learning more about it, we got convinced that cryptocurrencies were the future of money
>
> (Winklevoss brothers, n.d)

An important fact about what impulses people to get or buy cryptocurrencies is that there is no way to hack or steal them from the owners, like it happens with physical money or credit cards, you only must save them in a "e-wallet" with a password and no one will know how much you have or even the name of the owner person. That is another point in favor of cryptocurrencies if you compare them with a credit card or physical money.

1.2. Cryptocurrencies origin.

Throughout history there have been various types of coins for making commercial exchanges, many of them are still being use today and others have disappeared for different reasons.

Cryptocurrencies origin dates to the end of the 90s, when in a computer congress came up the idea of using cryptography in a monetary system that every kind of people could use without being subject to governmental regulations of banking systems and so not depend on them.

Currently there are more and more areas that are being linked with technology. In 2008 we met a rising type of currency called cryptocurrency, which appeared with a document published by Satoshi Nakamoto in which he explained how will "Bitcoin" works, and in that moment the first cryptocurrency was presented to the world. One of the biggest unknowns that exist about bitcoin is the unknowledge of its creator. We know the name of Satoshi Nakamoto, but nobody knows if it is a person, a group of people or a pseudonym.

Experts say that:

> The only thing that Satoshi Nakamoto have done is to stablish the rules, that developers had to follow, but without letting them control his work. So, the mission of knowing the creator original name is as uncertain as knowing who built fire for the first time
>
> (Almarcha, 2015, p. 26)

1.3 Why are they called cryptocurrencies?

The cryptocurrencies are called that way thanks to their encrypted nature that is protected through coding. The characteristic that makes it a very attractive monetary system is that it is difficult to change or hack or because it is not controlled by a bank or a government institution, so you don't have to public your personal information to use them. With traditional currencies each transaction must be approved by a banking institution, instead cryptocurrencies choose to use a decentralized transaction system known as a blockchain.

A lot of important people around the world has got caught with the word cryptocurrencies and they are talking in favor of it, "This will change the offer and demand equation. It is that great. It will not surprise me in absolute that bankers, financiers and Saudi princes are joining against this. It is a very disruptive technology" (Mark Yusko, n.d)

Chapter II

Cryptocurrencies the coin of the future

2. Cryptocurrencies future

2.1 Cryptocurrencies worldwide impact in society and economy.

Surely everyone remembers various crimes related to fraud, bankruptcy or fund misappropriation in public and private sectors. All these acts have in common the concentration of decision making from a person or institution, which is enriched at the expense of others and continues doing those things to not lose all this wealth.

This is a clear example in which centralization generates significant disadvantages, because when we corrupt this single entity, the entire system is affected or corrupted.

As an expert mentioned:

> Then it was presented an alternative to traditional currencies, which had been devaluated enough due to financial crisis, and cryptocurrencies started becoming a new digital system, that provides you the choice of safeguarding your capital and not be affected by future consequences
>
> (Cryptocurrencies advantages…, s.f., párr. 7)

Now we know that cryptocurrencies are becoming more popular every day because in some cases they are some people's life solution.

2.2 How does cryptocurrencies work?

When someone makes a purchase with a type of world currency, we already know that there are three or more people intervening in this act: the buyer, the seller and the central bank of

the state that issues the money. The bank would be the main issuer here because thanks to this, people have the possibility of making purchases because they are in charge of making physical money or providing credit or debit cards to people.

We already know that cryptocurrencies are decentralized, so they do not need the evaluation of any institution like these, but the question we will ask ourselves is: How is it that cryptocurrencies are so well managed if there is no financial institution controlling them?

According to Cryptocurrency experts: ¨…works a lot like bank credit on a debit card. In both cases, a complex system that issues currency and records transactions and balances works behind the scenes to allow people to send and receive currency electronically¨ (Cryptocurrency facts, 2017, párr. 1).

The cryptocurrencies have a system known as blockchain which involves many people who may want to make a transaction, others who verify transactions or those who are in charge of generating new cryptocurrencies. This system is transparent and guarantees that no cryptocurrency is going to be duplicated or people try to swindle with this.

2.2.1 Blockchain.

What is the blockchain? The blockchain is the software that controls the cryptocurrency, this provides a network of computers the opportunity to maintain a collective accounting through the internet. This accounting is neither closed nor controlled by any individual or organization, instead it is public and available in a digital ledger which is distributed and replicated around the network.

In the blockchain all transactions are blocked including information regarding dates, times, participants and volumes of each transaction. Each node in the network contains an identical copy of the complete blockchain.

A lot of experts in economy say that: “The Blockchain is a chronological record of transactions agreed by all users and therefore can be used to avoid double spending, that is, to prevent someone from transferring the same token twice” (Blockchain system…, 2010, párr. 4).

In the bases of the mathematical complexes the transactions are verified by the members called blockchain miners. The mathematical principles of the blockchain in this way also ensure that each miner automatically and continuously validates the state of the blockchain and each of the transactions that happen in it.

If someone tries to corrupt a transaction the miners would detect it immediately and the blockchain would refuse to generate a movement, then each transaction is public, and thousands of miners automatically validate that each transaction occurs in real time and date. This is the equivalent of having a notary present in each transaction and in this way, everyone has access to a shared source of truth.

