DECENTRALIZED FINANCES

Name:

JOEL SÁNCHEZ GARCÍA

Tutor:

ANDRÉS ARNAU PARADÍS

Grado en Finanzas y Contabilidad

2021/2022

ABSTRACT

Cryptocurrencies and blockchain technology are gaining more and more strength in many sectors, mainly in finance, in this work we will deal in depth as the DeFi (decentralized finance) phenomenon that has been taking on more and more prominence in this sector, detailing the operation, the advantages they have over centralized finance and possible strategies that can be carried out today in many platforms. Considering that both cryptocurrencies and DeFi are projects that are in the development and experimental phase but that advance very quickly. What I want to demonstrate in this paper is not that cryptocurrencies are the substitute for traditional finance, because today that is not possible, but they are increasingly adopting a stronger role in society since the profits they offer are immense and have many advantages over traditional finance.

Keywords: Cryptocurrencies, finance, decentralization, traditional finances.

METHODOLOGY

The elaboration of this work will be based on the synthesis of all the information collected in the web pages of all the projects that will be treated later to be able to deepen in the DeFi, adding to that my personal experience as an investor, dedicating many hours of study and research to projects in this sector with an experience of more than 2 years. In turn, all the concepts are consulted in the most recognized web pages in the cryptocurrency sector such as Bit2me Academy, Cointelegraph, Ethereum.org, Coingecko... and articles of Google Scholar.

INDEX

1. Introduction

Technology evolves one step further every day, this causes many sectors to adapt to all advances, such as finance. For many years before Bitcoin came out there were some who created cryptocurrencies similar to Bitcoin [1] but without success as is the case of "E-Gold" in 1996 [2] or "Bit Gold" in 1998 [3] all these projects were collapsed by the US government or the FBI, but Bitcoin in 2008 emerged as a cryptocurrency with an anonymous creator under the pseudonym of Satoshi Nakamoto, which meant that no government or authority could claim or judge the creator as in all the previous cases.

It was in 2008 when for the first time the "Whitepapper" [4] of bitcoin is published in the domain "Bitcoin.org" a totally digital currency, without intermediaries, what is known as the "Peer to Peer" system [5], and totally decentralized, which is supported under the network of the same users thanks to the "Blockchain" technology.

It is from that moment when cryptocurrencies begin to take more and more prominence and to attract the attention of many developers and computer scientists, such as Vitalik Buterin one of the co-founders of Ethereum, the network in which practically all the projects that exist today have been built. `

Ethereum is a decentralized and open-source network just like Bitcoin, but it is the first network that allows the implementation of "Smart Contracts". Thanks to that, developers can use their network and modify their code to create Dapps "Decentralized Applications" is where the DeFi "Decentralized Finance" is born.

DeFi are projects still in the development phase like Ethereum and other cryptocurrencies that seek to continue advancing and developing more technology to solve many of the current problems in the traditional financial system. In this work, it is shown that apart from traditional finance there are decentralized finances, which allow greater financial freedom and improved returns on capital with respect to traditional finance, without having to suffer the volatility so characteristic of cryptocurrencies.

2. Cryptocurrencies

Cryptocurrencies are digital currencies that use cryptography as a basis for their creation, being decentralized and anonymous so that no person and entity can control or issue more, cryptocurrencies work in a PeerToPeer way that is, from one user to another directly without the need for intermediaries. Being based on cryptography and on the blockchain network, all transactions are recorded in the network in a public and non-modifiable way since, being based on a decentralized system, in order to modify a data, it should have control over 51% of the network, something practically impossible at the computational level.

2.1 Origin of Cryptocurrencies

Cryptocurrencies emerged from the creation of Bitcoin in 2008 when its Whitepapper is published for the first time in the domain created on purpose for it "Bitcoin.org" signed by Satoshi Nakamoto, where in that whitepapper he detailed the creation of a fully digital currency supported by the same users who generated said currency by putting at their disposal their own equipment to solve the mathematical algorithms in the Blockchain (mined).

Little by little, over time, this payment system was gaining popularity and developers and computer scientists realized that Satoshi Nakamoto was only a pseudonym and not a person, so the creator of bitcoin is completely anonymous.

As more and more users entered the bitcoin network, Satoshi Nakamoto disappeared completely in 2011 [6]. It was from that moment that Bitcoin became increasingly decentralized and popular.

2.2 Problems they solve

It is complicated to say what problem cryptocurrencies solve since each one is created for different objectives, if we talk about bitcoin, the problem it solves is the centralization that is currently in the banking system, bitcoin is completely decentralized and works without any intermediary, as I explained above, uses the PeerToPeer system, with these features allows you to have complete control of your money, knowing that it will not be able to be manipulated by anyone thanks to the blockchain system.

If instead we talk about Ethereum, the second largest cryptocurrency by market capitalization [7], the problem it solves is to be able to create all kinds of decentralized applications on its network thanks to Smart Contracts that are incorporated into its own network and that can be modified to create any type of decentralized application [8].

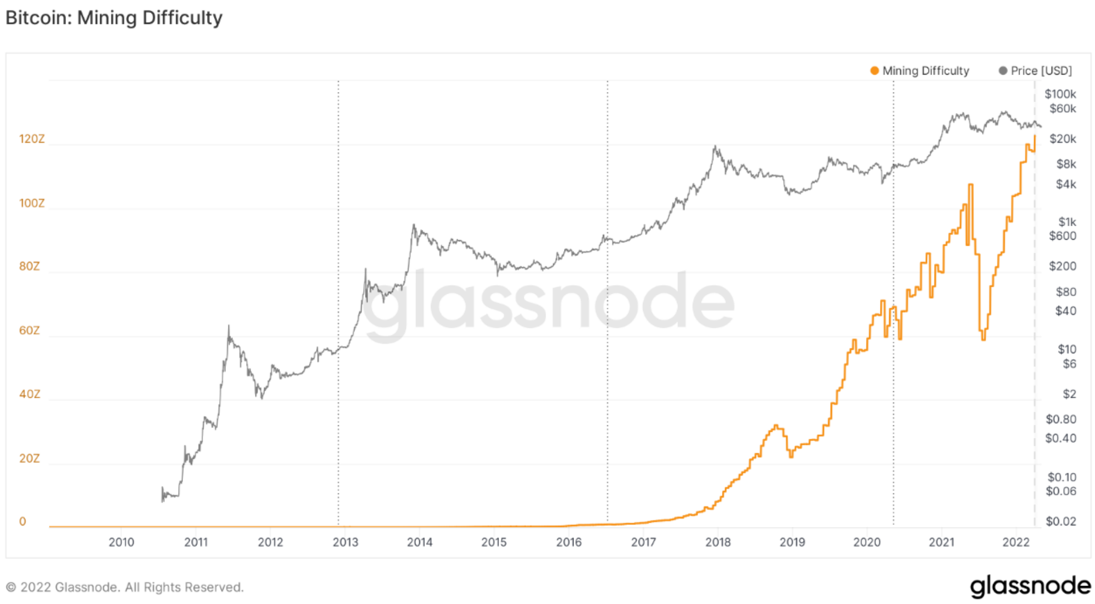
2.3 Functioning

The operation of cryptocurrencies is based on the blockchain, each cryptocurrency adapts this technology in relation to the objective it wants to obtain, but they all start from it.

