The Fundamentals of Cryptocurrencies

EMANUEL SOARES[1], GUALTER COUTO[2], PEDRO PIMENTEL[2]
[1]School of Business and Economics,
University of Azores,
9500-321 Ponta Delgada,
PORTUGAL

[2]School of Business and Economics and CEEApIA,
University of Azores,
9500-321 Ponta Delgada,
PORTUGAL

Abstract: - Cryptocurrencies lately are something that has been gaining notoriety as a way of creating value. This paper was a study of the due perception of Cryptocurrencies and their taxonomy and regulation and a hypothesis case of its implementation. In that regard, this study tries to separate Cryptocurrencies and Blockchains.

It also analyzed the barriers to the implementation of a Central Bank Digital Currency that is in parity with a fiat currency, even though, there isn't a real scenario where this was applied yet.

It also evaluated the gains of a portfolio of assets with Cryptocurrencies, where it is shown that it is possible to have a good portfolio with considerable returns. As for the portfolio of Cryptocurrencies, it has a return of 257,62% and a risk of 0,5424 with the following proportions, 9,7% on DOGE, 1,8% on XRP, 34% on ETH, and 54,5% on BTC, considering the criteria of maximization of the return per increment of risk.

In final regards, a suggestion of a Cryptocurrency that can solve nowadays problems in different industries, such as security and entertainment, as well as trying to answer the "Fundamentals of Cryptocurrencies".

Key-Words: - Blockchain, Cryptocurrencies, Digital Assets, Markets, Security

Received: March 27, 2023. Revised: July 6, 2023. Accepted: July 15, 2023. Published: July 27, 2023.

1 Introduction

Cryptocurrencies are a market that recently has been gaining notoriety. Currently, there is a lot of knowledge to explore including its taxonomy and regulation.

In this study, there was a distinct approach to the concepts of Cryptocurrencies and Blockchain because Blockchain is something that has evolved a lot, considering its various forms of consensus and given structure. As for Cryptocurrencies, given their growing presence in the markets, it was studied if these can replace fiat currencies.

It was important to try to perceive what Cryptocurrencies are and everything that is related. For that, it was necessary to find differences and similarities among other currencies, like Fiat currencies, as well as recent advances in technology, such as Blockchain. The objective is to try to give some common ground about these, given that this theme is still growing.

It also studied the point of view of investing in a portfolio of assets with Cryptocurrencies and their profitability. The data collected was from February 27 of 2019 to February 27 of 2021. The values obtained were positive in terms of profitability and risk, considering the volatility of Cryptocurrencies where, too, it is indicated that there is a trade-off for each increase in profitability in relation to risk. The method adopted was through CAPM, to obtain an optimal Cryptocurrencies portfolio that could justify an investment. CAPM is a model that can give a better understanding of having a portfolio of assets and its given profitability. Other models can assure a different look to investment in a given wallet, but in this case study we decided to choose the criteria of maximization of the Sharpe Ratio which gives an idea of how much is it worth investing in a given wallet compared to the risk associated with it. Other models include APT which has more variables.

The results obtained show that a portfolio of assets with Cryptocurrencies is of high value, with an expected return of 257,62 % and 0,5424 for the standard deviation. As for the Sharpe Ratio of 4,7, it determines that for each unit of risk, there is an increase in return of 4,7 which is, more than four times.

Regarding Cryptocurrencies in a social context, given the lack of control of Cryptocurrencies and their respective security, it is a bit pragmatic given the criminal activity underlying these, still, some Cryptocurrencies rose interest to investors in different areas given the number of services they produce, so they are worth not only for being a currency. Still, this paper is not meant to show that a cryptocurrency can substitute a fiat currency both have different properties something that will be studied in the paper, and, last and more important the high energy costs of mining Bitcoin make it difficult to replace the current fiat currencies. But there is the potential for Cryptocurrencies to improve society in many different areas of developers and researchers making good use of the advantages of Cryptocurrencies brought, for example, Blockchain. Such results show that even though the reality is always changing, it is difficult to ignore the impact that Cryptocurrencies have on our society, from the perspective of the investor as well as for those who are interested in developing them.

Finally, the suggestion of a Cryptocurrency can change the paradigm of Cryptocurrencies in relation to its perception and solve other problems in various industries of society, such as security and leisure.

2 Literature Review

2.1 Fundamentals of Cryptocurrencies

Cryptocurrencies have been gaining notoriety today for their versatile way of generating value. Although now their taxonomy is something that is yet to be defined, and there isn't a consensus on its legalization, they are present in several financial markets, and some of them work in different trading hours.

Currently, it is present that Cryptocurrencies can replace Fiat currencies something that will be analyzed, as well as the various strands that the underlying technology, namely, Blockchain can innovate not only the economic sector as well as other areas of science. The integration of Cryptocurrencies into a portfolio of assets is a challenge to their potential and presence in global markets.

As for the Cryptocurrencies that will be analyzed in this paper, they are Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), and Dogecoin (DOGE). As for Bitcoin (BTC), it was the pioneering Cryptocurrency developed by Satoshi Nakamoto in 2008. Some Cryptocurrencies may serve as a means of exchange or form of payment even though they aren't generated by Banks, [5]. Ethereum is a Cryptocurrency, according to CoinDesk it is based on the mining of a resource named "ether" that allows participants to perform Smart Contracts as well as other activities. Both work through a Permissionless Blockchain and one of their traits like other Cryptocurrencies is their immutability once created.

