



UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI

"M.FANNO"

**CORSO DI LAUREA MAGISTRALE IN ECONOMICS AND
FINANCE**

TESI DI LAUREA

CRYPTO-ASSETS AND DECENTRALIZED FINANCE

RELATORE:

CH.MO PROF. BRUNO MARIA PARIGI

LAUREANDO: MARCO CIVIERO

MATRICOLA N. 1130805

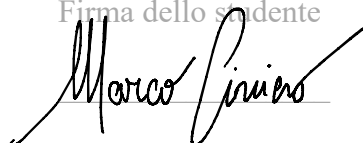
ANNO ACCADEMICO 2019 – 2020

Il candidato dichiara che il presente lavoro è originale e non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere.

Il candidato dichiara altresì che tutti i materiali utilizzati durante la preparazione dell'elaborato sono stati indicati nel testo e nella sezione "Riferimenti bibliografici" e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo alla pubblicazione originale.

The candidate declares that the present work is original and has not already been submitted, totally or in part, for the purposes of attaining an academic degree in other Italian or foreign universities. The candidate also declares that all the materials used during the preparation of the thesis have been explicitly indicated in the text and in the section "Bibliographical references" and that any textual citations can be identified through an explicit reference to the original publication.

Firma dello studente

A handwritten signature in black ink, reading "Marco Pinino", written over a horizontal line. The signature is cursive and stylized.

Ringraziamenti

Un ringraziamento speciale a Nicole, che mi ha accompagnato in questo lungo ed impegnativo percorso senza mai perdere la fiducia in me. Sin dall'inizio ti ho promesso che l'avrei portato a termine.

Un ringraziamento di cuore alla mia famiglia, in particolare a Flavio, difficilmente ce l'avrei fatta senza te.

Un grazie particolare a tutti i miei amici, in questi ultimi anni siete stati fondamentali. Vicini o lontani, il supporto morale che mi avete sempre dato è stato indispensabile.

Ringrazio Marco, un'amicizia ventennale ci lega, questa volta ti sei superato. Grazie di tutto!

Un ringraziamento a tutti quei colleghi che hanno avuto occasione almeno una volta di dimostrare interesse per i miei studi e i miei sacrifici al di fuori del lavoro. Tra di loro un grazie speciale a Matteo, quell'anno con te in sede è passato troppo in fretta!

Ringrazio il professor Parigi per tutti i preziosi consigli che mi ha fornito aiutandomi a redigere questa tesi.

“Trust is the raw material from which all types of money are minted”

Sapiens, a brief history of humankind,

Yuval Noah Harari

INDEX

1. Introduction and the scope of the thesis.....	1
Introduction.....	1
2. The new technology: The Blockchain.....	4
How Blockchains work.....	4
The Blockchain consensus mechanism.....	5
The network of the Blockchain: The nodes.....	6
The network of the Blockchain: The architecture.....	7
3. Crypto-assets.....	9
Cryptocurrencies as first application of the blockchain.....	10
Monetary policy in the cryptocurrencies framework.....	12
Bitcoin: The first Cryptocurrency.....	13
Value, Price and Bubble.....	15
Tokens.....	17
4. Stablecoins.....	20
Tokenized stablecoins.....	22
Collateralized stablecoins.....	23
Tether – tokenized fiat.....	25
MakerDao and the collateralized debt position.....	26
Collateralized debt position and target rate feedback mechanism.....	27
Nubit, an algorithmic stablecoins.....	29
From private to sovereign stablecoins: Central bank digital currency.....	32
The Digital Euro: The ECB’s CBDC.....	34
5. The project Ethereum.....	37
Ether Monetary Policy: “Minimum Necessary Issuance”.....	37
Ethereum Network Structure.....	39
Economics of Ethereum and Ethereum 2.0.....	39
Smart Contracts and Transactional costs.....	41
Smart Contracts and new kinds of governance models: the DAOs.....	42

ERC20 Tokens and Wrapped Bitcoin.....	43
Ethereum’s Markets.....	46
6. Decentralized finance.....	48
Introduction to Decentralized Finance.....	49
The Pros of a Decentralized Financial System.....	49
DeFI Structure	51
Main Business Models in Decentralized Finance.....	54
Numbers of DeFI Today.....	57
The Cons of Decentralized Financial System: Technical, Centralization, Liquidity and Regulatory Risks.....	59
7. Crypto World Regulation: How Cryptocurrencies And Decentralized Finance Relate To The EU Directives.....	63
Anti-Money Laundering 4 th And 5 th Directive.....	63
Aml5 Gaps And Next Steps.....	66
8. Conclusion.....	68
Crypto-assets: dynamics of the last years.....	68
Regulation and public opinion.....	70
9. Bibliography.....	73
10. Sitography.....	75

INTRODUCTION

The Blockchain technology is one of the most disruptive innovations developed in the last decades. It allows to collect, share and elaborate data through an online global database that anyone, having an internet connection, can view and use.

The term Blockchain derives from the structure of this technology: data is collected and divided into chronologically interconnected “blocks; the sequence of blocks is computed in a decentralized database existing on the net; the ledger is shared with each computer worldwide. The Blockchain is not just stored in one specific location or server with limited access.

The Blockchain guarantees its users transparency and immutability and its database ensures that no third party intervention is required. Each transaction, which is neither emendable nor erasable, is recorded and can be easily consulted all over the world.

The most revolutionary feature of the Blockchain is the decentralization of the ledger: the functionality of the whole system is no longer guaranteed by a central server or web domain but is rather unattended by the networks of its users. Thanks to this peculiarity, the Blockchain overturns the canonical concept of trust in a central entity and entrusts the control and regularity of processes to a refined cryptographic system.

The Blockchain technology is largely known thanks to its applications in the field of cryptocurrencies, in particular Bitcoin. Since the birth of Bitcoin, cryptocurrencies have been applied to a variety of Blockchain systems, ranging from internationally recognized payment systems to asset management and retail investment services provided by decentralized finance algorithms.

The scope of this thesis is to explore the financial applications of the Blockchain technology, with a particular focus on identifying the pros and cons of distributed ledger technologies as compared to traditional centralized finance.

The main target is the comparison of the intermediation cost of traditional banking with that of the new DeFI¹ system, with the aim of understanding whether the traditional banking sector could cooperate with – or implement – this new kind of technology or if these will remain separate alternatives for financial investors.