Blockchain as its name suggests is a chain of blocks, in which each block contains the data, the hash [9] and the hash of the previous block, the data contained in the block varies depending on the blockchain, in bitcoin the data contained in the block are the address of the wallet of the sender, that of the receiver and the amount transferred, each block has a unique hash, what makes this blockchain safe is that each block contains the hash of the previous one so to modify a hash it would be necessary to have to modify all the blocks of the network to be able to validate that change and as each node[10] contains a current copy of the blockchain, when contrasting that change they invalidate the block with the altered information.

To validate a block it is necessary to validate all the transactions of that block, solving the hash, for this the bitcoin blockchain uses the Proof of Work consensus protocol [11], an algorithm, which, to get the correct hash, the node tests random combinations until finding the hash, this makes a node take approximately 10 minutes to solve the hash and thus not be able to modify all the blocks since it would be impossible because at that time the other nodes would invalidate the transaction.

This is how the Blockchain system becomes increasingly secure and stronger as new users enter the system, as can be seen in illustration number one, the difficulty of mining has been increasing as the network has been growing and being increasingly decentralized.



Ilustration number 1. Mining Difficulty. Source: https://studio.glassnode.com/metrics?a=BTC&category=Miners&m=mining.DifficultyLatest

3. Wallets, Tokens and Stablecoins

To understand how decentralized finance works, it is necessary to know three basic concepts within the ecosystem, wallets, which help us to have access to our funds within the blockchain, on the other hand, tokens, which are the currencies issued by a private entity, and, finally, stablecoins, necessary to not be exposed to the volatility of cryptocurrencies.

3.1 Wallets

To be able to interact with the blockchain and manage all transactions and store cryptocurrencies, digital wallets are used, in these wallets both private and public keys are stored to access the assets on the blockchain, each wallet that is created generates between 12 and 24 words or seed phrase, it depends on the wallet, those 12 or 24 words are the only way to access the wallet, if they are lost you will not be able to access the funds in any way.

There are two types of wallets, cold wallets and hot wallets, the first are the most secure since they keep our keys that are necessary to access the funds on the blockchain, off-line, with those keys the wallet signs the transactions and allows to do all the operations in the Blockchain , with cold wallets these signatures are made with a hardware device off-line so you reduce the risk of being hacked since your keys are not in an online wallet exposed to hacks.

On the other hand, hot wallets are those that are hosted in applications on the computer online, the operation is the same as in cold wallets but with the difference that the keys are constantly hosted on the internet being very vulnerable to possible hacks.

As can be seen in figure number two, the number of active Wallets has increased exponentially accompanying the rise in the price of Bitcoin.

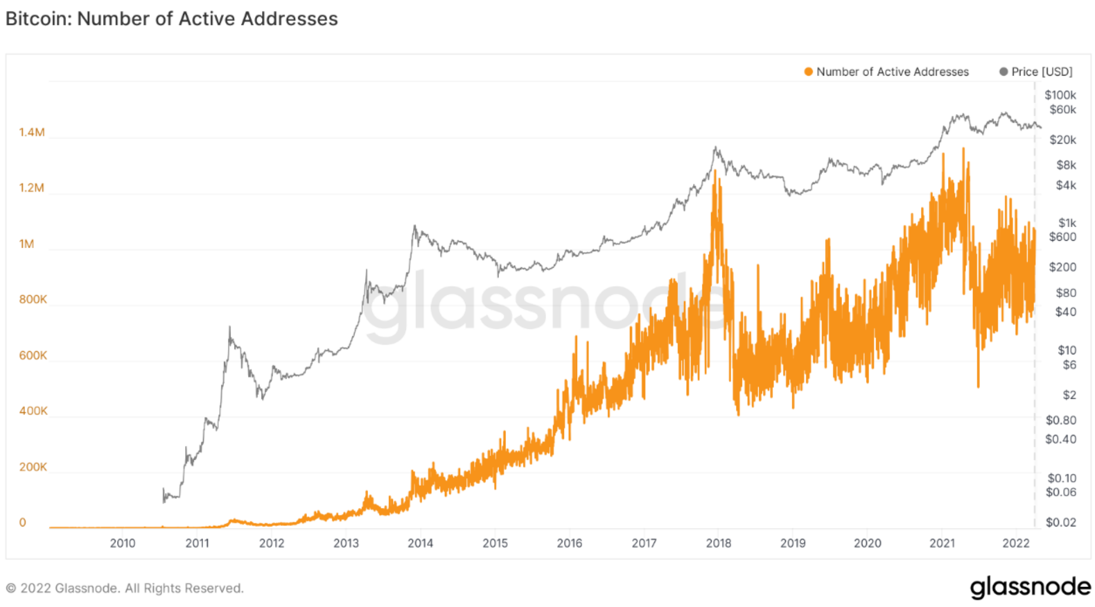


Illustration number 2. Number of Active Addresses. Source: https://studio.glassnode.com/metrics?a=BTC&category=Addresses&m=addresses.ActiveCount

3.2 Tokens

Tokens are one of the most important concepts in cryptocurrencies, they are objects that resemble currencies, but lack legal tender value, since tokens are issued through a private entity, which determines a use.

All tokens are based on the blockchain of a third party, that is, the tokens are created on the blockchain, there are countless blokchains that allow you to create tokens, such as Ethereum, Waves, Tron ... The one that has more tokens created on its blockchain is Ethereum, thanks to the implementation of the Smart Contracts mentioned above, they allow to create tokens in a very simple and fast way for developers, currently has around 180,000 ERC-20 tokens on its blocakchain. [1 2]

There are three types of tokens, the Utility Token, are tokens intended to offer a utility within the blockchain and not with a financial objective, they are used in the DAO (Decentralized Autonomous Organization) and serve for votes within the DAO on modifications in the project, proposal of improvements.. That is, the owners of the tokens participate in the project.

On the other hand, there are the Equity Tokens, they are the synonyms of the shares of the companies, they represent the ownership of some asset or some company of third parties.

And finally, Security Tokens, which are similar to Equity Tokens, give users certain rights and obligations over an asset or company.

3.3 Stablecoins

Cryptocurrencies are very volatile and in order to mitigate their volatility stablecoins were created [13], they are cryptocurrencies that are guaranteed by another asset and have a permanent reference value, usually the price of the dollar.

There are three types of stablecoins, on the one hand, there are the stablecoins with fiduciary guarantee that are those that are backed 1 to 1 by an underlying government currency, usually the dollar, such as the USDT stablecoin, this type of stablecoins are centralized, since they must keep in custody the USD that is deposited in exchange for the USDT that is issued.

On the other hand, there are the stablecoins backed by other cryptocurrencies, which depend on a Smart contract and allows through loans to generate new stablecoins, in this way regulate supply and demand, such as aUSD of the Acala blockchain, being stablecoins with a degree of decentralization.