Ripple is a Cryptocurrency that works similarly to a trading market that allows users to make instant payments in Cryptocurrencies as well as Fiat currencies, according to source Ripple, without a banking account resembling, by its nature the appearance of a digital asset, works in a Permissioned Blockchain.

Finally, Dogecoin (DOGE), is a Cryptocurrency that according to Coindesk as well started as something that was not supposed to generate value, but its one-minute Proof-of-Work (PoW), along with its interactive way of "mining" its Cryptocurrency, made it very interesting. The reason why this currency is being mentioned is due to the issue of supply of a given Cryptocurrency which is a barrier already verified in Cryptocurrencies such as BTC and ETH thus being a target of analysis.

With four Cryptocurrencies with different aspects to be taken into analysis, to better understand what a Cryptocurrency is, first, there was a study on what is Blockchain.

2.2 Blockchain Technology

Blockchain consists of a network of blocks with properties very intrinsic in their design. A blockchain is a form of permanent transaction registration, which requires the approval of users who are part of the Blockchain so that they can be registered, and depending on the form of consensus of the members of the Blockchain, time or method, a new block is generated that validates all transactions previously made by confirming that the hash of the new block, the hash is the randomly generated code that confirms all transactions, is equal to the hash of the previous block, which then validates the new block by solving an algorithm by the people who are "mining" a certain Cryptocurrency, [13].

The process of "mining" is the resolution of an increasingly complex algorithm, using a computer, having better effectiveness the better the components of the computer, namely the graphics card and processor.

Still, nothing is bulletproof, for example, at the core of the internet is the concept of all its users being connected to a server, however, to date there have been major leaks of information, this happens because of the nature of the internet in which its users connect to a server, and hackers take the opportunity to change the "link" between the user and the domain, and thus steal the information of its users or even from the people who provide the website. Decentralization, which is the base property of Blockchain, makes it more difficult for a Blockchain to be a target of hacking unlike what happens on the internet, [13].

So, with Blockchain it is more difficult to steal information, because at its foundations of Blockchain is encryption and trust between its users, reinforcing trust through various consensus that allows the validation of transactions that are recorded, thus building a Distributed Ledger Technology (DLT). The information in the DLT is stored in decentralized blocks and visible to all its participants, [2].

However, all technologies have their flaws and one of the flaws of Blockchain Technology is Forks, that happens, when more than 50% of the people integrated into a Blockchain hold more than 50% of the computational power of the respective Blockchain, changing it, [4].

Forks can be divided into Soft Forks and Hard Forks. Soft Forks happen when there are changes in a Blockchain, an example is, changing the size of the record of operations in a given block. As for Hard Forks when they happen, they can generate new Cryptocurrencies, something that has previously happened with Bitcoin, resulting in Bitcoin Cash, [7]. So, Hard Forks can be useful if everyone who is "mining" a given Cryptocurrency wants to change the code or the properties of the Blockchain of the Cryptocurrency, but it can be a form of hacking something that could be harmful to the holders of a particular Cryptocurrency.

Although the pioneering Cryptocurrency, BTC, was based on a Permissionless Blockchain, which means, anyone can change the code and can "mine" the Cryptocurrency, it has some flaws in how to establish a hierarchy, similar to those already existing in companies, that can transmit security and reliability to its participants.

In these regards, it was taken as an approach to the differences between a Permissioned Blockchain and a Permissionless Blockchain.

2.3 Permissionless Blockchain and Permissioned Blockchain

One of the properties of Cryptocurrencies is Blockchain and it can be worked through Permissionless or Permissioned Blockchain.

Cryptocurrencies that work on a Permissionless Blockchain are more attractive, since there are fewer barriers to the entry of persons who choose this Cryptocurrency, even though they are less safe given the anonymity of users, so if people are stolen it will be harder to track.

So, it becomes important for people and companies to have the choice to be able to develop applications or store their possessions safely, and the closest solution was through a Cryptocurrency that has a Permissioned Blockchain Platform, [11]. Although the immutability of a Blockchain is something that transmits a lot of security, its immutability prevents the dynamics in the creation of a Blockchain because for this it is necessary to always create a new Blockchain, since you can’t change it once developed, [11].

Although cryptocurrencies may leverage many people’s wealth, they can not only be forked which can cause its miners to lose credibility of what has been recorded on the blockchain, as well as holders for example bitcoin losing their wallet which has caused the loss of many people’s savings, [12]. Also, the recent collapse of the Hedge Fund FTX, made it more insecure for people to hold their savings in a crypto bank leaving many customers and investors in a loss of billions of dollars.

Then in a brief analysis, there is a need to make Blockchain Technology more dynamic, technology that is associated with the creation of various Cryptocurrencies. So, there is a need to evaluate the taxonomy of Cryptocurrencies and the possibility of them being able to replace fiat currencies and assess the benefits that society can take from Blockchain Technology.

Taking the aforementioned into consideration, recent studies question the possibility of central banks implementing their own Cryptocurrency that works in parity with the fiat currency, which might replace the fiat currency. The next chapter goes through a short review of the concepts of a Central Bank as well as the possibility of a Central Bank Digital Currency (CBDC).