The blockchain does not care if a cryptocurrency represents some value in dollars, euros, etc. that is why each cryptocurrency is divisible up to 100 million units and each unit is individual and programmable, meaning that users can assign properties to each unit.

Through the blockchain, users can program each cryptocurrency to represent euros, dollars, shares of a company, etc. that's why the cryptocurrency is much more money and payments.

2.2.2 Miners.

> Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the block chain, and the means through which new bitcoin are released. Anyone with access to the internet and suitable hardware can participate in mining.
>
> (What is Bitcoin Mining, 2018, párr. 1)

As we already know, the miners oversee controlling the security of bitcoin in every area, verifying the transactions and validating each of them so that it is not corrupted or tries to generate false units. There are thousands of miners around the world that is why it is not possible to try to certify false transactions that are intended to be made. This works as an assembly, a law is approved or disapproved when most of assembly members vote for or against it. To make a movement, it requires the approval of the largest number of miners around the world.

At the beginning when Satoshi Nakamoto presented the cryptocurrency project and the blockchain software, to incentivize people to work as miners, they were given 50 bitcoins for mining a block of the blockchain, which can be translated into registering transactions and deciphering hashes that they are coding to protect each cryptocurrency, and as time went by, more bitcoins were going to be generated, but the reward for mining blocks every 4 years is going to go down because there is a limited number of bitcoins that can be generated which is the of 21 million bitcoins.

2.2.3 What is a hash?

When we talk about cryptocurrencies for obviously reasons we understand that they are encrypted, but this is one “simple way” to describe them.

The definition of encryption is something that is converted into a complex way so people can't see what it really looks like. Years ago, websites used encryption to keep people passwords safe so no one could enter another one's account, until they knew that hackers had the knowledge to decode this encryption technology, so they decided to stop using this technology. Basically, this is the reason why hashes were created.

What is a hash? A hash function takes an input that could be a piece of text like a password or it could be a file and it turns that into a string of text that always has the same length. There are many different hash functions available.

Hash functions are very different from encryption because they only work in one way. You can calculate the hash of a password, but you cannot take a hash and turn it back into the original data and that is an interesting property to have. By using hashes companies can verify that you're logging in with the correct password without having to store your actual password.

Now we know the definition of a hashes we could think, why are hashes so important in cryptocurrencies? Hashes are essential in cryptography because this is what miners use to create a block in the blockchain. A combination of millions of hashes makes up a block, this way miners can't know the identifications of the people that they are registering when someone trades a cryptocurrency and either the amount of that cryptocurrency those persons possess.

Also, that is why to be miner of the blockchain you need a lot of knowledge in cryptography, if the blockchain o hashes had worked differently (easily), everyone would have millions of cryptocurrencies around the world today, or trading cryptocurrencies wouldn't be safe.

Chapter III

Trading cryptocurrencies

3. Cryptocurrency storage

3.1 Cryptocurrency wallet.

A cryptocurrency wallet is a piece of software that you use to communicate with the blockchain network and then you can tell this network when you want to send and receive any transaction.

The best way to understand a cryptocurrency wallet is by comparing it to email, once you've set up an email address you need some kind of software to allow you to send a receive emails to that new address. This software may be an app on your phone, it may be an app on your laptop or it could even be an app online that you log into, with the email you enter the username and the password for your email address and you enter that into the app, and that is how the internet knows that it is really you that wants to send and receive emails to that address.

Of course you can tell everybody the email address and you have to do that in order for anyone to be able to send you a message, but just because someone knows your email address that doesn't allow them to send emails from that address for the simple reason that if they could do that it would be bad because then they could send emails pretending to be you and cause all kinds of problems. In order to be allowed to send email from a particular email address you have to know the password and if someone finds out your email password then there's nothing stopping them from logging into your email app and then sending messages and this is very similar to how cryptocurrency wallets work.

Every cryptocurrency for example a Bitcoin account has two elements: one of them is called your public address which is kind of like your email address, and one of them is called your

private key which is like your password so just like email you can give anyone your Bitcoin public address and then anyone anywhere in the world can send you some bitcoin they don't need or want to change.

Everything you need to know is the public address and you can send the money to anyone. Now your Bitcoin's private key on others hand is the one thing that you must protect, it's called your private key for a reason because you should never reveal this to anybody. Using the email example, someone gets your email password that's pretty bad because they can start sending emails from your address but that is not quite as bad as someone getting your cryptocurrency private key because they can actually then steal all of your cryptocurrencies by sending them somewhere else, and just like email once a bitcoin transaction had been sent it's a "one-way trip".

The only way to get it back will before that person to send it back to you voluntarily, so cryptocurrencies literally works like digital cash. Once you've handed over the Bitcoin belongs to that other person, and the same goes when you receive cryptocurrencies, if someone sends it to you now it is your own propriety no one can take it away from you. The only way they could do that is if they knew your private key.

"What's happening is that you'll never see the private key because the person or organization who created the wallet holds onto the private key [in the app's system] …There are advanced wallets which you can download onto your computer where you will be the only one ever who holds onto the private key.