And finally, algorithmic stablecoins, whichare always stable, use algorithmic methods that regulate the supply and demand of the stablecoin and are usually backed by other cryptocurrencies in order to maintain parity with the price of the dollar. When the price loses parity increasing in value, the algorithm issues currency, if on the contrary it loses parity decreasing in value, the algorithm buys currency from the market and withdraws it from supply, an example of algorithmic stablecoin would be USDN from the Waves blockchain, they are the most decentralized stablecoins.

With these three methods, stablecoins can maintain their price and thus hedge against volatility.

Stablecoins are not decentralized applications as such, but they are of vital importance to make DeFi applications much more accessible to everyone and to be able to have a stable store of value.

Within the stablecoins the most important by market capitalization [14] are USDT, USDC and BNB, all three are centralized stablecoins and backed 1 to 1 with dollars.

As I said before, stablecoins are very important for an ecosystem and for DeFi, if they lose parity and cease to be stable, the result is very negative. As for example, the case of UST, the stablecoin of the Terra ecosystem, it is an algorithmic stablecoin and backed by the native token of the LUNA blockchain.

This stablecoin lost parity with the dollar and caused a fall of the entire ecosystem and capital outflow of the protocols hosted in its Blockchain, causing a fall in the price of the LUNA token from $ 120 to $ 0.0002926 [15] and losing the parity of the stablecoin with the dollar reaching $ 0.19 [16].

In one of its most important DeFi protocols in the entire ecosystem of cryptocurrencies called Anchor Protocol went from having 14.50 billion dollars deposited in its protocol to 315 million dollars [17] in just ten days.

4. Ethereum

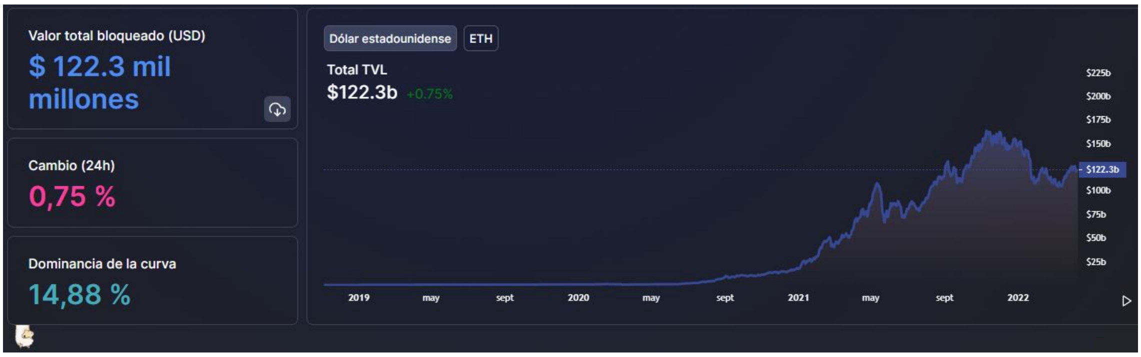
Ethereum was the second blockchain that was created after bitcoin, with the same consensus protocol (PoW) but with a different objective, Ethereum was the first blockchain that implemented programmable Smart programs to be able to create Dapps (Decentralized Apps) that interact with its blockchain.

The Dapps act just like a normal web page, but the reality is that the Dapps are interacting with the blockchain and running the Smart Programs that have been previously programmed, without these the DeFi would not be possible.

Smart Programs are the same as traditional contracts, one agreement and two parties, at the moment that all the conditions of the contract are met, it is activated automatically, these are intelligent, programmable, digital and automatic. This allows you to automate actions or events and thus create Dapps.

Currently the Ethereum network is the one that has the most DeFi protocols on its blockchian with a total of 459 protocols on the network [18], a protocol, is a system of rules that allow two or more computers to communicate with each other to transmit certain information.

On the other hand, the Ethereum network has a TVL (Total Value Locked) of 122 billion dollars as seen in illustration number three. The TVL in this aspect is the most important thing since it is what gives you the most confidence of a network, since it is the total blocked value that is in the network, that means that users trust the protocols that are built on that network and block their tokens so that it works while giving them certain returns.



Valor total bloqueado (USD)
$ 122.3 mil millones

Cambio (24h)
0,75 %

Dominancia de la curva
14,88 %

Total TVL
$122.3b +0.75%

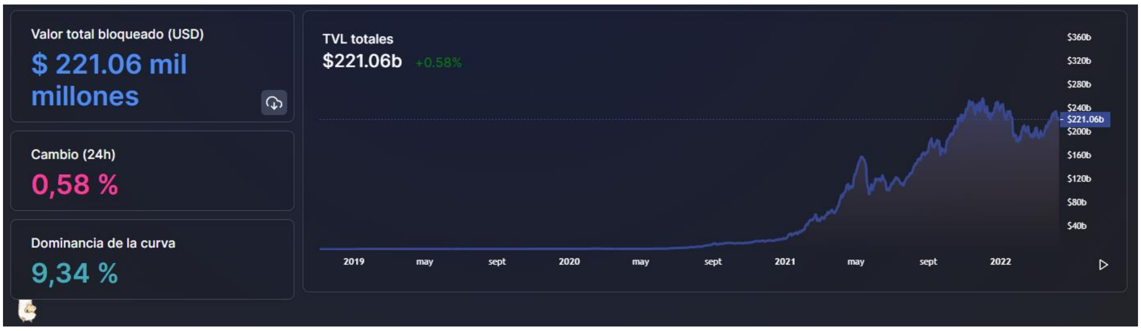
Ilustration number 3. (2022). Total Value Locked in Ethereum. Source: https://defillama.com/chain/Ethereum

5. Decentralized Finances

Decentralized finance (DeFi) arise to eliminate intermediaries in finance and to be accessible to anyone, thanks to blockchain technology this can be achieved, but it is still an experimental and constantly evolving product, which is being developed based on trial and error, every day thousands of new projects arise with hopes of solving all the current problems of the DeFi, but the reality is different, many of these projects do not manage to realize what they proposed, since as I said before, they are in a phase of complete development.

It is a sector that does not stop growing with an upward trend in which little by little more people are joining and are adding value to the ecosystem.

The DeFi, to be useful need to have a monetary value, this is achieved by blocking the cryptocurrencies in the Smart contracts. As can be seen in figure four, the TVL at the beginning of 2021 was around 18 billion dollars, in a year it has reached 238 billion dollars, obtaining the highest peak at 254 billion dollars approximately at the end of 2021.



Valor total bloqueado (USD)
$ 221.06 mil millones

Cambio (24h)
0,58 %

Dominancia de la curva
9,34 %

TVL totales
$221.06b +0.58%

Ilustration number 4. (2022). Total Value Locked in DeFi. Source: https://defillama.com/

5.1 How DeFi works

Thanks to the Ethereum blockchain and its Smart Contracts, it allowed users to modify their code and the Smart Contracts of that network to create DeFi projects, which were initially based on liquidity markets, loan systems and decentralized exchanges (DEX).