2.4 Implementation of a Central Bank Digital Currency

The management of the monetary policy is carried out by central banks, which means, the number of coins, banknotes to be produced or the volume of currency to be produced is decided by them. Central banks also take into account the management of interest rates and inflation present in the various economies, [3].

The properties of a fiat currency and a Cryptocurrency are different, for example, the management of the supply. In the case of Cryptocurrencies, by default given their varied forms of consensus, by other words their validation time intervals of another new block on the respective Blockchain, their stock will be predictable or, given their costly form in terms of the "mining" process, this will eventually have its supply limit reached. Thus, the principle of markets being efficient is not verified because they are predictable.

Although Cryptocurrencies have interesting properties such as their immutability when created as well as, reliability in the registration of all transactions, and because they are decentralized giving more security to their participants, they do not have the same properties as fiat currencies.

The obstacles encountered for the implementation of a CBDC are in the monetary policies that currently govern Fiat currencies. Given what has been described in relation to Cryptocurrencies according to their acquisition of them being done by solving complex algorithms, in other words, “mining" or through financial markets, there is no way to give the guarantee to regulators that, if necessary, the people who hold certain Cryptocurrency will have the same behavior according to Fiat currencies. Even if a bank produces a certain Cryptocurrency and it was with a Permissioned Blockchain so that there could be, a regulatory body and a hierarchy that transmits security to its participants, there is the risk of central banks being the target of thefts, [3]. The authors of the article leave open the hypothesis of the implementation of a CBDC by each Central Bank, [3].

On the other hand, there is the hypothesis that implementing a CBDC will be much more challenging than imagined due to monetary law, [14]. Looking towards a reform of central bank law some of the things mentioned below raise fundamental questions and thoughtful discussions must be taken into solution in political organs with a very rigid law analysis. Aside from that, according to the above the ability of a state to be involved in the reform of monetary law to accommodate CBDC emissions could be limited by the constitution. In the first scenario, a CBDC token that could match the monetary mass or notes would take a lot of effort. So the countries would need to first take the status of legal tender, [14]. An option is to go step by step and limit the entities that could have access to this CBDC such as the state, public bodies, and merchants beyond a certain size and firms with authorized activities, such as banks. The next step would be to classify a CBDC as a token so it could be a new way for this token to have privileges of private law so there could be circulation among people. And lastly, and more important authorities should see any definition of all cybernetic crimes to ensure it covers all CBDC crimes.

However, there is a study that analyzes situations similar to the implementation of more than one currency in an economy of a country which speculates various types of results in the implementation of it where a comparative approach to the case of Cryptocurrencies will be made, [8].

2.5 Ecology of Money and Collaborative Economy

The concept of "Ecology of Money" is the hypothesis of several currencies, in a country being divided by region and hierarchically in terms of the economic needs of each citizen, [8].

A plural monetary system would give more resilience to economic crises, and these currencies would work in parallel with the economy, so having a more diverse system of currencies, it could reduce economic growth, which is somewhat detrimental given the scarcity of resources, [8].

On the other hand, a more diverse economic system will be more resilient and stable to financial crises, because if a certain currency were to generate a crisis others could replace this, [8]. One example is the case of WIR in Switzerland which functions as a complementary currency and has an important role to play in countering economic cycles that help stabilize the economy. WIR is a currency that helps small and medium-sized enterprises to buy goods and services, [8].

An interesting note is that there is a phrase from Tobin that states that “money will only make sense if it is accepted by a certain number, [8]. That is, if there is acceptance of complementary currencies, in this case, Cryptocurrencies, it is possible to see a new economic scenario that can solve various crises in different sectors, given the segmentation made by several currencies.

The benefits of a Collaborative Economy, are in various areas such as food, accommodation, transportation, as well as other goods and services, [5]. The Collaborative Economy changes the market concept in the sense that it involves P2P exchanges on the Internet, with purchases, resales, and donations in a monetary way.

With regards to the conclusion of Collaborative Economy, is that Collaborative Economy today has a great impact on being able to live in a more collaborative society, which reduces the development of monopolies and can change the way of managing platforms in different areas of science, [5]. Also, it isn't set aside from the hypothesis that Blockchain Technology can improve the decisions of organizations, increase the storage capacity of information, and reduce the risk of fraud and legal care given the creation of Smart Contracts, [5].

From the analysis made between the concepts of Ecology of money and Collaborative Economy, although both articles say that it is premature to conclude, nowadays it is remarkable the increase of Cryptocurrencies presence, the evolution of Blockchain Technology, something that may have been accelerated given the pandemic situation that is lived because much of the labor activity is closed, and there seems to be an increased acceptance of a safer society, with a greater focus on the sharing of goods and services produced.

Lastly a note of Cryptocurrencies on the aspect of audit and its benefits, as well as the exchange ratio for Fiat currencies and Cryptocurrencies.

2.6 Cryptocurrencies under Audit and Exchange Rate Ratio

Cryptocurrencies, considering the underlying Blockchain Technology, have the property of immutably storing the registration of all transactions. Blockchain Technology has brought an innovative way to exchange information, [4]. Blockchain Technology allows users to validate transactions, which are stored in blocks using Cryptography, [4].

One advantage of Blockchain is increased transparency, since the participant obtains a copy of the ledger records facilitating access to information, [4]. More control is also gained through the form of consensus on the part of the participants, for example, Proof-of-Work (PoW), something that is recorded in several blocks. There is also a reduction in error and fraud as transactions are automatic and there is a cost reduction and the data has more security because it is encrypted once validated. Finally, more transparency in the delivery of assets, considering that there is a history that can be seen by the participants, and they can see how the products were developed and thus transmit more security to investors who intend to buy the products.