(Fenney. What is a digital wallet, 2017, párr. 15)

3.2 Stock Exchange.

How can a coin that does not have a great nation that makes it its official currency, or an institution be supported internationally? The answer is simple: It is the people and the different uses that give these coins the ones that give them a value.

> "It had a big increase in the Christmas of 2017 when announcing amazon that accepted bitcoin for its purchases. Subsequently, there have been downward adjustments, among many things due to the threat of regulatory agents or the restrictions that China wants to impose to stop the cryptocurrencies. Beyond these recent changes in general the price of the crypts has gone up, and bitcoin for example quotes more than double than a year ago."
>
> (Peiroten. Cryptocurrencies future value,2018, párr. 9)

But there are also other factors that give value to the cryptocurrencies as the limited number that exists, for example at this time there are 12,500,000 bitcoins and there will be a max of 21,000,000. There is also a class of users who are holders who do not trade with the virtual currency but on the contrary only buy them and save it in large quantities and it is precisely this action that raises the price of bitcoin and cryptocurrencies.

An example of this was when in the past years bitcoin had a high growth in its value due to the large number of Chinese users entering the market, but when the Chinese government banned the use of the currency in that territory, it caused the bitcoin to have a great decrease

in its value. If a lot of people earn bitcoins and start saving them like their usual money, the price of them will raise like an aerostatic balloon.

In conclusion, the greed of having more and more virtual currencies increases the value of them. This happens many times with gold which goes up in price when many people buy it in order to safeguard their money but in turn increase its value.

Chapter IV

Survey statistics

4. Society opinion about cryptocurrencies

4.1 Survey applied

In this chapter, the results of the different people who carried out the survey will be analyzed. Half of the results are from people under 18 years old and the other 50% is from people over 20 years old. Obviously, there are two completely different faces and very different ways of thinking between them, and it was clearly noticed.

4.2 Kind of survey applied

-Non-probabilistic sampling

It is used to obtain an exploratory result, choosing people who meet certain criteria and in a representative manner.

- Discretionary sampling

This type of sampling is used when the researcher chooses people according to the result he wants to obtain or compare to make a contribution or confirm something in the study.

In this survey they were only 5 simply and concrete questions.

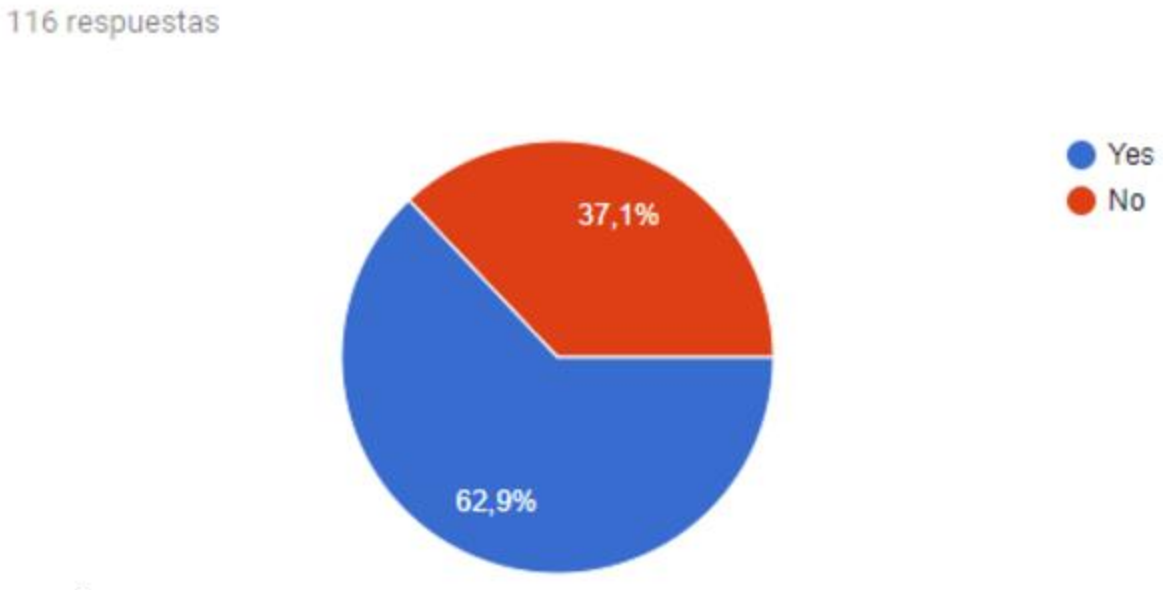

Figura 1

Have you ever heard about cryptocurrencies?

In society, lately we are talking about different areas that adapt to technology, including, as this research says, cryptocurrencies.

Clearly that people have heard this term and most people reflect it, but a part of society, most people over 40 have not heard about this issue.