Todo began extrapolating traditional finance to blockchain technology and Smart Contracts, but little by little it evolved to be completely decentralized, without any intermediary or central control to be able to carry out any operation.

In December 2014 MakerDao was founded, being the first DeFi platform on the Ethereum network, founded by Rune Christensen.

This protocol works in a similar way to the traditional system, the borrower requests a loan through the dapp, to a lender, directly without intermediaries, this agreement is registered in the blockchain and in a Smart contract, the borrower deposits a collateral that is blocked until he returns the loan, this collateral is usually 150% of the value of the loan in a cryptocurrency different from the one he receives to over guarantee the lend and protect the lender from price volatility. In this way the lender receives an interest for lending its stablecoin. The moment the borrower returns the loan automatically the Smart contract is activated and unlocks the collateral to deposit it in the borrower's wallet and returns to the lender the borrowed funds plus the interest on the loan. All this happens automatically and without any intermediary.

This sector, like many others, offers advantages and disadvantages over traditional finance.

5.1.1 Advantages

One of the main advantages of this financial system is decentralization which allows it not to be controlled by a central entity that makes the decisions or manipulates the system, the decisions that are made in each project are made in the form of votes among all the users of the network that provide liquidity to the network and thus obtain voting power through the governance tokens or utility tokens, on the other hand, this system is completely anonymous and does not require KYC (Know Your Customer) [19] so everyone has the same opportunity to access, only with an internet connection. This also allows companies to access financing more easily.

There is no bureaucracy or procedures that hinder access. Another of the main advantages is the total control that each user has over their funds, has full control and can spend or invest it as you want, when you want and without having to request banking permits as it happens on many occasions.

Transparency makes it another significant advantage since being open source and decentralized, all operations that are carried out on the network are public and auditable.

5.1.2 Disadvantages

On the other hand, there are also many disadvantages in this sector, being in full development presents certain shortcomings and weaknesses that have not yet been resolved.

In theory, DeFi are accessible to everyone, but in practice it is different, since they currently require a moderately high level of knowledge at a technical level that does not allow all users to access this system.

On the other hand, the platforms are complex to understand and navigate at a visual level which worsens the user's user experience.

Security is another of the spectators that still has to improve since they are based on Smarts contracts, if a Smart contract is poorly programmed or with deficiencies, being completely public it can be hacked.

A relevant aspect in this system is that being an immutable system, all the transfers or operations that are made are irreversible, so, if the user makes a mistake in one direction, he would lose all the funds, since being totally decentralized there is no institution behind to claim.

Being a product in the process of development, users who are joining as this system expands, do not have sufficient or necessary knowledge about cybersecurity, so many hackers take advantage of it, being decentralized and anonymous, no institution can act or defend new users who suffer phishing scams or scams, this type of scams are based on exactly copying a page of a project and that the user enters and enters his wallet and his keywords so that the scammer can access his wallet and withdraw all the funds available to the user, or send false rewards to the users so that they can claim them in their wallet and sign the transaction, what they really sign is to allow access to the wallet and have all their funds stolen.

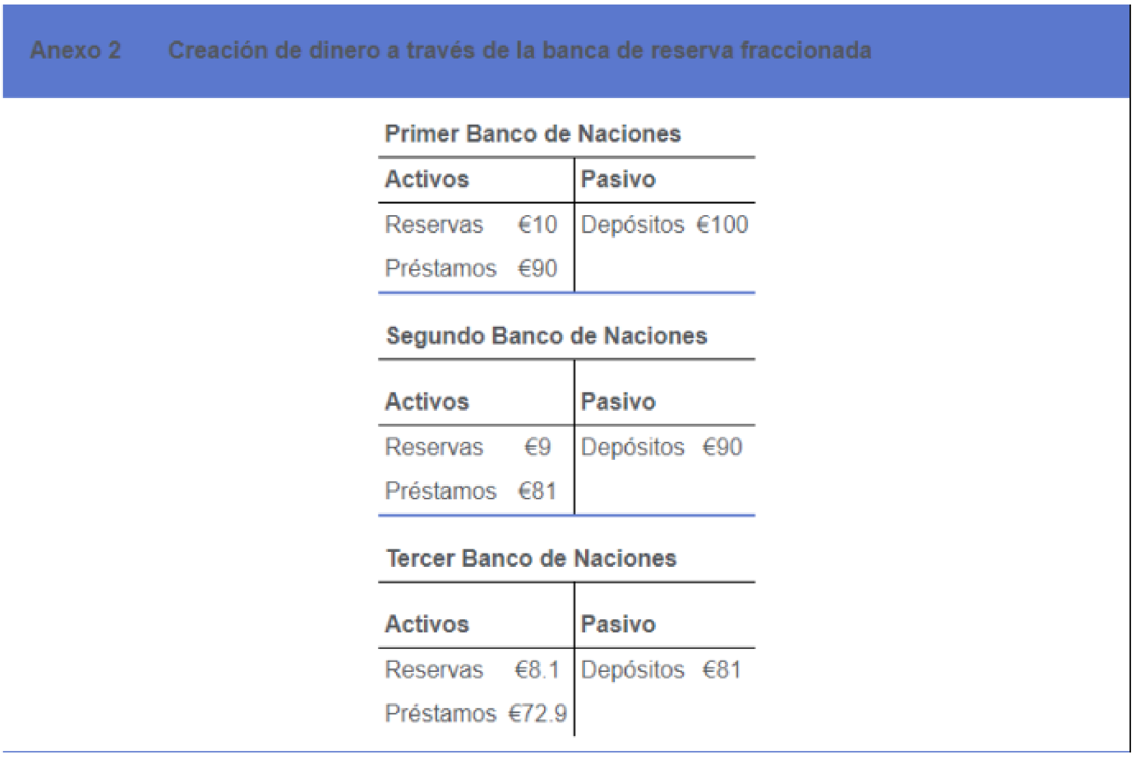
Another of the negative aspects are the network fees or congestion of this, since this system works through supply and demand of transactions, so the more transactions are made in the network the higher the fee that will have to be paid so that the transaction can be made, and if the offer of validators that make the transactions does not increase, many transactions are not made and are left waiting, it is one of the biggest problems that Ethereum has suffered, this has caused network fees higher than the value of the same transaction and very high waiting time, this is due to the consensus protocol used by the Blockchain, in this case Proof Of Work is the most secure protocol but the least scalable at the level of transactions by second.

6. Traditional Financial System

Banks are currently the means by which people, companies, institutions and governments can make transfers between them, borrow or lend money, all this makes the economy move, because if someone asks for a loan it is because they need money to buy some good or service and that means consumption, which translates into boosting the economy, that is why the economy depends so much on banks, if they offer loans at very low cost, borrowers have very little cost to request that money and go into debt to be able to acquire more goods and services, this causes an increase in consumption and production of a country, but what happens if this is done constantly? As money is not finite, that is, it does not have a maximum amount fixed in circulation but is created out of thin air and without limits, this causes that the greater the supply of money the lower its value, that is known as inflation.

Through banks people deposit their savings, so that they keep them and can lend that money to other people in exchange for a return.