In order to describe and analyze the most innovative applications of the Blockchain in the financial field and the economic issues related to the topic, I decided to proceed with a bottom-up approach.

¹ Decentralized Finance, the new financial market sector based on the Blockchain technology.

As matter of fact, in the second chapter I will proceed with the basics, I will describe the composition and functioning of the Blockchain technology, as well as the peculiarities that differentiate it from other types of IT infrastructures. Once the foundations of the Blockchain have been dealt with, in the third chapter I will provide the reader with the declination of this technology in the economic and financial field, and I will proceed with an analysis and description of all the types of crypto-assets currently existing. I will focus particularly on the crucial issue of stablecoins, both because they represent a further turning point towards the greater fungibility of crypto-currencies, and because they represent the most studied research field by central banks and supranational institutions, that do not want to remain extraneous to the crypto world.

Unlike many studies and publications, I will just quickly mention the Bitcoin phenomenon. As matter of fact, I believe that, despite its fundamental role for the emergence of the crypto ecosystem in the eyes of the mainstream public, Bitcoin has already been extensively analysed from every point of view, including the big problem regarding the inefficiency and wastefulness of resources inherent in its operating system.

Instead, I will devote a chapter to Ethereum and the potential of its Blockchain network, which is fundamental for understanding the present and future applications that may occur thanks to its development.

Ethereum is currently the second most capitalized cryptocurrency in the world, behind Bitcoin, but its applications go far beyond a simple peer-to-peer payment system and digital currency.

As a matter of fact, almost all the DeFI platforms called Dapps (Decentralized applications) are based on the Ethereum Blockchain. The DeFI world will be described and analysed in the sixth chapter.

An important reasoning and reflection on the current regulation of cryptocurrencies and crypto-assets will be carried out in the seventh chapter. A fundamental milestone for the Crypto world will take place when the regulatory bodies decide to provide complete and comprehensive legislation regarding these innovative financial instruments. At the European level, institutions have begun to focus the spotlight on these technologies and in this part of my work I will discuss how the anti-money laundering directives in the world of cryptocurrencies are declined and the limits constraining them.

Finally, I will reserve a space for personal reflection on this emerging world by commenting on current news and regulatory developments inherent in this sector. In choosing these themes for the development of my master's thesis, the curiosity that prompted me to study and deepen this world was fundamental. I believe that today it is necessary and essential to study and understand these technologies, which in the most likely of hypotheses will determine a strong change in the finance and society of the future.

THE NEW TECHNOLOGY: THE BLOCKCHAIN

HOW BLOCKCHAINS WORK

Blockchain is a particular type or subset of the so-called distributed ledger technology (“DLT”) (R.Houben and A.Snyers, 2018). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), based on the exact same data records, which are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. Blockchain is a mechanism that employs an encryption method known as cryptography and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure –to which data can only be added and from which existing data cannot be removed – that takes the form of a chain of “transaction blocks”, which functions as a distributed ledger (H. Natarajan et Al, 2017). The result of these characteristics is an open, neutral, affordable and secure system, where it is no longer necessary to trust a central body.

The Blockchain can be considered as a distributed database in which each modification and addition made by one of its users (network nodes) creates a new "block" of information that is recorded. This new block is then broadcasted to every party in the network in an encrypted form (utilising cryptography) so that the transaction details are not made public (World Bank Group, 2017). Those in the network (i.e. the other network nodes) collectively determine the block’s validity in accordance with a pre-Defined algorithmic validation method, commonly referred to as a “consensus mechanism”. Once validated, the new “block” is added to the Blockchain, which essentially results in an update of the transaction ledger that is distributed across the network (Committee on Payment and Market Infrastructure, November 2015). The information that can be recorded in the blocks of a Blockchain can be of any type and any asset with a digital copy can benefit from transactions on the Blockchain.

Each user on the Blockchain has two keys available. A private key that is used to digitally sign the transaction the users want to carry out, and a public key, with a doublefold purpose:

- 1) it serves as an address on the Blockchain network;
- 2) it is used to verify a digital signature / validate the identity of the sender.

A user’s public and private keys are kept in a digital wallet or e-wallet. Such wallet can be stored or saved online (online storage is often referred to as “hot storage”)

and/or offline (offline storage is commonly referred to as “cold storage”) (ECB, February 2015).

THE BLOCKCHAIN CONSENSUS MECHANISM

Each node of the Blockchain can request the addition of new information in the ledger. This request is not immediately accepted and the transcription of this information is subject to the "general consent" of the whole network. The mechanism by which transactions are first validated and then transcribed is called the consensus protocol. In short, a consensus mechanism is a predefined specific (cryptographic) validation method that ensures a correct sequencing of transactions on the Blockchain (H. Natarajan et Al, 2017).

A consensus protocol can be built according to different criteria. The two most used criteria in the Blockchain field are Proof of Work (PoW) and Proof of Stake (PoS):

- Proof of Work: in PoW systems, the nodes of the Blockchain have to solve so-called “cryptographic puzzles” to add new blocks. The process of cryptographic solving is called “Mining”. All information previously recorded on the Blockchain and the new set of transactions are put together and computed through the Hash function ²to obtain the new block.

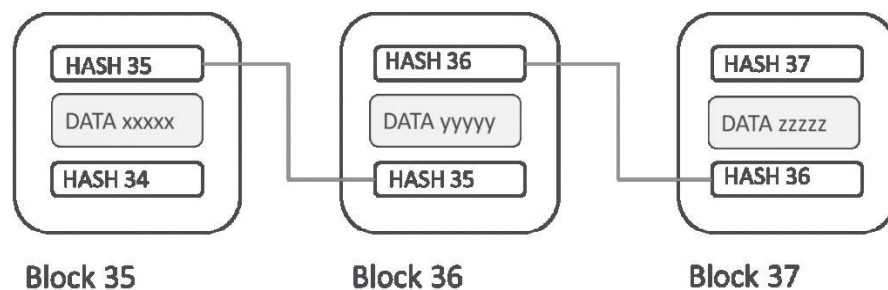


Figure 1: Recording new data process and Hash function

The node of the first chain which solves the cryptographic computation and subsequently validates the new block obtains a digital value reward in form of cryptocurrencies depending on the underlying Blockchain. This

² The Hash function is the algorithm that allows the Blockchain to standardize the dimension of the output (fixed dimension block) from the arbitrary dimension input. The input of a hash function can change but the output, called *hash*, has the same number of bits for the whole Blockchain. The hash function has three fundamental rules:

- Same inputs always bring to same outputs
- Little changes in outputs determine drastic changes in outputs
- The hash function is unidirectional. It is easy to compute outputs from inputs but it is quite difficult to obtain inputs from the hashes: the only way to reverse the function is computing all the possible combinations (brute-force method).

remuneration system guarantees the stability of the platform itself. Examples of Proof of work based Blockchains are Bitcoin, Litecoin, Bitcoin cash and Monero.