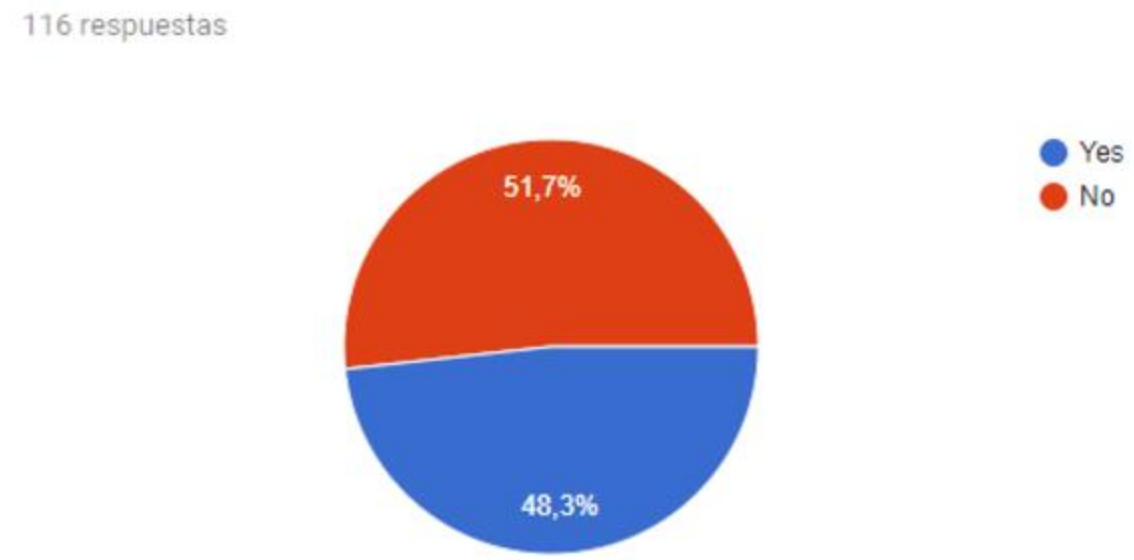

Figure 2

Would you be interested in having electronic money?

The results of this question were the ones that left me most shocked, because most people still knowing or having heard something about cryptocurrencies would not want to have them

in their possession, in summary the explanations they gave are that they do not trust this type of currency in a 100%, some religious issues, because they feel that it will devalue and then they will be useless.

As for the people who would like to have them in their power, it is because they define it as the currency of the future and they feel that soon cryptocurrencies will be very valuable and of great importance in the world, explaining that these are a step forward in the global economic sense and they would be thrilled to be able to manage them and have them in their domain.