From the point of view of audit, it is impossible to change the recorded information, using encryption, which reduces human error thus allowing greater security to regulators, [4].

Figure 1 illustrates an example of the architecture of a "Permissioned Blockchain" which is structured as the simple form of a Blockchain for Audit purposes, where the nodes are the participants, [4].

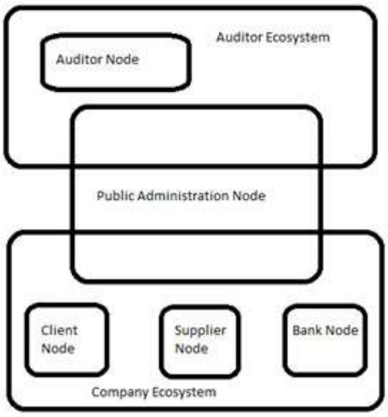

Fig. 1: Blockchain Ecosystem

According to Figure 1, it contains the Auditor's Ecosystem, the Company Ecosystem, and the Public Administration node, where the link between both Ecosystems is made and where all the information is stored. The access of the various elements for each participant is made through encryption that thus solves the problem of privacy, [4].

Still, there has been some tough hacking according to sources from Crystalblock, even though it might be possible to create a safe blockchain. Some of them are Mt Gox in 2011 the first major breach and many others incurred like Binance and Coincheck.

Finally, Blockchain Technology can make it more efficient to make money, in assets, and transaction information, also improving issues such as privacy and security, [1].

From a security point of view, there are still security flaws for those who have Cryptocurrencies and may be the target of hacking, [4]. In addition, given the anonymity present in Blockchain Technology some use this Cryptocurrency for criminal activities.

Regarding the exchange ratio between fiat currencies and Cryptocurrencies, since Cryptocurrencies are not available by governments, they act as complements to fiat currencies, [1]. ETH is a good asset to have in the investment portfolio, while Cryptocurrency BTC serves to leverage the number of people who own this market, [1].

Also, from Binance, it is important to note trading markets like FTX or Binance which have been around for a long time and make it possible for traders to trade fiat currencies and cryptocurrencies with derivatives such as futures and options and with other current tools that have existed in former trading markets and give also the ability to create a token, this without the help of an intermediary.

Now after analyzing both Blockchain and Cryptocurrency and all their benefits and flaws as well as similarities and differences, it was now studied the expected return of a portfolio of Cryptocurrencies as well as a few scenarios and their implications for investors given the obtained results.

3 Method of Analysis

3.1 Calculation of Return and Standard Deviation

To calculate the Expected Return as well as the Standard Deviation of the four Cryptocurrencies BTC, ETH, XRP, and DOGE, information was taken from the source Coindesk about their closing price. To this end, a coincident date, 27/02/2019, was used for the 4 Cryptocurrencies to compare them more efficiently.

The value of the annual return was calculated through the compound annual growth rate, [6].

$$CAGR = \left(\frac{Final\ Value}{Inicial\ Value}\right)^{\frac{1}{t_{final}-t_{inicial}}} -1 \qquad (1)$$

Subsequently, the standard deviation will be calculated, through the daily yields of the respective Cryptocurrencies, [9].

$$\sigma_{Daily} = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}} \qquad (2)$$

Next, to obtain annualized values, taking into account that Cryptocurrencies are subject to financial markets 24 hours a day, the standard deviation was annualized by multiplying the whole of days in a year, through the following equation:

$$\sigma_{Annualized} = \sigma_{Daily} * \sqrt{365} \qquad (3)$$

3.2 Approach by Capital Assets Pricing Model (CAPM)

To obtain an optimal portfolio with the set of assets, BTC, ETH, XRP, and DOGE, it was calculated the annual return and standard deviation. Initially taking into account that the information collected so far was up until February 27, 2021, an American R_f report in 2020 was chosen, obtained in Kroll.

The formula for calculating the expected return of the Markowitz assets portfolio is, [10].

$$E(R_P) = X_A * R_A + X_B * R_B + X_C * R_C + X_D * R_D \qquad (4)$$

For standard deviation, [10].

$$\sigma_P = (X_A^2 * \sigma_A^2 + X_B^2 * \sigma_B^2 + X_C^2 * \sigma_C^2 + X_D^2 * \sigma_D^2 + 2 * X_A * X_B * Cov_{A,B} + 2 * X_A * X_C * Cov_{A,C} + 2 * X_A * X_D * Cov_{A,D} + 2 * X_B * X_C * Cov_{B,C} + 2 * X_B * X_D * Cov_{B,D} + 2 * X_C * X_D * Cov_{C,D})^{\frac{1}{2}} \qquad (5)$$

3.3 Markowitz Border and MVP

To obtain the Markowitz Border as well as the MVP, a set of calculations were done using Microsoft Excel Solver. First, the objective was to obtain the MVP, and for that using a set of restrictions while minimizing the value of Standard Deviation, a value for the expected return was achieved.

From there, both the Efficient Border and Inefficient Border were calculated with a series of restrictions using the value obtained as the MVP as the starting point, for example, the sum of proportions being equal to one and not negative. The restrictions were the same for both, for the Efficient Border the objective was to maximize the expected return in comparison to the increase of risk, and for the Inefficient Border, the objective was the opposite.