- Proof of Stake: In a PoS system, participants must prove ownership of a certain asset in order to become a “transaction validator” and participate in the validation process (which, in the case of this particular criterion, is called "forging") (EY, 2018). For example, in the case of cryptocurrencies, a transaction validator will have to prove his “stake” (i.e. his share) of all coins in existence to be allowed to validate a transaction. Depending on how many coins he holds, he will have a higher chance of being the one to validate the next block (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position). The transaction validator is paid a transaction fee for his validation services by the transacting parties (R.Houben and A.Snyers, 2018).

An important variable of the poof of work Blockchains is the hashrate, which represents the number of the hashes computed per second ($HR=H/s$).

The network hashrate is the sum of the hashrate of the miners, and the probability for a miner to first find the proof of work is equal to the hashrate of the miner divided by the network hashrate of the Blockchain.

The proof of stake protocol doesn't need computational power of the nodes, but it is rather based on the “staking rule” of the validators. This means that those with the majority of “stakes” in the Blockchain have the right and the duty to validate the transaction first. The majority of the stakes in the Blockchain is determined by the number of cryptocurrencies held by the participants. During the staking process it can be decided to lock tokens and exchange them with the right of validating the transaction and obtain a reward. The proof of stake protocol is much more efficient than the proof of work because it does not require lots of complex computations by the miners, thereby reducing in a not negligible way the costs for hardware and electricity (S.Lee, 2018).

THE NETWORK OF THE BLOCKCHAIN: THE NODES

One of the most important purposes of the Blockchain is to allow people from all the corners of the world to benefit from this technology without the intermediation of a central institution. The mechanism that allows this to happen is the network.

The network is the group of machines sharing information and working on the same ledger on the internet. Each computer is called a “node” of the network.

As far as the Blockchain network is concerned, there are two types of nodes: full nodes and light nodes. A full node downloads and archives completely the entire Blockchain in which is working and makes sure that each transaction follows the rules Defined by the system itself. A full node is always independent from others, propagating valid blocks and ignoring the invalid ones. Light nodes do not save the whole Blockchain but refer to the information reported by the nearest full node. Obviously the most secure way to use a Blockchain is through full nodes but the process would become long and cumbersome. On the contrary, using light nodes can be easier and faster but not independent (from full nodes) (Bianchi et Al, 2019).

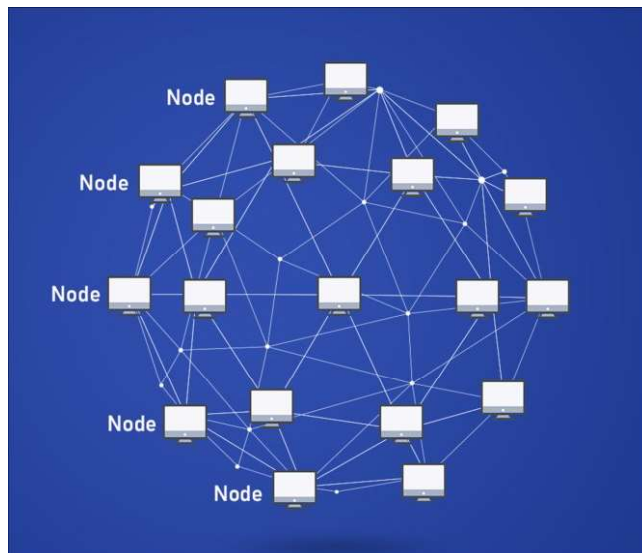


Figure 2: Blockchain nodes

THE NETWORK OF THE BLOCKCHAIN: THE ARCHITECTURE

The architecture of a network is determined by the structure and function of its nodes. As a result, three different models can be identified:

- Centralized architecture;
- Decentralized architecture;
- Distributed architecture.

A centralized architecture network is an infrastructure with a single point of failure: the central server. In case of failure of this single point, the whole system would crash.

In a decentralized architecture network instead, the information, data and files are distributed and duplicated among all the nodes in the network. As a consequence, all the participants can run the system without a single point of failure.

When a server is submitted to central authority but data and computations are distributed among different nodes, it is known as distributed network. This allows to minimize risks and management difficulties. Nowadays the most famous distributed networks are Google, Facebook, Amazon, etc. They don't work on a single database but they run their platforms thanks to many data centres working as big nodes of the network around the world.

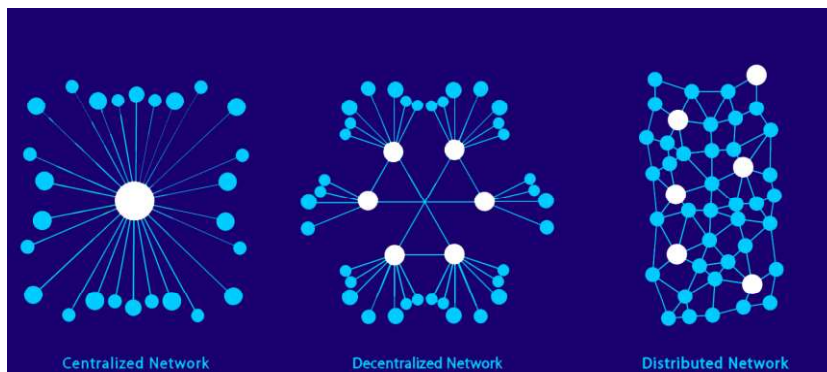


Figure 3: Different types of networks structure

There can be different models of Blockchains: permissionless (public) or permissioned (private).