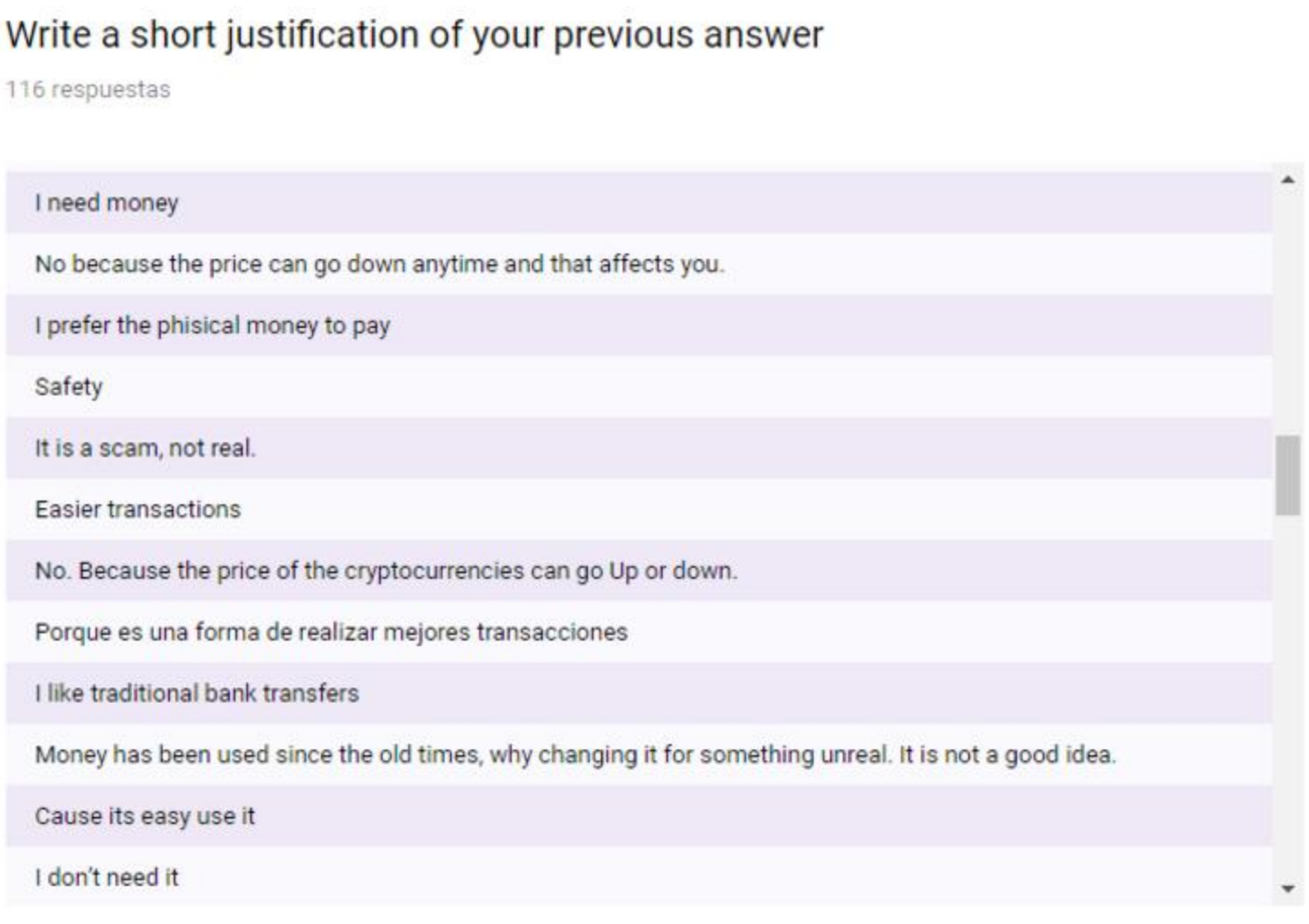

Figure 3

Justifications to previous answers

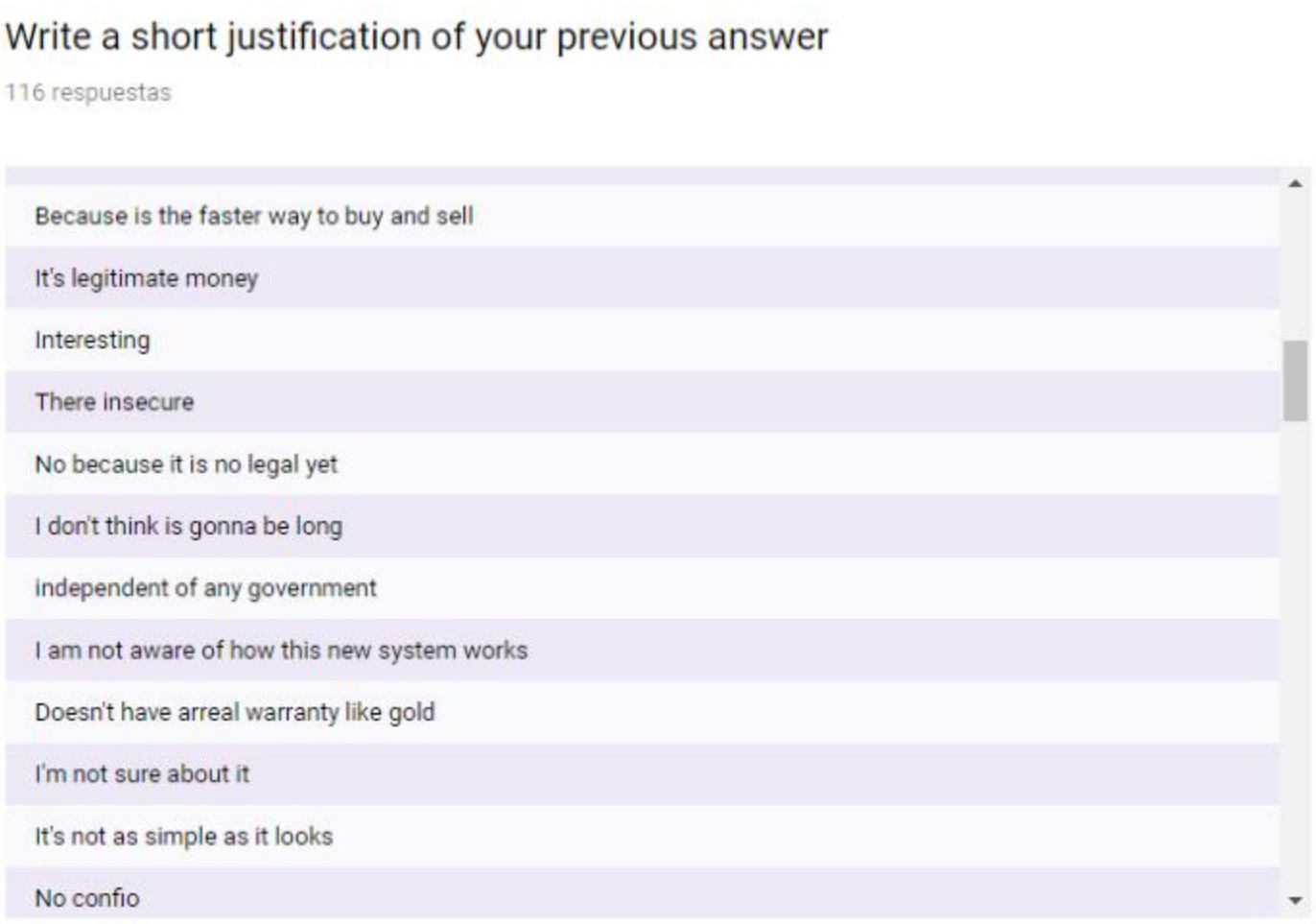

Figure 4

Justifications to previous answers

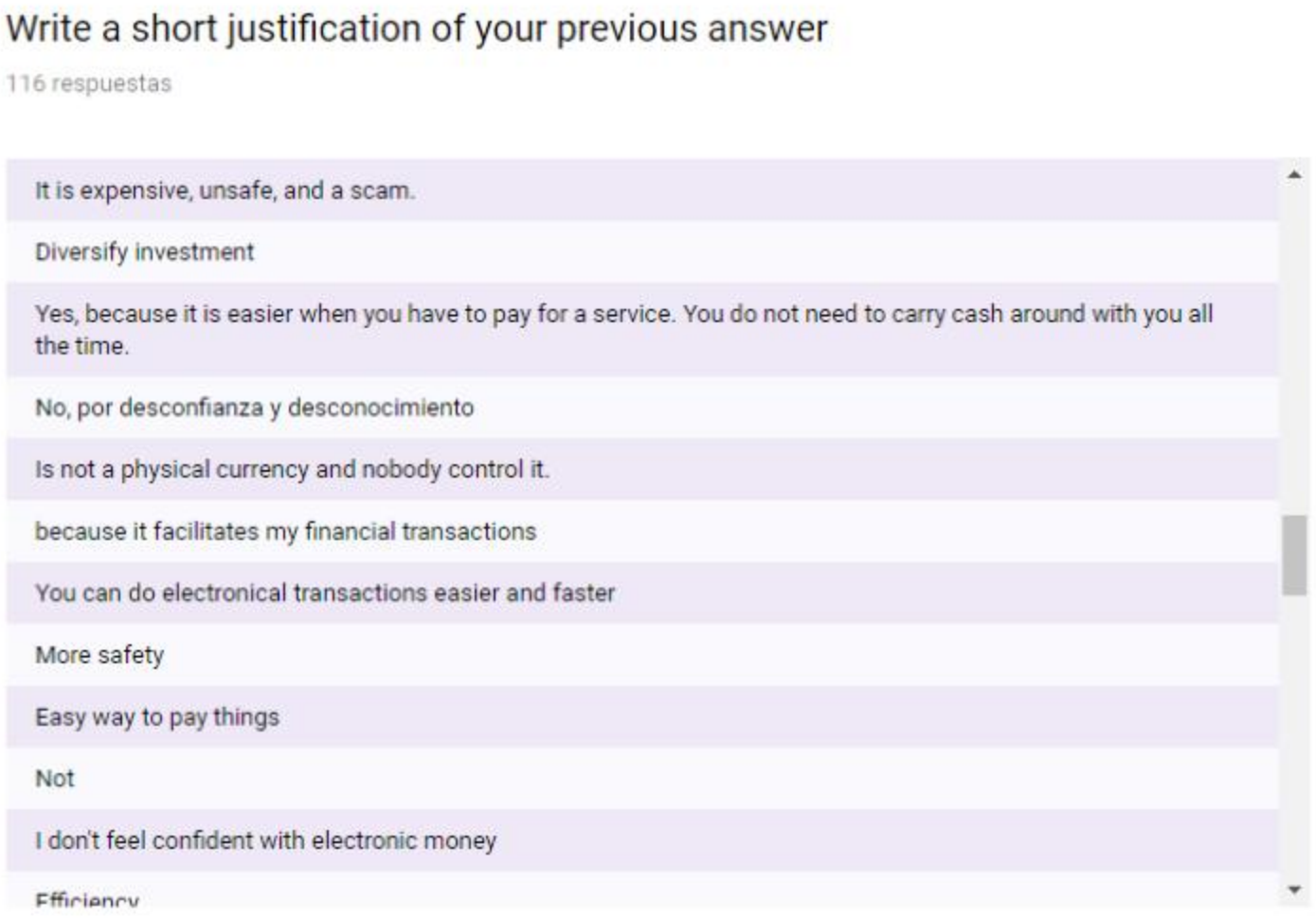

Figure 5

Justifications

Write a short justification of your previous answer

116 respuestas

I'm not interested because I prefer to use cash and debit/credit card.

Me parece poco confiable