With the values obtained, then it could be finally drawn the Markowitz Border and thus proceed to the calculation of the Capital Market Line.

3.4 Capital Market Line Calculation (CML)

For the calculation of the capital market line (CML), in Microsoft Excel a line was made with combinations of proportions, using a solver. The CML equation is:

$$\text{CML: } E(R_c) = R_f + \frac{\sigma_c}{\sigma_p} * (E(R_p) - R_f) \qquad (6)$$

From the above-mentioned equation, it can be concluded that CML is a line, more specifically the line of the Capital Assets Pricing Model (CAPM) that is intended to determine.

However, there is currently no information on how to determine CML, but it is known that Sharpe Ratio is the slope of the CML line.

$$\text{Sharpe Ratio} = \frac{E(R_p)-R_f}{\sigma_p} \qquad (7)$$

Using Microsoft Excel, more specifically Solver, Sharpe Ratio is maximized by changing the proportions of the portfolio, with the restrictions of non-negativity and the sum being equal to one, obtaining the point of tangency, from a line originated in R_f, to the efficient border of Markowitz, [10]. In this point of return, it has its optimal value on the efficient border of Markowitz, representing the optimal market portfolio (P).

This way, it is already possible to draw the line of the CAPM, because we have two points, the point where R_f is and the optimal market portfolio. To have a more complete CML, another point was added that was obtained, giving an arbitrary value to σ_p , by solving the following equation:

$$E(R_P) = R_f + (\text{Sharpe Ratio} * \sigma_p) \quad (8)$$

As for the calculation of a portfolio that is composed equally of all assets, also including the risk-free asset, the following equations were used:

$$R_e = \sigma_t^2 * X_t^2 + X_f^2 * \sigma_f^2 \quad (9)$$

$$\sigma_c^2 = \sigma_t^2 * X_t^2 + \sigma_f^2 * X_f^2 + 2 * \sigma_f * \sigma_t * \rho_{X_f,X_t} \quad (10)$$

As for σ_f, it will have a value of zero considering that it is a risk-free asset, and it has no risk, so its standard deviation is zero. This approach will give a better insight into where to put our savings, namely in the optimal portfolio or put it in the R_f. It's a case scenario where it will also give a better idea of how worth it is to invest in this portfolio also taking into consideration its risk.

4 Data

4.1 Statistical Inference of Collected Data

Considering the information collected from 27 February 2019 to 27 February 2021 for the calculation of the annual returns of each of the Cryptocurrencies, as well as the remaining parameters of analysis.

The following Table 1 was drawn up, which demonstrates the results obtained for all assets.

Table 1. Sample Representation of Cryptocurrencies

	BTC	ETH	XRP	DOGE
Days	365	365	365	365
Quote 27/02/2019	3 772,94 €	131,67 €	0,30770 €	0,001944 €
Quote 27/02/2021	46 642,61 €	1 495,81 €	0,44170 €	0,050144 €
Annual Return	251,60%	237,05%	19,81%	407,88%
Average Daily Standard Deviation	0,037964	0,04656098	0,0536748	0,11497138
Annualized Standard Deviation	0,725305902	0,889546356	1,0254557	2,19652519

Given Table 1, it is possible to see the quotes which gave the possibility to calculate the Annual Return, showing high values of profitability being the most notable Cryptocurrency DOGE with a return of 407,88%. Through these values stated in Table 1, it is also noted the values for the average standard deviation, which gives a better insight into how risky it is to invest in a given Cryptocurrency, is riskier to invest in DOGE with a value of 2,2 and being BTC the more rewarding when comparing risk and return with values of 251,6% and a risk of 0, 72. Also, it is possible to note the difference in the closing price of BTC and ETH throughout the years, which can be deducted and will have some weight in the optimal market portfolio obtained later in this study.

4.2 CAPM Data

The data for Sharpe Ratio will be illustrated in Table 2.

Table 2. Data for Sharpe Ratio

DOGE	BTC	ETH	XRP	Sum	DOGE	BTC	ETH	XRP	R_e	σ_c
0,219385	0,787081	0,929908	0,920522	2,856895	0,096644	0,54487	0,340653	0,017834	257,62%	0,5424

From the representation of Table 2, what can be obtained is the investment proportions for each of the Cryptocurrencies which are respectively, 1,8 % in XRP, 9,7% in DOGE, 34 % in ETH, and 54,5% in BTC, which, optimal return (P), is 257,62 % with a standard deviation of 0,5424. The optimal portfolio (P) was obtained by maximizing the Sharpe Ratio equation and this portfolio (P), is also on the Efficient Border of Markowitz.

Finally, the data for CML are explained in Table 3.

Table 3. Data for CML

CML	Expected Return	Standard deviation
Rf	2,50%	0,0000
P	257,62%	0,5424
O	289,42%	0,6100

5 Results Analysis

5.1 CAPM

The analysis of the results obtained from the CAPM considers CML and its Sharpe Ratio, as well as a portfolio composed of a risk-free asset, analyzed below in Figure 2.