Permissionless Blockchains are also called “public” and they are structured according to three main characteristics, namely, decentralized architecture, authority and a centralized logic. These Blockchains are often open source and they are created in order to allow everyone to participate into the network. Public Blockchains are the most used worldwide, but they may have inadequate characteristics in a corporate/industrial context. It is precisely in these sectors that private Blockchains have developed with the aim of protecting sensitive company data: they allow to establish which subjects are enabled to consult and modify recorded data. The inherent features of this type of Blockchain are a greater centralization and the presence of nodes with a greater degree of authority, which are responsible for verifying transactions.

CRYPTO-ASSETS

After having treated the structure, the technical characteristics and the functioning of the Blockchain, in this second chapter I will proceed with the discussion on the first applications of Blockchain technology in the financial economic field.

I will therefore talk about crypto-assets, in the most recent meaning of the term, and not just about cryptocurrencies.

The study "Crypto-assets, key developments, regulatory concerns and responses" commissioned by the ECON commission of the European Parliament justifies this choice of nomenclature in relation to the developments that have taken place in recent times, with the birth of many blockchains and private platforms. Since each of these is characterized by its own currency, as well as by different forms of governance and methods of consensus, we should no longer speak of cryptocurrencies but rather of "crypto-assets". This distinction highlights the emerging differentiation of financial instruments based on their purpose and function in "cryptoeconomy".

However, there is no single and unambiguous Definition of the term "crypto-assets", but instead, a series of different Definitions adopted by the major regulatory bodies around the world:

- the **ECB Crypto-Assets Task Force** Has Defined the term very narrowly as “any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity”;
- **IOSCO** has Defined the term as “a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity or security”
- the **FSB** has put forward a similar Definition and Defines the term as “a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value”. This Definition is also referred to in **BIS** documentation;
- in line with FSB’s Definition, the **ESMA** has Defined a crypto-asset as “a type of private asset that depends primarily on cryptography and DLT or similar technology as part of their perceived or inherent value”. ESMA uses the term to

refer both to so-called ‘virtual currencies’ and ‘digital tokens’ (which it Defines as “any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use”). According to the ESMA, crypto-asset additionally means an asset that is not issued by a central bank;

- the **EBA** has Defined a crypto-asset in a similar way as “an asset that: a) depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, b) is neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service” (R.Houben and A.Snyers, 2020).

Within the category of Crypto-assets, the distinction proposed by the authors is that between cryptocurrencies and crypto-tokens.

Cryptocurrencies or cryptocurrencies are those crypto-assets designated to cover the role of currency or to put into a more technical way, they were created to provide a peer-to-peer alternative to government-issued legal tender fiat-currencies.

Tokens, on the other hand, are crypto-assets that give their holders governance rights within the digital platforms in which they are issued. “They are digital representations of interests, or rights to (access) certain assets, products or services. Tokens are typically issued on an existing platform or Blockchain to raise capital for new entrepreneurial projects, or to fund start-ups or the development of new (technologically) innovative services” (R. Houben and A.Snyers, 2020).

CRYPTOCURRENCIES AS FIRST APPLICATION OF THE BLOCKCHAIN

The first and most important application of the Blockchain technology came with the introduction of cryptocurrencies. For the first time in history, non-physical and non-centralized means of payment were created, having the same validity as digital and as cash money.

“[...] It is therefore necessary to have an electronic payment system based on cryptographic evidence instead of trust, which allows any two counterparts to negotiate directly with each other without the need for a third party of trust”

(Nakamoto, A Peer-to-Peer Electronic Cash System 2008).

And it is precisely with these words that Satoshi Nakamoto, the pseudonym that gave birth to the bitcoin Blockchain, criticized the concept of trust that underlies any centralized monetary system. Indeed, cryptocurrencies, and above all, bitcoins are created to eliminate the variable of trust, which is essential with other forms of money. The term cryptocurrency refers to all digital assets based on Blockchain technology. Contrary to fiat money, cryptocurrencies are not legal tender and are not managed by any central financial institution.

All the technical characteristics of Blockchain technology, described in the first chapter, are typical of the cryptocurrencies to which they originate.

In essence, cryptocurrencies are a peer-to-peer version of electronic money, and their revolutionary feature consists in the fact that no third party is required to act as an intermediary in the case of a transfer of value between subject A and subject B.

Today there are about 5100 different cryptocurrencies³ and although they rest on different Blockchains, each with its peculiarities and heterogeneous characteristics, they share common properties that can be catalogued in the following way:

All cryptocurrencies are necessarily:

- Virtual: there is no physical equivalent of a cryptocurrency.
- Trustless: the system is managed by a distributed consent protocol.
- Global: There are no political borders for cryptocurrencies, anyone can transact.
- Safe: ownership of cryptocurrencies can only be demonstrated cryptographically, only those in possession of "private keys" can make transactions.
- Immutable: every transaction confirmed and added to the Blockchain cannot be modified or removed.
- Consent-based: Only the Blockchain's consent protocol can validate and Define the monetary policy of a given cryptocurrency.
- Open: There are no barriers to entry, anyone inside is free to innovate the technology used.
- Neutrals: They are systems without censorship and discrimination, transactions can be carried out without any limit and control (Bianchi et Al 2019).

³ Department for Economic, Scientific and Quality of Life Policies, 4 March 2020.

MONETARY POLICY IN THE CRYPTOCURRENCIES FRAMEWORK

Each economic and monetary system is subject to an independent central body which has the task of determining the supply of money in circulation. All decisions regarding the amount of money offered are called Monetary Policy.

The main objectives of monetary policy are the regulation of quantity, the growth rate and the distribution pattern of money.

In Blockchain-based monetary ecosystems, there is no central body that manages monetary policy. The quantity and growth rate of the coin is determined a priori by the Blockchain algorithm while the coins' distribution model is managed by the consensus protocol and mining.

Each cryptocurrency, based on a specific Blockchain, determines a monetary system in its own right. Each of these networks differs from the others on the basis of quantitative variables. The first of these is the total supply, which is the total amount of coins created up to this moment. The second is the circulating supply which is the quantity of "potentially expendable and transferable" money in circulation. The circulating supply differs from the total supply in that some coins created could be partially and momentarily "blocked" during the staking process (proof of stake protocol); or some coins could be paradoxically unusable if the holder were to lose the private key (digital signature) necessary for their disposal. In the latter case, the coins in question would be part of the total supply but not of the circulating supply.