Easey to use

Less probability of having problems when buying things

I think is the future of money

More secure

Is saver not to carry cash

The electronic money isn't safety

Investment

Because is the faster way to buy and sell

It's legitimate money

Figure 6

Justifications

116 respuestas

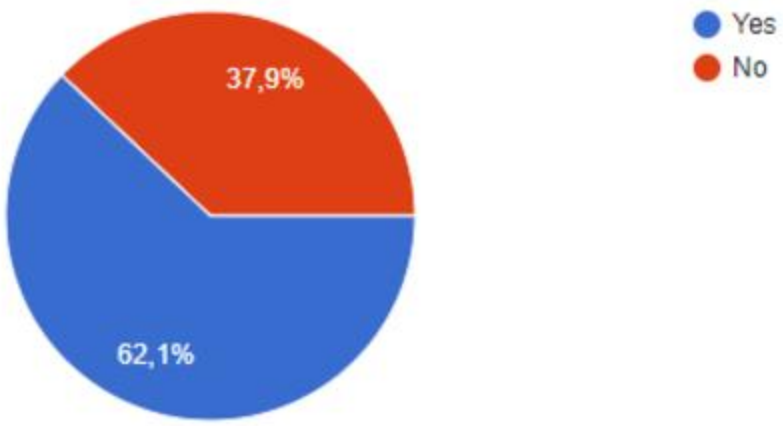

Figure 7

Do you know how electronic money works?