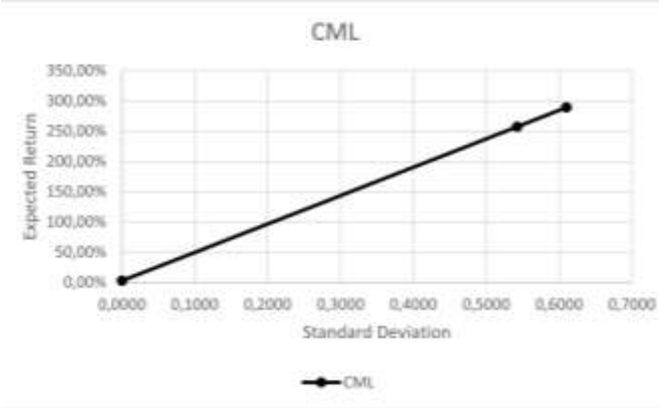

Fig. 2: Capital Markets Line (CML)

The CML chart translates what was intended to be obtained with CAPM, which is, the portfolio composed of Cryptocurrencies and a risk-free asset. The option of having a portfolio with a composition consisting exclusively of a risk-free asset provides a return of 2.5%. Any wallet that results from the combination of Cryptocurrencies and a risk-free asset is located along the CML, generating different expected yields for different risk exposures.

The optimal market portfolio (P) was obtained by maximizing the Sharpe Ratio from where the expected return value is 257,62% with a standard deviation of 0,5424. This consists of 4 Cryptocurrencies, BTC, ETH, DOGE, and XRP with the following proportions: 9,7% in DOGE, 1,8% in XRP, 34% in ETH, and the remaining 54,5 % in BTC.

As for the value of the Sharpe Ratio obtained it was 4,7 this means, the return obtained by each unit of risk is 4,7.

The analysis of the graph obtained with the CML and Markowitz Efficient Border is illustrated in the following Figure 3 and commented on below, [10].

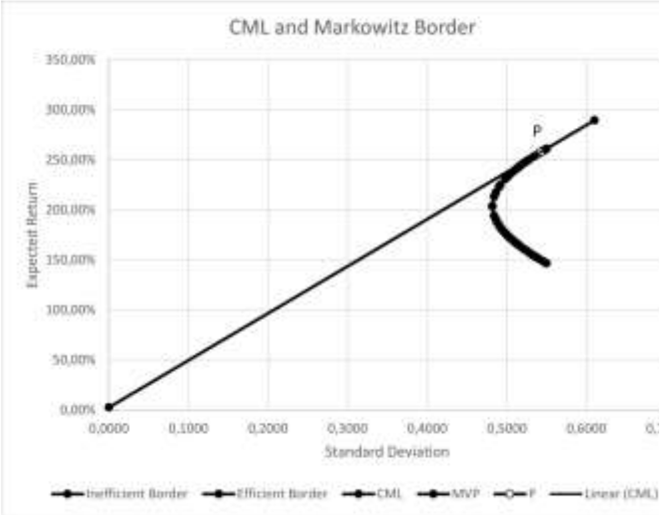

Fig. 3: Graph CML and Markowitz Border

Figure 3 shows the objective result, which illustrates the CAPM line, CML, as well as the Markowitz Border, and the optimal market portfolio (P) which maximizes the Sharpe Ratio, [10].

The results obtained, allowed us to conclude that it is possible to have a portfolio with assets with Cryptocurrencies in the same way as it does for any other portfolio of assets, from where the proportions to be invested are 9,7% in DOGE, 1,8% in XRP, 34% in ETH and 54,5% in BTC with an expected return of 257,62 % and a standard deviation of 0,5424 previously illustrated in Table 2.

Lastly when compared to the return obtained for an investment portfolio with assets such as Facebook, Amazon, Apple, Microsoft, and Google (FAAMG), according to Portfolioslab, which has a return on the portfolio, as of July 11, 2021, of 25.19%. The portfolio with Cryptocurrencies relative to the FAAMG portfolio is about 10 times more profitable. As for the Sharpe Ratio it is 1,67, while the wallet with Cryptocurrencies is 4,7. So, it is shown that the potential of Cryptocurrencies is notorious, given that they have much more significant gains than in traditional markets, even compared to the best companies in the technology sector.

From the values obtained, it can be concluded that the expected return having a value of 257,62% and a standard deviation of 0,5424 is an acceptable value that instills a good investment opportunity given the difference between profitability and risk. As for the proportions, given the increasing appreciation of Cryptocurrencies BTC and ETH, these have more weight in the optimal market portfolio.

If, for example, an investor wanted to invest part of his wealth in a risk-free asset and the remaining Cryptocurrencies, 20 % in each, he would see his wealth be along the CML line, in other words, he wouldn't have to become indebted to the risk-free asset to obtain yields in excess of (P). The values obtained were an expected return of 206,59% and a standard deviation of 0,4339. The next Figure 4 illustrates these results.