This is done through fractional reserve banking [20], banks are obliged to hold only a small percentage of the capital deposited by customers, the rest can be lent to other customers as shown in figure number five and thus get interest on those loans.



Anexo 2 Creación de dinero a través de la banca de reserva fraccionada

Primer Banco de Naciones

Activos	Pasivo
Reservas €10	Depósitos €100
Préstamos €90	

Segundo Banco de Naciones

Activos	Pasivo
Reservas €9	Depósitos €90
Préstamos €81	

Tercer Banco de Naciones

Activos	Pasivo
Reservas €8.1	Depósitos €81
Préstamos €72.9	

Ilustration number 5. Ejemplo del sistema de reserva fraccionaria. Source: Own.

In this way, following the example of illustration number five, with a first deposit of € 100, € 171 has been created making loans, thus increasing the money supply in circulation from "nothing".

6.1 Advantages

The main advantage offered by traditional finances are the security when it comes to guarding your assets, they have very sophisticated security systems so that users can deposit their funds without having to worry about being stolen.

The personal treatment with users is one of the advantages of this financial model, but that is losing strength every time, customers have a team of professionals who can solve all the problems or doubts that may arise with their funds in a more personal and safe way. At the same time, they offer financial advice to manage these assets and obtain a return for them in a personalized way.

The second point is linked to another advantage, which is access to finances for non-digitized users, who do not have enough knowledge to manage their funds in a totally digital way.

On the other hand, an advantage of traditional finance is the support offered by these institutions for any problem or error that may have happened with a transaction.

6.2 Disadvantages

A disadvantage of this system is that institutions have all the personal information of all users in their centralized databases, vulnerable to possible hacks with which the private information of all customers could be accessed.

The time of transfers between accounts is usually from 24h to 48h business, having to wait days to be able to make a transfer and have the funds available. And wait until it is a working day, thus limiting the freedom of users when making any transaction, also freezing the client's funds if they consider it necessary.

Another aspect to highlight is the privacy when making transactions, since in many cases the bank itself asks you for information about the operation that is going to be carried out looking for some type of explanation by the client.

Maintenance fees and any other type of fees are factors to take into account in this system, since they charge all kinds of commissions for keeping your funds in the account and for operating with it, often becoming completely disproportionate.

7. Differences between Centralized Finance and Decentralized Finance

The main difference between these two types of finance as its name suggests is decentralization, in traditional finance, all transactions, custody of assets, security ... They are centralized in an agency that controls 100%, unlike decentralized ones, which are not controlled by a third party but the user himself is the one who stores and guards his assets and the network through which the transactions are made is the one that verifies all the operations thanks to the validators who are in charge of it in exchange for certain rewards.

Another difference would be the identification of users, in traditional finance it is necessary to identify yourself by offering your personal data that are stored in the databases of institutions, while in decentralized finance it is not necessary any type of identification, since they are completely anonymous.

On the other hand, transparency in transactions is a big difference between the two types of finance, since in the traditional ones the information they offer is what the institution wants, while in the decentralized ones all the information is public and auditable being able to follow the trace of any transaction through the blockchain.

Maintenance fees is another difference, in the traditional ones the commissions charged by banks for maintaining the account are very common, while in the decentralized ones, those commissions do not exist since as we have mentioned above the user himself is the one who is in charge of the custody of his own assets.

The money issuance system is a big difference between these two types of finance, in traditional finance the issuance model is based on inflation, issuing more and more money supply unlimitedly, unlike in the decentralized model, it is true that there are projects with moderate inflation, but, most projects have a deflationary model as is the case of Bitcoin that its issuance is a maximum of 21 million, or unlike other projects, which do not have an established maximum offer but more tokens are eliminated from the market than are issued such as Ethereum 2.0.

8. Examples DeFi Projects

There are thousands of DeFi projects that replace many of the operations that are carried out in traditional finance, such as loans or brokers / exchanges, and little by little new solutions are emerging that improve the previous ones and implement more utilities. In this paper we will discuss two of the most popular protocols within the DeFi sector.

The first is Compound, a DeFi protocol of decentralized lending of the Ethereum blockchain.

And the second project we will discuss is Uniswap, one of the first decentralized Exchanges of the Ethereum blockchain, a protocol to be able to exchange cryptocurrencies in a decentralized way.

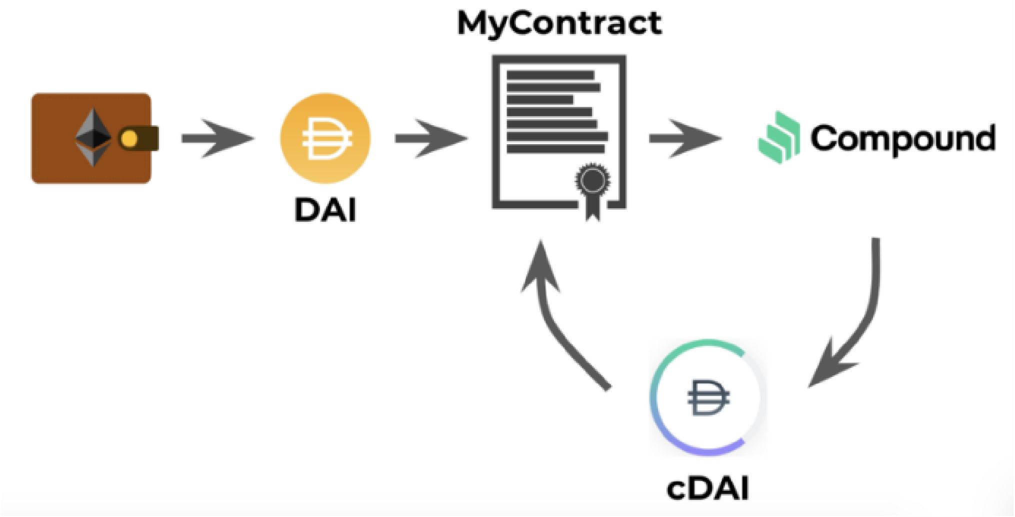
8.1 Compound

Compound is one of the most TVL DeFi protocols, totaling approximately $4.11 billion. It is a DeFi protocol of the Ethereum blockchain. Compound is a money market protocol, that is, it establishes money markets of groups of assets with algorithmically generated interest rates, based on the supply and demand of the asset.

In compound there is the possibility of being able to lend and borrow many assets, whether volatile such as ETH (Ethereum) or stablecoins such as USDT (Tether).

The Smart Contract that is in charge of the Compound protocol is the EVM (Ethereum Virtual Machine) along with the cTokens, which are the means by which the protocol is interacted, these are CErc20 and CEther, the first represents an underlying ERC-20 token, which translates into a token of the Ethereum blockchain, while the second involves Ether, an ERC-20 stablecoin.

The operation of the money market is based on forming a group of asset deposits such as USDT or ETH. This system creates groups so that users offer liquidity and lenders can borrow, in this way borrowers do not have to wait for any loan to mature to be able to withdraw their funds and can withdraw them at any time, this mechanism is much more flexible than a peer to peer system since it offers much more liquidity, unless all the group's assets are already borrowed, but the protocol incentivizes liquidity through its algorithm.