People tend to confuse cryptocurrencies with the electronic money that we currently use to make purchases in online stores with a credit card or a gift card. In the survey it was clearly seen that in general there are people who do not know how this type of currency work and for these reasons they did not want them, and that there are also some people who want to be able to handle them but do not know how to use or exchange them. 38% of the people who carried out this survey did not know how they work or how they can be applied in the world market, so their way of thinking will probably change if they understand them better in the future. Although some will still prefer to have their money physically as they have done all their life.

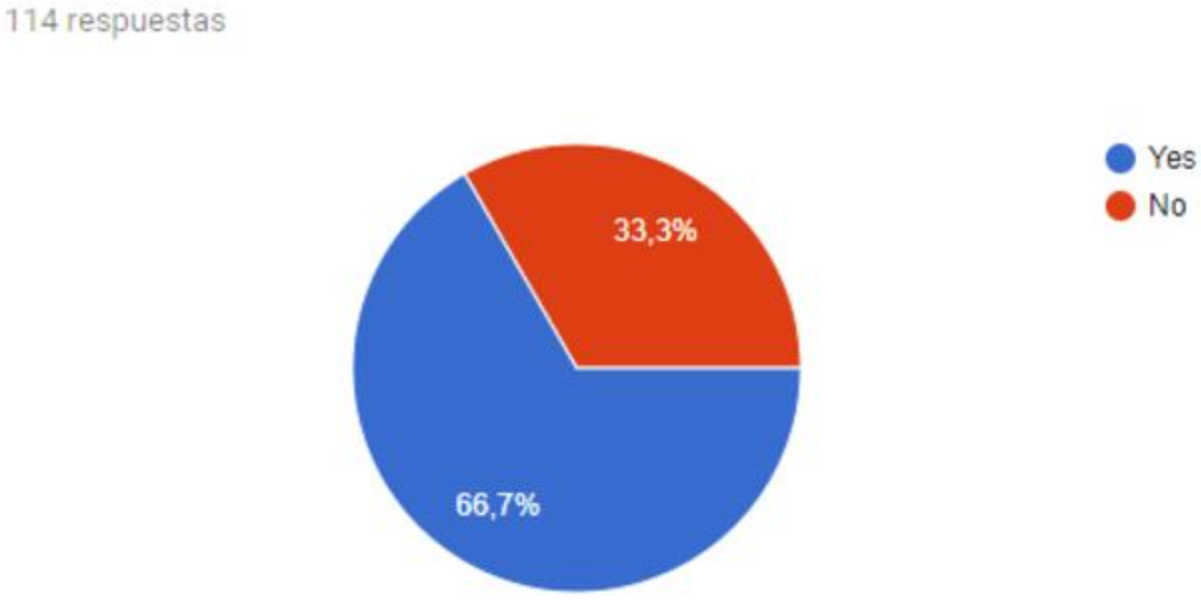

Figure 8

Do you know how you could use electronic money?

76 people of the 116 know how this type of currency could be used and this is a clear answer to the previous question because nowadays you can't buy everything you want with cryptocurrencies, it depends if the seller wants to accept them. This fact make people dislike cryptocurrencies because it will be money that you would only spend if another wants to receive it, and this also makes people distrust this system.