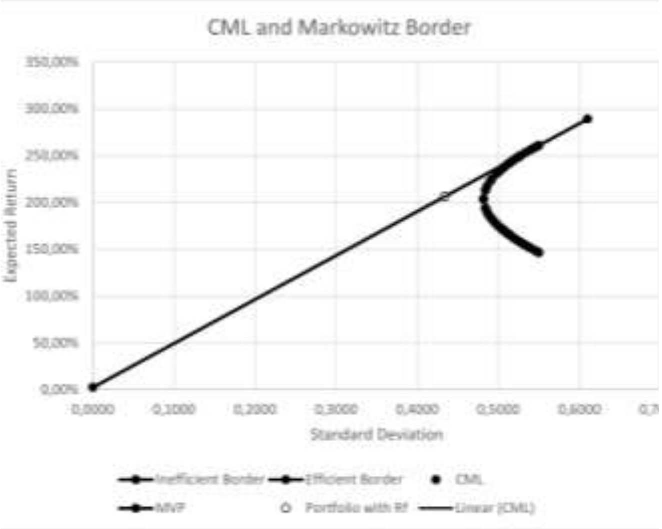

Fig. 4: Portfolio with P and risk-free asset

In conclusion, from the investors' point of view, for any investment, there is always a risk regardless of what we are investing. In the specific case of Cryptocurrencies, it is a volatile market, with different trading conditions, even with financial instruments equal to those already existing, where it is traded 24 hours a day. Considering the results obtained it is shown that the greater the gain, the greater the risk, and there is always the same direct relationship between risk and return, identical to the reality of other traditional financial markets, through the portfolio of assets that can be held.

In the context of the analysis carried out previously, considering that Blockchain Technology has drastically changed the way one looks at society, the hypothesis of the creation of a Cryptocurrency could benefit society.

From a less formal perspective, one person can see Blockchain Technology as the wheel. Having Blockchain Technology arisen with Bitcoin, this technology has been evolving since its invention, in a sense that potentiates the improvement of people's quality of life. Since the creation of Bitcoin, other Cryptocurrencies have emerged that have used the benefit of Blockchain Technology and have developed applications and other ways to improve the social context in various areas such as logistics of an asset, Smart Contracts, or other productive activities.

Bitcoin can be seen as "digital gold", still, given the costly expenditures in terms of electricity and its limitation in its stock, it is predictable that it will eventually lose value with the emergence of other more efficient Cryptocurrencies.

This way raises the idea of a Cryptocurrency that can solve in many ways the problems that society faces in various areas. Based on the act of the internet in which we connect directly to the servers there is thus a possibility to see our information being stolen, something that by the decentralized nature of Blockchain Technology can give more security.

Taking into account what was mentioned, arises the idea of a Cryptocurrency called "Speed of Sound" (SoS), which aims to solve this problem, from the perspective of security as well as other various areas, such as restaurants, leisure such as movies, games, bookstores among others. As its name implies, SoS has the purpose of having a PoW corresponding to the speed of sound. Also, the stock issue can be something that can hinder the duration of a Cryptocurrency and so arose the premise of this Cryptocurrency having an unlimited stock. As a whole, SoS would be a digital asset that would give its users security, given its PoW, because whenever there was an attempt to steal information, it would be emitted for example the sound of an alarm that would block this attempt to steal information and alert its users of it.

This idea comes in a pandemic context considering that many people are currently using the internet and that many of them have lost some contact with other people and, with activities they did in a pre-pandemic context and saw their information stolen. It could also be used to emit sounds in other aspects such as the purchase of a good or service, or the sound of a cash register would be emitted, when sending a message would be emitted the respective sound of sending the message, among others. This may be an idea of giving more life to technology and, consequently, more safety to people.

Through the analysis done so far, Cryptocurrencies are worth what they produce as any asset which means the idea was to incorporate this Cryptocurrency as a digital asset. Thus, this could be a way to properly reclassify Cryptocurrencies in relation to their taxonomy and what they might be worth as a productive asset.

Finally, this new notion of Cryptocurrency can change the way Cryptocurrencies are seen, from their integration in the markets as well as in a more social context and their regulation.

6 Conclusion

Currently, Cryptocurrencies are a theme much addressed by everyone given their innovative nature and because they still have much to explore.

Cryptocurrencies are crypto of encryption and currency because they can be exchanged. Currently, there is still confusion about what Cryptocurrencies are, which somehow makes it impossible to properly have their taxonomy as well as their legalization.

One of the objectives of this paper was to try to solve this problem. It is known that an asset is worth what it produces, and this should be the approach of Cryptocurrencies. However, Bitcoin is an asset that serves only as a record of transactions but given its form of consensus of validation of new blocks on the Blockchain, it becomes very safe and impossible to change, thus justifying its growing value.

In this study with the given literature, it was possible to have a better understanding of the proper functioning of a cryptocurrency by separating blockchain and having an approach towards fiat currency, to know if there was any possibility to have cryptocurrencies as legal tender, as well as a replacement of fiat currency. So, after researching the literature at the time, it is known that there is the possibility for cryptocurrencies to be accepted as legal tender and there is also space for them in the fiat market, by understanding better how Blockchain works, and its restrictions to supply and forms of mining gives a better approach to fiat currencies.

However, other Cryptocurrencies have appeared since Bitcoin, which have brought improvements to new forms of consensus, the type of Blockchain, and what they produce, such as the case of Ethereum or Ripple.

Due to this huge appreciation of Cryptocurrency markets, there is interest on the part of central banks to adopt this new premise. However, the properties of fiat currencies and Cryptocurrencies are different, so there is a barrier that makes it impossible to implement for the time being, a Cryptocurrency that operates in parity with its fiat currency.

There is a need to distinguish Cryptocurrencies from Blockchain Technology. Blockchain Technology has been something that has been evolving immensely. Cryptocurrencies have been valuing their respective consensus in "mining", and effectively for what they produce.