Some Blockchains are also characterized by a third quantitative variable, the maximum amount of money that can ever exist within it. This derives from the fact that the algorithm underlying these Blockchains determines a priori the maximum amount of cryptocurrencies achievable, the most famous example is Bitcoin.

The "monetary policy" dictated by the Bitcoin algorithm is deflationary. The rate of growth of the supply of bitcoins decreases over time until it reaches zero. The motivation behind this decision was the desire to create a digital asset that could not only act as a decentralized means of payment but that replicated the scarcity of gold. Bitcoin, as a matter of fact, was also Defined as "digital gold" (N. Popper, 2016), that is, as a scarce resource that cannot be replicated.

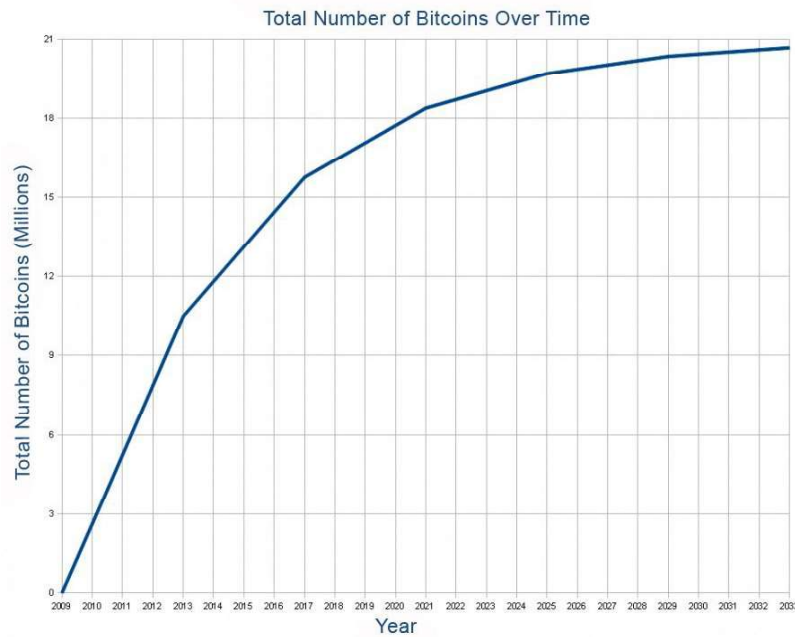


Figure 4 : The growth path of bitcoin supply

BITCOIN: THE FIRST CRYPTOCURRENCY

The great interest shown towards cryptocurrencies, which has progressively overcome the boundaries of the financial world, stems primarily from the great popularity of Bitcoin.

Bitcoin was the first cryptocurrency to be mined, as well as the first practical application of Blockchain technology.

The genesis block of bitcoin dates back to January 3, 2009, even if its origin is formally attributable to 2008, with the publication of the famous Whitepaper signed by Satoshi Nakamoto (previously mentioned).

This document promoted the idea according that, as a consequence of the deep financial crisis that has just exploded, a digital payment system should be created that is free from the conditioning and control of a central body, but which was totally characterized by a peer-to-peer network.

The bitcoin network is based on the consensus proof of work protocol: the moment a new block is added; the system generates a mathematically established reward for the miner who creates that block. The original reward set by the developers was 50 bitcoins per validated transaction. The Bitcoin algorithm automatically halves such reward every 210,000 blocks created. On average, it has been calculated that each block created on the bitcoin Blockchain takes ten minutes to validate. Given these characteristics, Bitcoin total supply is perfectly calculable at any time. At the time of writing, the money supply increases by 6.25 bitcoins for

each block created⁴ and the maximum coin limit allowed by the system will be 21 million bitcoins (Redman J.,2018), reachable around 2140.

As previously said, these characteristics make Bitcoin a deflationary system. Once the maximum amount of bitcoin Defined by the algorithm is reached, this economic ecosystem will reach an inflation rate equal to zero.

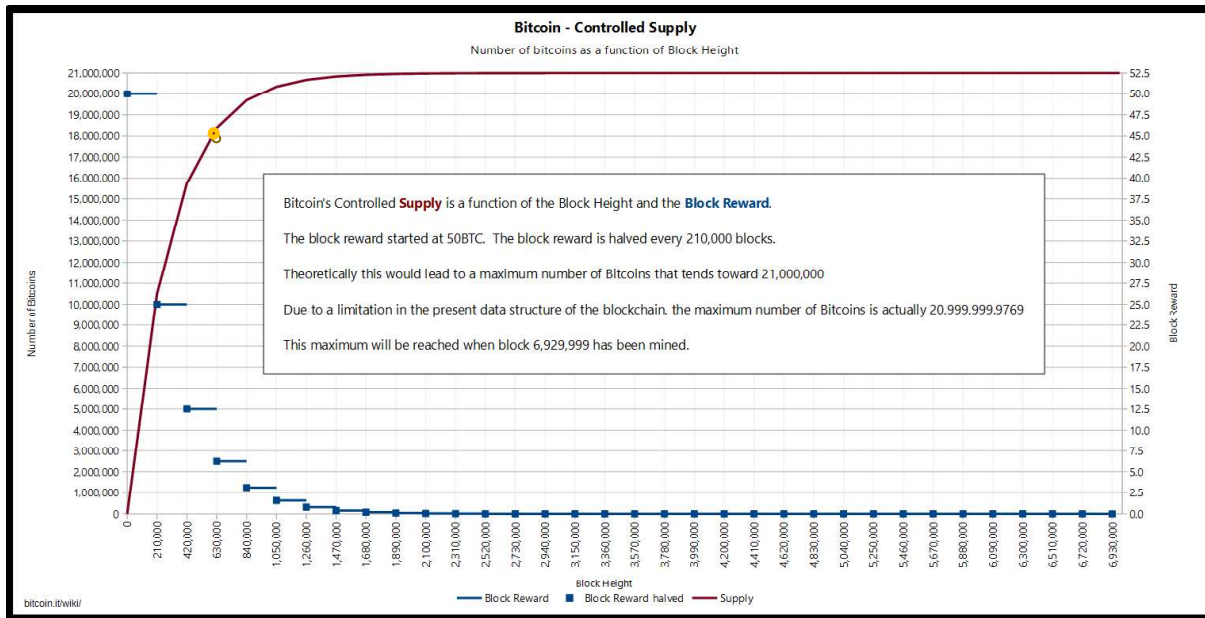


Figure 5 - Mining rewards vs Bitcoin supply over time

Figure 5 shows the supply of Bitcoin in relation to the number of confirmed blocks increasing over time (LHS) and the Block reward for miners completing new blocks (RHS).