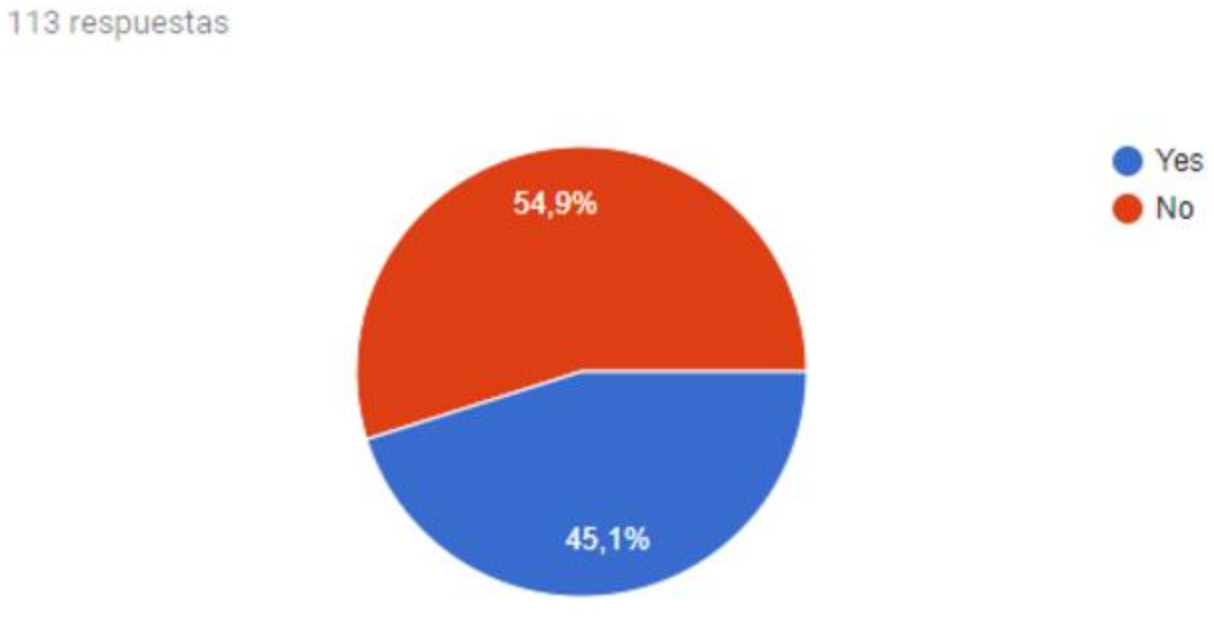

Figure 9

Would you be willing to invest in cryptocurrencies?

To finish my survey, I asked people if they would invest their money in a cryptocurrency now. of which the answer that most people chose was "no". I deduced that because most do not know how to use them or distrust their origin or how they are used then they would not be interested in ever investing, buying, or exchanging these as they think they would be useless in this country in the future or that They could devalue and lose their value and if this happens they would lose their money and investment.

Conclusions

At the end of this monographic work it is concluded that:

- In conclusion, cryptocurrencies still do not reach their "boiling point" but it is clear that they are rising little by little, and people are becoming increasingly familiar with this term. It is known that some people understand the concept of cryptocurrencies and others have only heard it, there provides the lack of knowledge of what it really means.
- The people who know them are almost 50% in agreement with them and would sometimes invest their money in this type of currency. There is another point of view that is that of people who do not agree with that type of currency and never in their lives would invest their money or change it to cryptocurrencies, because they consider that they are not safe or that they could lose their investment, but it has to mentioned that most of them do not know in depth the meaning of these.
- The term cryptocurrency causes interest in people and leads to more and more research by society, this leads some governments to prohibit the use in their countries because this type of money could be the cause of a significant devaluation in their local currency and this obviously, would not benefit them. Another point would also be that since they are decentralized, they do not have control of state authorities or any security agency, so we must be very careful when managing them, not because they could be doing something illegal, but because they could lose them and not have them back.
- To manage cryptocurrencies (exchange, spend, create, etc.) you need a certain level of knowledge informatically speaking, for some people controlling them would be easy but others would need courses to learn in their entirety how to do with them what they want.

- Some people believe that cryptocurrencies will increase its value again and that is why they acquire them and see them as an option to earn money in a long term.
- Maybe invest a part of our money would not be a bad decision when talking cryptocurrency, of course we speak of a currency that can increase its value as it can also be devalued, but if we acquire them now we could be one step ahead of society economically speaking, and as it was mentioned before, you could get great profits from them.

Recommendations

At the end of this work it is recommended that:

1. After analyzing what are cryptocurrencies in general and reaching the conclusion that they are likely to become the future of the world economy, from an equitable point of view to different ways of thinking, it is recommended that people give an opportunity to the cryptocurrencies. We do not talk about investing all your money in these but a small part of it and in case you lose your money does not cause great damage.

2. It is recommended that society at some point acquire a quantity of this type of currency because probably in the future will be universal, and then you would be a step forward than society economically speaking.

3. Another point to talk about is that to handle them it requires some knowledge of computational science or informatics, and people who want to acquire them should know it because then they could have problems when using them.

4. It is also advisable to know that it is anonymous and that if you accidentally exchange it with someone you didn't want, you will not get it back unless that person wishes to return them, so you have to be very careful because the fact of being decentralized means that it has no control of higher authorities.

References

C. K. D. L. Á., &, P. L. E. (2017-09). Tesis. Recuperado a partir de http://repositorio.ug.edu.ec/handle/redug/23667

Be2Me (2016a) ¿Quién es el creador de Bitcoin? Recuperado de http://blog.bit2me.com/es/quien-ha-creado-bitcoin/

Be2Me (2016b) ¿Qué es la Cadena de Bloques (Blockchain)? Recuperado de http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/

Maeztu, D. (2018) Aspectos legales del Bitcoin: De la blockchain a las ICO's. En: J. Valero (Coord.). Seminario del grupo de investigación iDerTec, Universidad de Murcia.

Queesbitcoin.(s.f.). Bitcoin, la moneda que está cambiando el mundo. Recuperado de https://www.queesbitcoin.info/

Telefónica (2016) ¿Qué es el blockchain o cadena de bloques? [blog]. Recuperado de https://www.openfuture.org/es/new/que_es_el_blockchain_o_cadena_de_bloques

UNIC. University of Nicosia. (2017) Academic Certificates on the Blockchain (up to Mar 2017). Recuperado de https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

BEN, Blockchain Education Network (2016) What is the Blockchain Education Network? Recuperado de https://blockchainedu.org/ben/

Herting, A. (2014) EduCoin: The Digital Currency That Makes Us Smarter [blog]. Recuperado de https://www.cryptocoinsnews.com/educoin-digital-currency-makes-us-smarter/