However, there is the problem of "mining" because, in the acquisition of a given Cryptocurrency, it is not possible to have the same control as there is with a fiat currency, in terms of regulation and also in terms of currency supply. For this reason, it was addressed to Cryptocurrency Dogecoin which has an unlimited supply of Cryptocurrency with a fast PoW.

It was also important to evaluate the return of a portfolio of assets with Cryptocurrencies. Through the CAPM method, with a portfolio of Cryptocurrencies and with a risk-free asset, it was possible to obtain results that demonstrate that it is possible to obtain a good portfolio of assets with low volatility, compared to the gains obtained.

Considering the literature review carried out, it was proposed the creation of a Cryptocurrency. Although without programming notions, it is based on the resolution of security problems as well as other sound utilitarian ways to give another more materialized perspective of Cryptocurrencies.

As for the benefits of this study, it allows a better understanding of Cryptocurrencies as well as Blockchain. It makes it easier to understand the advantages of Cryptocurrencies in society and their impact if they were to be considered legal tender.

As for the limitations of this study, it goes through the controversy generated by the theme itself that it tried to resolve by addressing Blockchain and Cryptocurrency differently. Possibly, over time it is possible that there will be a greater integration of both, and this might happen in an early stage through the implementation of a CBDC and by forms of validation of blocks less harmful to the environment. As for Blockchain Technology, it seems to already have a place in society and whether through Cryptocurrency or not, this will certainly evolve over the next times to come.

As for the developed study, Cryptocurrencies have been gaining their place in society and their presence should remain. A suggestion for the future of Cryptocurrencies, given the issue of "mining" in relation to electricity spending and supply predictability, may include having an unlimited supply and making it possible to be acquired as assets and thus having their fair value.

References:

[1] Angelo Corelli. 2018. Cryptocurrencies and Exchange Rates: A relationship and Causality Analysis. *Risks,* 6(4), 111.

[2] Artyom Kosmarski. 2020. Blockchain Adoption in Academia: Promises and Challenges. *Journal of open Innovation: Technology, Market, and Complexity,* 6(4), 117.

[3] Belke, Ansgar and Edoardo Beretta. 2020. From cash to central bank digital currencies and Cryptocurrencies: a balancing act between modernity and monetary stability. *Journal of Economic Studies,* Vol. 47 N.º4, pp. 911-938.

[4] Bonsón, Enrique and Michaela Bednárová. 2019. Blockchain and its implications for accounting and auditing., *Meditari*

Accountancy Research, Vol. 27 N.º5, pp.725-740.

[5] Ertz, Myriam, and Émilie Boily. 2019. The rise of digital economy: Thoughts on Blockchain Technology and Cryptocurrencies for the collaborative economy. *International Journal of Innovation Studies*, Vol 3, N.º4. pp.84-93.

[6] Jason Fernando. 2021. Compound Annual Growth Rate (CAGR). *Investopedia*. Available online: https://www.investopedia.com/terms/c/cagr.asp (acessed on 20 May, 2021).

[7] Katsiampa Paraskevi. 2019. An empirical investigation of volatility dynamics in the Cryptocurrency market. University of Sheffield.

[8] Louis Larue. 2020. The Ecology of Money: A Critical Assesment. Ecological Economics. *Ecological Economics*, Vol. 178, 106823.

[9] Marshall Hargrave. 2021. Standard Deviation. *Investopedia*. Available online: https://www.investopedia.com/terms/s/standarddeviation.asp (acessed on 20 May 2021).

[10] Markowitz, H. .1952. Portfolio Selection. *The Journal of Finance*, Vol. 7, N.º.1. pp. 77-91.

[11] Shi, Zeshun, Surbiryala, Jayachander, Hu, Yang, Laat, Cees and Zhiming Zhao. 2019. An Automated Customization Performance Profiling Framework for Permissioned Blockchains in a Virtualized Environment. Paper presented at IEEE International Conference on Cloud Computing Technology and Science, Sydney, Australia.

[12] Sidhartha Shukla and Emily Nicole. A Hedge Fund hit by FTX Collapse Defaults on $36 Million on Debt. *Bloomberg*. Available online:https://www.bloomberg.com/news/articles/2022-12-06/crypto-fund-orthogonal-defaults-on-36-million-debt-as-ftx-contagion-spreads FTX opposes new bankruptcy investigation as it probes Bankman-Fried connections | Reuters

[13] Yano, Makoto., Dai, Chris, Masuda, Kenichi and Yoshio Kishimoto. 2020. *Blockchain and Crypto Currency, Building a High Quality Marketplace for Crypto Data*. Tokyo: Yano Makoto.

[14] Wouter Bossu, Masaru Itatani, Catalina Margulis, Arthur Rossi, Hans Weenink and Akihiro Yoshinaga. Legal aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations. IMF Working Paper. WP/20/254

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

-Emanuel Soares conducted, conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, software, validation, visualization, writing – original draft, writing – review & editing.

-Gualter Couto carried out, conceptualization, methodology, validation, resources, visualization, supervision, project administration, funding acquisition, and writing – review & editing.

-Pedro Pimentel carried out, conceptualization, methodology, validation, resources, visualization, supervision, project administration, funding acquisition, and writing – review & editing.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This paper is financed by Portuguese national funds through FCT–Fundação para a Ciência e a Tecnologia, I.P., project number UIDB/00685/2020.

Conflict of Interest

The authors have no conflict of interest to declare.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)