Ilustration number 6. Compound supply ERC-20 tokens. Source: https://medium.com/compound-finance/supplying-assets-to-the-compound-protocol-ec2cf5df5aa

8.1.1 Lending

To be able to lend to the protocol, it is necessary to deposit any cryptocurrency that accepts the protocol, such as USDT, and in exchange you receive a cToken that represents the asset you have lent plus the interest generated by the loan.

With those cToken, being underlying assets of the ERC-20 token as I have explained above, they can be used anywhere on the Ethereum blockchain.

8.1.2 Borrowing

To borrow in the compound protocol, it is necessary to deposit cTokens in the contract as collateral, in this way this guarantee can be used anywhere on the Ethereum blockchain.

The main parameter when applying for a loan is the borrowing capacity, which will vary depending on the assets that the borrower has to be able to co-outsource the loan and the quality of these assets.

Compound defines a loan-to-value (LTV) ratio for each loan through the Comptroller tool, which focuses on risk management and determines how much collateral borrowers should hold, borrowing capacity, and when their loan will be liquidated.

That is, it indicates what percentage of the asset contributes to the borrowing capacity of a debt position. LCTs vary between 0-1 depending on the volatility of the collateral provided asset and its liquidity. If the asset contributed is a stable and liquid asset, such as a stablecoin, the LTV will be high so the borrowing capacity will be higher, if on the contrary the asset is volatile and with less liquidity, the LTV will be lower, thus reducing the borrowing capacity.

If a wallet contains an X asset with an LTV of 80%, only 80% of the value of asset X will be considered as borrowing capacity.

Compound's Smart contract adds the value of all the collateral assets of the wallet and multiplies them by its LTV indices in order to determine the total debt capacity of the user.

8.1.3 Interest Rate

To determine the interest rate at which lenders lend and borrowers borrow, the Compound protocol uses an interest rate algorithm based on the supply and demand of loans. The algorithm receives the utilization rate of the protocol pool, that is, how much of the pool is borrowed.

The algorithm increases the interest rate to borrowers and offers more interest to lend to lenders as the utilization rate increases.

On the other hand, if the index decreases, the borrower will pay less interest on the loan, which translates into lower interest for the lender. In this way the algorithm incentivizes the loan when the utilization rate is low and discourages the loan when the index is high.

The utilization ratio U for each marker unifies supply and demand into a single variable:

$$U_a = Borrows_a / (Cash_a + Borrows_a)$$

8.1.4 Liquidations

If the borrower's borrowing capacity decreases, due to the depreciation of the assets of its collateral or the appreciation of the borrowed asset, the protocol launches the "liquidateBorrow" function, which exchanges the borrowed asset for the value of the collateral at a slightly better price than the market. In this way, arbitrage agents act quickly to reduce the borrower's exposure to debt and thus eliminate the risk of the protocol.

In order for the liquidateBorrow function to work properly, Compound uses the Comptroller tool discussed above.

In order for it to carry out the risk assessments, amount of collateral, borrowing capacity and timing of the loan settlement, Comptroller uses the Price Oracle system by which, through oracles [21], it collects the information on the price of the assets of the ten most important exchanges.

8.2 Uniswap

Cryptocurrencies apart from offering decentralized lending protocols, there are also projects focused on creating Decentralized Exchanges (DEX) as is the case with Uniswap.

Uniswap was one of the first projects that solved one of the problems that existed in the DeFi ecosystem, which is to be able to exchange some cryptocurrencies for others in a decentralized way, without having to be registered on any platform and completely anonymously, this is achieved through a chain system, of smart contracts hosted on the Ethereum blockchain, which has implemented an automated liquidity protocol AMM (Automated market maker).

The protocol used by uniswap is based on liquidity pools, that is, to be able to acquire a token, for example, ETH (Ethereum) you must contribute another one different from the pool to be able to keep the same amount of the token that you contribute in ETH. If you have 3000 USDT (Stablecoin) and you want ETH, you would contribute to the pool 3000 USDT along with the commission for the exchange and the pool would give you 1 ETH approximately.

The pool system works with pairs, that is, the protocol creates pairs depending on the demand for these, for example, ETH / USDT, in the pool there must always be the same amount of both assets, so if you have both you can provide liquidity to the pool of both tokens and receive a return, this is obtained from users who acquire one of the two tokens in the pool that pay a commission for the transaction.

8.2.1 Liquidity Pools

The system of liquidity pools has an important feature when it comes to providing liquidity, it is the impermanent loss, liquidity pools always have to maintain the same value so if two different assets are deposited to a pool, the sum of the two assets always has to remain stable, The Smart contract what it does is that if you deposit a volatile asset together with another stable one, such as ETH/USDT, if ETH increases in value, the contract will sell part of your ETH and compensates it with USDT to maintain the value of the pool.

In this way if you deposit ETH/USDT to the pool to obtain a return by providing liquidity, and the price of ETH increases, you will lose amount of ETH and it is possible that your return after all is lower than if you had not contributed liquidity to the pool, by the impermanent loss.

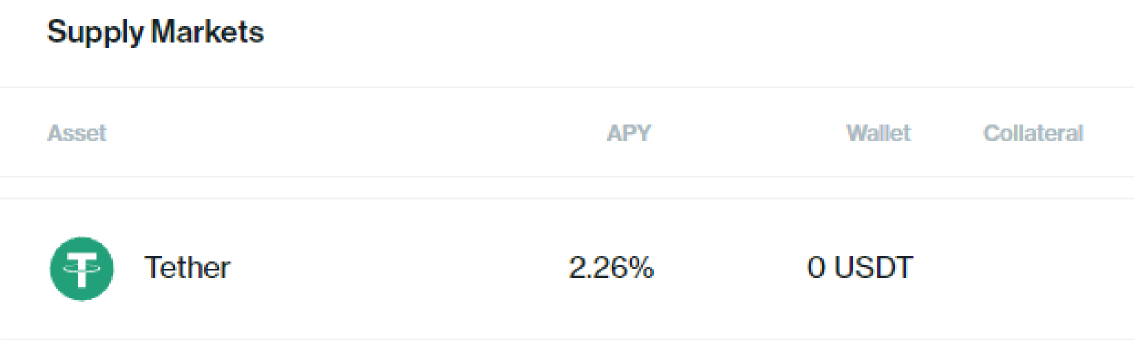
9. Passive Returns

Within the two types of finance there are different methods of generating returns passively without having to be exposed to volatility. In this work I detail two ways to obtain returns in both centralized and decentralized finance.

9.1 DeFi Strategy

Once two of the most important projects in the sector have been explained, I will explain how passive returns can be obtained in a totally decentralized way and reducing risk as much as possible.

Compound offers an APY (Annual Percentage Yield) of 2.26% at the moment, in the USDT stablecoin as can be seen in figure number seven. In order to obtain this performance, it is necessary to provide liquidity to the Compound protocol with the USDT stablecoin, through any wallet that the protocol supports, such as Metamask, the most popular hot wallet in the entire cryptocurrency sector.