Due to the decreasing remuneration and the complexity of the bitcoin mining computation increasing over time, one of the biggest criticisms of the bitcoin Blockchain by the community is about the energy sustainability of the system. Bitcoin is currently the largest project in the world to use consensus through proof of work, which, however, implies an important operational problem.

The consensus protocol requires an enormous amount of electricity that is used to keep the network running safely: the more energy and computational capacity is required, the higher the security level of the Blockchain will be. The security limit of the proof of work protocol is set at 51%. If 51% of the system's computing power is reached from a single Blockchain node, it would have the power to create and authorize blocks faster than anyone else, effectively monopolizing the Blockchain (Gervais et Al, 2016).

It is therefore necessary that the network requires such high computational power and energy expenditure. The high energy consumption is nothing more than the price to pay to ensure that

⁴ Showed by the yellow dot in the Figure 5

the limit of 51% of the computing power cannot be reached and exceeded in any way, so that the entire ecosystem is protected.

VALUE, PRICE AND BUBBLE

“With all of the calls of bubble, it’s worth remembering that we’re in the early stages of global adoption as well as the early stages of development of the technology”

(Ari Paul, Forbes 2017)

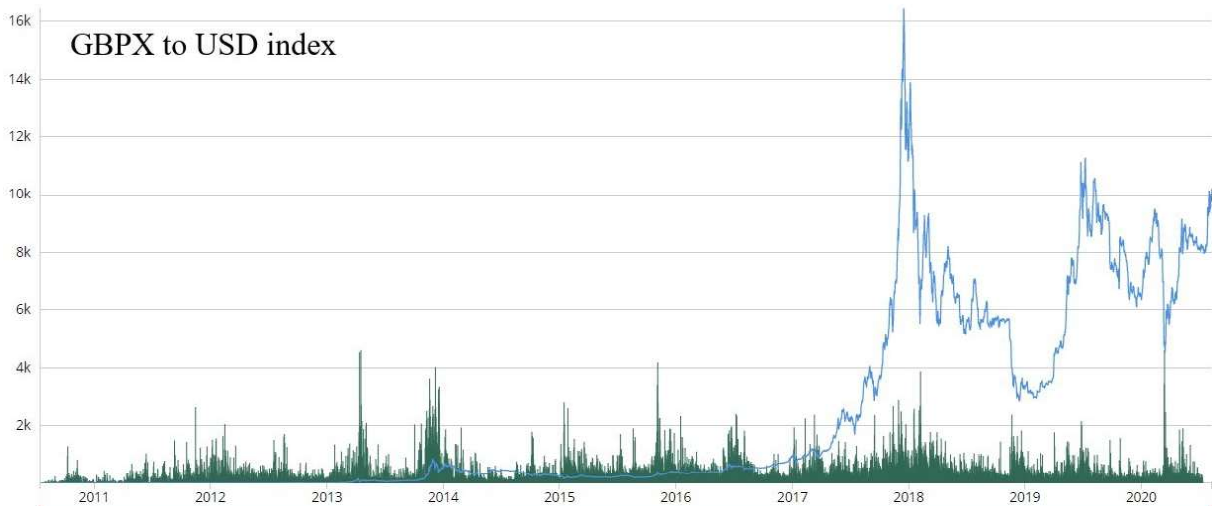


Figure 6: Global bitcoin price index 2010-2020

The GBPX index or (global bitcoin price index) is the index that detects the exchange rate of bitcoin with the main global currencies (USD, EUR, GBP, JPY, CNY, etc.) on a daily basis.

A quick glance at the trend of this index is enough to deduce that the price of bitcoin has suffered from heavy volatility caused by large speculative waves.

Bitcoin's value grew in 2017 from less than 1,000 to more than 20,000 USD, drawing global attention to this new market.

This exponential growth, followed by a crash of nearly 80% in value, made bitcoin the largest financial bubble in history, surpassing even the 17th century "Dutch tulip mania" (Torsten Dennin 2019).

A big dilemma that afflicts financial analysts around the world, therefore, is the determination of the intrinsic value of this cryptocurrency. Some economists, referring to the Fisher equation - which takes into account the total amount of bitcoins - the speed of transactions and the trading volumes, claim that the intrinsic value is between 20 and 25 dollars, which would show that the price market of Bitcoin is absolutely overvalued.

For the purpose of the study, it is useful to recall the Fisher “Quantity theory of money equation” applied to Bitcoin Framework:

$$M \times V = P \times Y^5$$

The equation $MV=PY$ means that if the product of M multiplied by V decreases, then the product of P multiplied by Y decreases as well (M. Zeller, 2019).

This economic model, however, takes into account only these current variables and completely ignores the future potential and all the applications that could be developed with this technology.

The most important supporters of Blockchain technology say that most of the value of bitcoin is attributable to the discounting of the value that this currency will have in the future when it is widespread and in common use.

In conclusion, we can say that the intrinsic value of Bitcoin is difficult to explain through a classic economic model, as a matter of fact, we are talking about a quite recent phenomenon, the potential of which is largely left to explore.

Unlike intrinsic value, the price of bitcoin is absolutely explicable with the “classic” model of supply and demand. Miners currently produce around 900 bitcoins per day, a portion of which is sold to cover electricity and IT operating costs. The price dynamics of bitcoin are therefore affected by both the daily supply, the price of electricity and how the supply is absorbed by the demand for the purchase of cryptocurrency on exchanges around the world.

There is no doubt, however, that the great interest in the world of cryptocurrencies that has arisen after the 2017 bubble has shifted the attention of retail and institutional investors towards these digital assets, causing a large increase in aggregate demand.

At the time of writing, Bitcoin's market capitalization is approximately \$ 200 billion, with daily trading volumes of \$ 35 billion and a "BTC dominance" (market capitalization of bitcoin on the total capitalization of cryptocurrencies) of nearly 60%⁶.

Faced with these numbers, the world of cryptocurrencies and in particular Bitcoin can no longer be considered a niche phenomenon, but instead one of rapidly growing global interest, which will radically change the world of economics and finance in the coming decades.