Supply Markets

Asset	APY	Wallet	Collateral
Tether	2.26%	0 USDT	

Ilustration number 7. Compound Supply Markets. Source: https://app.compound.finance/

Just by providing liquidity, you can obtain an annual return of 2.06%, without suffering the volatility of cryptocurrencies and reducing the risk as much as possible, this is one of the best options to maintain the liquidity of a portfolio generating returns and not have the investment portfolio exposed to high volatility.

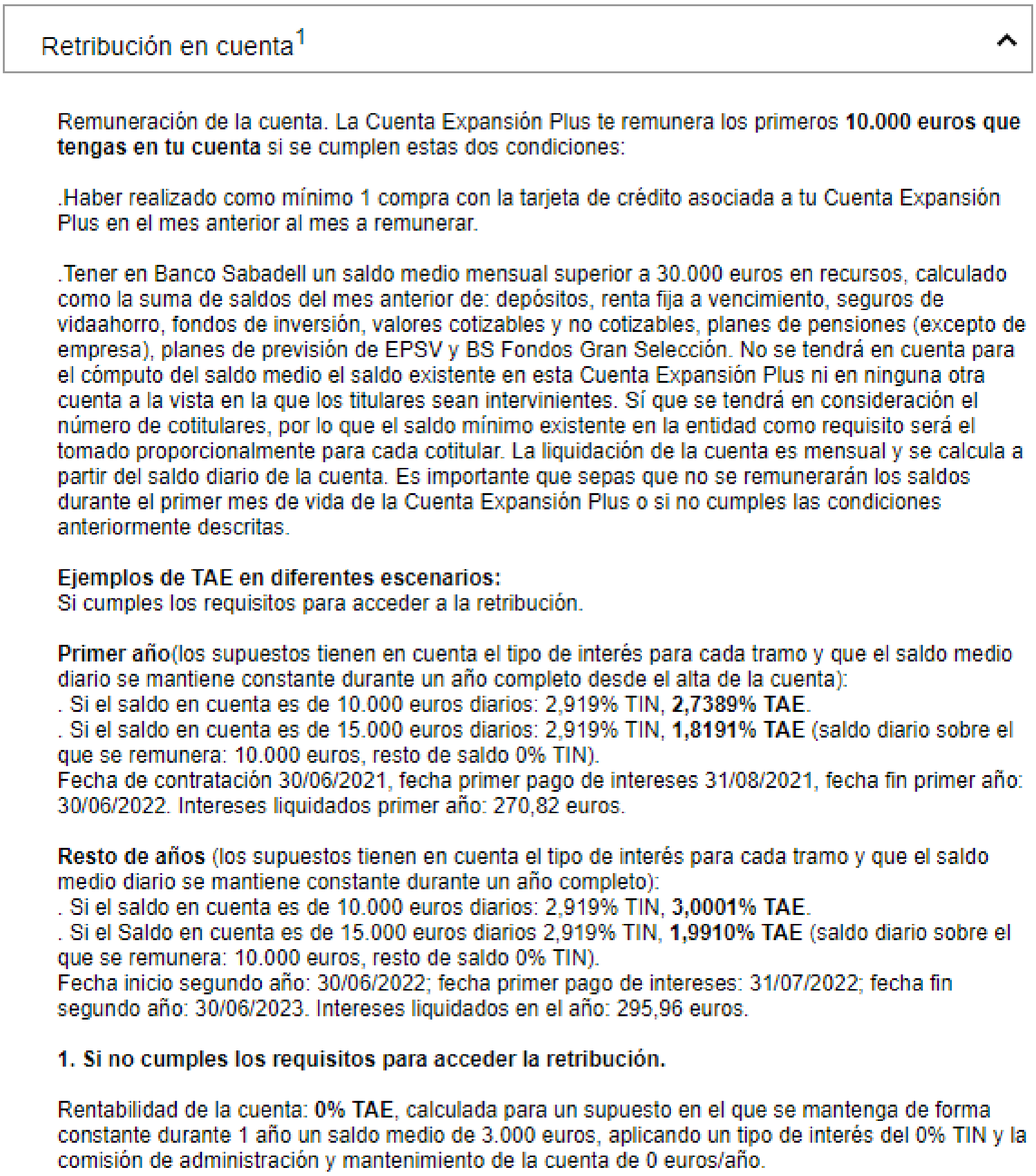
These returns in stablecoins are not permanent, since as they are regulated with supply and demand, so, if the protocol detects that there are more lenders than borrowers, the APY will decrease, and if, on the contrary, the demand for USDT loans increases, the APY will increase.

9.2 Traditional Finance Yields

In traditional finance, little by little, banks have been offering a lower profitability to customers for depositing capital in their bank accounts. But they also use that capital to lend it and thus obtain a return without benefiting the users who deposit that capital.

As we can see in illustration number eight, the Sabadell bank in one of its savings accounts that offers the most profitability, the Expansión Plus account, the annual return during the first year for having deposited € 10,000 constantly is approximately 2.73%, on the other hand if that account increases in amount more than € 10,000, the yield is 1.81%, since the capital above € 10,000 is not remunerated. From the rest of the years, the profitability for € 10,000 increases to 3% and for a capital that exceeds € 10,000 the profitability increases to approximately 2%.

On the other hand, if the account decreases from € 10,000 it will not be remunerated. They also require an average monthly balance of more than € 30,000 between all accounts, which the client has in the entity to be able to remunerate the Extension Plus account. And have at least one monthly expense in the account so that it can be remunerated.



Retribución en cuenta[1]

Remuneración de la cuenta. La Cuenta Expansión Plus te remunera los primeros **10.000 euros que tengas en tu cuenta** si se cumplen estas dos condiciones:

.Haber realizado como mínimo 1 compra con la tarjeta de crédito asociada a tu Cuenta Expansión Plus en el mes anterior al mes a remunerar.

.Tener en Banco Sabadell un saldo medio mensual superior a 30.000 euros en recursos, calculado como la suma de saldos del mes anterior de: depósitos, renta fija a vencimiento, seguros de vidaahorro, fondos de inversión, valores cotizables y no cotizables, planes de pensiones (excepto de empresa), planes de previsión de EPSV y BS Fondos Gran Selección. No se tendrá en cuenta para el cómputo del saldo medio el saldo existente en esta Cuenta Expansión Plus ni en ninguna otra cuenta a la vista en la que los titulares sean intervinientes. Sí que se tendrá en consideración el número de cotitulares, por lo que el saldo mínimo existente en la entidad como requisito será el tomado proporcionalmente para cada cotitular. La liquidación de la cuenta es mensual y se calcula a partir del saldo diario de la cuenta. Es importante que sepas que no se remunerarán los saldos durante el primer mes de vida de la Cuenta Expansión Plus o si no cumples las condiciones anteriormente descritas.

Ejemplos de TAE en diferentes escenarios:
Si cumples los requisitos para acceder a la retribución.