⁵ :

- M is *Money supply* in Bitcoin, M is equivalent to 21 million of Bitcoins (BTC).
- V is the *velocity of money*: this is the number of units traded during a defined period of time in the context of economic exchanges.

It is complex to define V for Bitcoin. Each transaction is recorded but it is hard to know whether it is a transaction to acquire a good or a service (a transaction in the economic sense), a transaction between two accounts held by the same person (with no economic impact) or a “donation” to another person or entity (which has a different impact than an economic transaction). Two sources give different conclusions:

- P is the *price of the goods and services in the same monetary unit*. If P decreases, it indicates a gain in purchasing power.
- Y: is the *economic output*. This is the number of goods and services produced available for purchase and sale. In the context of Bitcoin, very few goods and services are sold or purchased in BTC, and even more rarely exclusively in BTC.

⁶ According to Coinmarketcap.com

RANKING OF THE FIVE MOST CAPITALIZED CRYPTOCURRENCIES

RANK	NAME	MARKET CAPITALIZATION (Millions USD)	VOLUME (24h, Millions USD)	CIRCULATING SUPPLY (in its own currency)
1	Bitcoin	199.570,97	35.672,711	18.497.606 BTC
2	Ethereum	40.452,794	10.502,996	112.720.935 ETH
3	Ripple	10.920,933	1.573,420	45.097.364.449 XRP
4	Bitcoin Cash	4.241,613	1.378,162	18.525.469 BCH
5	Polkadot	3.703,626	393,470	852.647.705 DOT

Table 1: The ranking of the top 5 global cryptocurrencies⁷

Table number 1 ranks the top 5 crypto-currencies according to their market values: capitalization and daily trading volume. Capitalization is nothing more than the product between the daily price of the cryptocurrency and the quantity of it in circulation.

Bitcoin and all other listed cryptocurrencies are traded daily on cryptomarkets, the sum of all daily transactions determines the trading volume (reported in the fourth column of the table). The platforms where it is possible to buy, sell and exchange cryptocurrencies are the so-called "crypto-exchanges", which offer financial intermediation services and allow supply and demand to meet. The best Crypto-exchanges currently on the market are Binance with an average of almost \$ 5 billion in daily exchanges, Huobi Global with over \$ 1 billion in exchanges and Coinbase with around 250 million⁸.

TOKENS

As previously highlighted, there is no general Definition of crypto-assets, but rather a variety of interpretations proposed by regulatory bodies. It is interesting to focus on the taxonomy proposed by the European banking authority in this area. As proposed by the "EBA report with the advice for the European Commission on crypto-assets" of January 2019, the crypto assets that can be identified on the market are of three types.

⁷ According to Coinmarketcap.com

⁸ According to Coinmarketcap.com

The first one consists of "payment tokens", which are attributable to what we previously Defined as "cryptocurrencies"; the second is identifiable as "investment tokens"; finally, the third type is that of "utility".

The distinction between these last two categories of crypto-tokens is made on the basis of the purpose attributed to the specific token being issued. As a matter of fact, investment tokens offer their owners rights similar to those that confer dividends (EBA, January 2019) on a traditional investor. This type of tokens is generally issued to raise capital on the market during the ICO (initial coin offering) phase and show strong similarities towards traditional debt and equity instruments. Utility tokens differ as they have the function of guaranteeing their holder access and use of applications or services in a specific Blockchain network (S. Blemus and D. Guegan, 2019). Again, utility tokens can be issued for the purpose of raising resources for financing further development of the issuer's applications, products or services. Unlike investment tokens however, they are not intended to generate future cash flows for investors, but rather to have all the future benefits of the developed and improved platforms. Once both types of tokens have been issued, they can be listed on secondary markets called "crypto-exchanges" where they can be bought or sold in exchange for fiat money or other cryptocurrencies (M. Nannings, 2019).

RANKING OF THE FIVE MOST CAPITALIZED CYPTO-TOKENS

RANK	NAME	MARKET CAPITALIZATION (Millions USD)	VOLUME (24h, Millions USD)	CIRCULATING SUPPLY (in its own currency)
1	Crypto.com Coin	3.121,270	61.178,343	20.215.525.114 CRO
2	Chainlink	2.943,132	1.274,254	350.000.000 LINK
3	Unus Sed Leo	1.262,526	17.236,035	999,498,893 LEO
4	Wrapped Bitcoin	992.740	51,088	85,473 WBTC
5	Huobi Token	974.215	107,876	209,994,599 HT

Table 2: The ranking of the top 5 global Crypto-tokens⁹

As can be seen by comparing tables 1 and 2, crypto-tokens are financial instruments that are much less traded and capitalized than "canonical cryptocurrencies". This is due to two factors.

⁹ According to Coinmarketcap.com

Firstly, it reflects a chronological issue, as crypto-tokens conceived after the ordinary cryptocurrencies. Secondly, the tokens listed on the crypto market generically consist of assets launched by private platforms that intend to regulate monetary exchanges and decision making rights within them and through the use of their own currency.

Let's take the example of the Crypto.com coin, the first token by capitalization in the market, born in November 2018 (10 years after Bitcoin). As the name may suggest, this token is the trading currency within the Crypto.com platform. This consists of a large digital crypto exchange, a place where all the cryptocurrencies on the market are traded daily as a real stock exchange. At the time of registration, Crypto.com customers are required to open a digital "wallet" within the site for the deposit of their funds (a small part of such funds is renamed into CRO¹⁰ which are used to cover commission fees and fund management required by the platform). CRO's are the bargaining chip for any service offered within the site, and, given the fact that they are quoted in real time on the market, each customer is able to buy or sell them at will. Because of the fact that the platforms listed in the previous table issue their tokens within limited contexts, these crypto-assets have a lower volume of exchange and capitalization than cryptocurrencies.

¹⁰ Crypto.com coin symbol

STABLECOINS

Since their first introduction, Cryptocurrencies have attracted the attention of many, not because of the peculiarities of peer-to-peer digital payment systems, but rather due to the considerable price volatility that has occurred in the market. This market mechanism has made cryptocurrencies a kind of highly speculative financial instrument. On the other hand, the high volatility of the prices of these "assets", opens up many questions relating to the scalability of a technology which was born to create payment systems, - that is, means of exchange for goods and services - and is nevertheless strongly used for financial speculation purposes. Which economic operator would accept a currency that could suddenly depreciate as a means of exchange for its commodity?