Primer año(los supuestos tienen en cuenta el tipo de interés para cada tramo y que el saldo medio diario se mantiene constante durante un año completo desde el alta de la cuenta):
. Si el saldo en cuenta es de 10.000 euros diarios: 2,919% TIN, **2,7389% TAE**.
. Si el saldo en cuenta es de 15.000 euros diarios: 2,919% TIN, **1,8191% TAE** (saldo diario sobre el que se remunera: 10.000 euros, resto de saldo 0% TIN).
Fecha de contratación 30/06/2021, fecha primer pago de intereses 31/08/2021, fecha fin primer año: 30/06/2022. Intereses liquidados primer año: 270,82 euros.

Resto de años (los supuestos tienen en cuenta el tipo de interés para cada tramo y que el saldo medio diario se mantiene constante durante un año completo):
. Si el saldo en cuenta es de 10.000 euros diarios: 2,919% TIN, **3,0001% TAE**.
. Si el Saldo en cuenta es de 15.000 euros diarios 2,919% TIN, **1,9910% TAE** (saldo diario sobre el que se remunera: 10.000 euros, resto de saldo 0% TIN).
Fecha inicio segundo año: 30/06/2022; fecha primer pago de intereses: 31/07/2022; fecha fin segundo año: 30/06/2023. Intereses liquidados en el año: 295,96 euros.

1. Si no cumples los requisitos para acceder la retribución.

Rentabilidad de la cuenta: **0% TAE**, calculada para un supuesto en el que se mantenga de forma constante durante 1 año un saldo medio de 3.000 euros, aplicando un tipo de interés del 0% TIN y la comisión de administración y mantenimiento de la cuenta de 0 euros/año.

Ilustration number 8. Retribución Cuenta Expansión Plus, Banco Sabadell. Source: https://www.bancsabadell.com/cs/Satellite/SabAtl/Cuenta-Expansion-Plus/6000028476345/es/

As we can see, the profitability is minimal for having deposited practically € 40,000 since you need € 10,000 in the account and another € 30,000 in different accounts of the same bank.

So, the real return is approximately 0.68% on all the capital contributed to the entity.

9.3 Differences Between Both Strategies

If we compare the first most basic investment strategy in DeFi with that of savings of the Sabadell bank, we can observe the return offered by the DeFi protocol compared to the capital you need to deposit in the bank, it is much higher.

In the DeFi protocol there are no requirements to deposit your savings, there are no minimums to deposit, unlike the Sabadell savings account.

You deposit what you have, whenever you want and without any type of bureaucratic or intermediary procedure, in this way anyone can access that return regardless of the capital.

On the other hand, it is not necessary to have the capital a minimum of time or have to spend a minimum of times a month to obtain the return.

10. Conclusion

In conclusion, cryptocurrencies and Blockchain technology are a reality today, thanks to this technology, people can have more options for finance, have more decision about our capital and organize ourselves in a totally decentralized, secure and without intermediaries.

Decentralized Finance is a small demonstration of all the potential they have, as we have been able to demonstrate, in the field of investment and profitability, these offer better returns than those that can be offered by any bank, investment fund ... And without being exposed to the volatility of these, which is one of the factors why traditional finance professionals do not invest.

The DeFi are increasingly taking more prominence as we have seen in the TVL of the protocols, for the freedom they offer, for example, when entering and leaving different DeFi protocols without the need for authorizations from third parties or bureaucratic processes and the power it gives users over their assets, as users are always in full control.

Currently I do not consider that they can be a substitute for traditional finance, there is a lack of adoption by society that is gradually being achieved, it is a slow process, since going to have all the control of your money is complicated, it may sound strange, but it is the reality, for example, currently in the war between Ukraine and Russia we have unfortunately been able to observe how Ukrainian citizens, wanting to leave the country, have not been able to withdraw all their savings that they had in the banks, since as I said before, they are not obliged to retain all deposits effectively, and the "financial corralito" occurs. all citizens want to withdraw the funds, but the bank does not have them, so they have a maximum daily amount to be able to withdraw.

With cryptocurrencies this would not have happened since your capital is available anywhere in the world with only an internet connection, having 100% control over the capital.

In short, cryptocurrencies and especially DeFi offer many opportunities in the field of investment and passive profitability, which, if applied in a correct way to today's society, can become a substitute or complement traditional finance as we know them.

11. Bibliography

[1] Bitcoin Whitepapper. (2008): https://bitcoin.org/bitcoin.pdf

[2]E-Gold (1996): https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html

[3]Crypto4Dummy. (2022) "¿*Qué es BitGold*?": https://crypto4dummy.com/que-es-bitgold/

[4] Bitcoin Whitepapper. (2008): https://bitcoin.org/bitcoin.pdf

[5] Bit2me Academy. (2021). "¿*Qué es una red P2P*?": https://academy.bit2me.com/que-es-una-red-p2p/

[6] LEMIEUX, Pierre. Who is satoshi nakamoto?. *Regulation*, 2013, vol. 36, no 3, p. 14-16.

[7] Coinmarketcap (2022). Top Cryptocurrencies: https://coinmarketcap.com/

[8] Ethereum Org. (2022)." *Introduction to Samart Contracts*.": https://ethereum.org/es/smart-contracts/

[9] Redes zona. (2022). "*Criptografía: Qué son los algoritmos hash y para qué se utilizan*": https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/

[10] Bit2me Academy. (2018). *"¿Qué es un nodo?"*: https://academy.bit2me.com/que-es-un-nodo/

[11] Bit2me Academy. (2017). *"¿Qué es Prueba de trabajo / proof of work (PoW)?"*: https://academy.bit2me.com/que-es-proof-of-work-pow/

[12] Bit2me Academy. (2021). *"¿Qué es un token?":* https://academy.bit2me.com/que-es-un-token/

[13] Coinbase. (2022). *"¿What is a stablecoin?":* https://www.coinbase.com/es/learn/crypto-basics/what-is-a-stablecoin

[14] Coinmarketcap. (2022). *"Top Stablecoins Tokens by Market Capitalization"*: https://coinmarketcap.com/view/stablecoin/

[15] Coinmarketcao. (2022). "*TERRA*"*: https://coinmarketcap.com/currencies/terra-luna/*

[16] Coinmarketcap. (2022). *TerraUSD:* https://coinmarketcap.com/currencies/terrausd/

[17] DeFi Llama. (2022). *Anchor*: https://defillama.com/protocol/anchor

[18] DeFi Llama. (2022*).” Total Value Locked All Chains”:* https://defillama.com/chains

[19] BIRYUKOV, Alex; KHOVRATOVICH, Dmitry; TIKHOMIROV, Sergei. Privacy-preserving KYC on Ethereum. En *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

[20] FRACCIONARIA, QUÉ LA RESERVA. POR QUÉ LA RESERVA FRACCIONARIA NO ES UNA INSTITUCIÓN DEL LIBRE MERCADO. En *IX CONGRESO DE ECONOMÍA AUSTRIACA*. 2016. p. 28.

[21] Etereum.org. (2021). “*Oráculos”:* https://ethereum.org/es/developers/docs/oracles/