The solution of this dilemma is given by the birth of the so called "Stablecoins".

Stablecoin is a variant or subcategory of cryptocurrencies typically pegged or linked to the price of another asset or a pool of assets, designed to maintain a stable value, stablecoins are intended to perform the roles of currency. Unlike traditional "non-backed" cryptocurrencies, which are generally decentralised, and do not have an identifiable issuer or at least not an institution that can easily be held accountable by or towards the coin's users, stablecoins typically represent a "claim" on a specific issuer or on underlying assets or funds, or some other right or interest. They are, in other words, backed by something and not just perceived to be something of value." (R. Houben and A. Snyers, 2020).

The first and most famous example of stablecoin on the market is the "Tether". This stablecoin has, to date, a market capitalization of more than 15 billion dollars and on average the daily trading volumes of this currency amount to 50 billion dollars¹¹. Its price is pegged to the US dollar and in the paragraph I have reserved for the economic functioning of its fixed exchange rate, I will go into more detail on this stable cryptocurrency.

An important and institutional study and in-depth analysis regarding stablecoins can be found in the ECB's occasional paper n.230 (D. Bullmann et Al, 2019).

The author begins this article by justifying the need to use stablecoins as compared to volatile cryptocurrencies. According to their thesis, Crypto-assets are characterized by a strong volatility of their prices, making them suitable to perform the function of money. As a matter of fact, cryptocurrencies cannot be considered a store of value, a means of payment and a unit of account. The stablecoins were introduced by their creators precisely to overcome these weaknesses and to ensure greater security for the revenues deriving from financial

¹¹ According to Coinmarketcap.com

transactions on crypto-assets. Secondly, the authors list different types of stablecoins based on the economic mechanism underlying the setting of exchange rates.

The article deduces the existence of a fundamental trade-off for the functioning of stablecoins: the higher the level of stabilization with respect to the target currency, the greater the need for centralization of the system towards a subject acting as guarantor; vice versa, the more decentralized and innovative the stabilization mechanism, the more the fixed price of the stablecoin is at risk.

The resulting criteria, therefore, are the existence (or absence) of an issuer who is responsible for the satisfaction of any related request; the degree of decentralization of responsibilities on a stablecoins initiative; and the underlying assets that stabilize the value in the reference currency.

“The stabilisation mechanism at the core of a stablecoin initiative is crucial to determining whether the units issued can maintain a stable value or not. Different stabilisation mechanisms may either require the intervention of accountable institutions, in the role of issuer and custodian, or delegate these tasks to stablecoin users”. (D. Bullmann et Al, 2019).

According to the authors' analysis, stablecoins can be Defined as:

- "tokenized funds" or “fiat collateralized” when they are collateralized by funds (denominated in fiat currency), held by an issuer that keeps them for the purpose of safeguarding and redeemability.
- "off-chain collateralized stablecoins" (if collateralized by traditional financial instruments) or “commodities collateralized stablecoins” (if commodities like gas, oil etc. are used as collateral), that require custody and are in the possession of the issuer until the user redeems the stablecoins, or the residual value in the event of default.
- "on chain collateralized stablecoins" or “crypto-collateralized stablecoins” when they are collateralized by other crypto-assets that can be accounted for in a totally decentralized manner without the need for an issuer.
- "algorithm stablecoins" or “non collateralized stablecoins” when the stabilization mechanism is totally based on the expectations of the purchasing power that will keep the currency following adjusted by some monetary supply function.

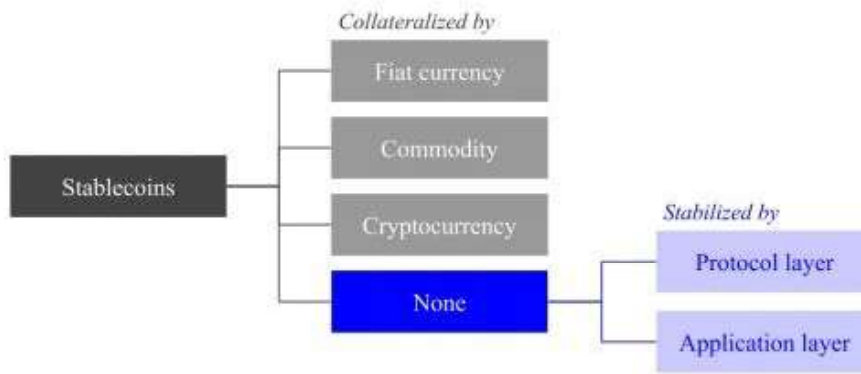


Figure 7 - Taxonomy of Stablecoins¹²

TOKENIZED STABLECOINS

This type of stablecoin is a fiat-collateralized currency which uses fiat money as collateral. Specifically, it employs a simple and intuitive mechanism that issues new stablecoin on condition that target pegged asset is collateralized and, like the gold standard, commits to exchange the stablecoin for collateral at a fixed rate at any time. Despite this simplicity, however, the fiat-collateralized stablecoin has a problem of requiring a centralized custodian to manage deposited collateral and issue new stablecoins (Makiko Mita et Al, 2015).

Specifically, this type of stablecoins are units of monetary value stored in a distributed ledger. Each of these units represents a claim to the issuer of stablecoins with respect to the funds it receives as a collateral from the user. The issuer can either hold the collateral himself or channel it to a person who carries out custody work. The issuing process takes place when the user deposits the collateral funds - denominated in fiat currency - in custody, and subsequently allocates the established amount of stablecoins to the user through a "smart contract" according to a certain exchange rate. In this case, the redemption process is the reverse of the issue. The user will return the stablecoins to the issuer and the latter will return the collateral through the custodian service. In fact, the operation of the transfer of funds within the distributed ledger is different, in that the movement of funds between different users is authorized by the networks itself and the collateral funds are not touched and are maintained by the issuer through the same smart contract.

The advantage of a tokenized stablecoin anchored to a fiat currency, compared to a volatile cryptocurrency, lies in its spendability and its redeemability at any time towards the same fiat currency. Furthermore, the advantage of a stablecoin compared to a traditional fiat currency is that, is that the former can be used as a means of payment in the new decentralized finance

¹² Makiko Mita et Al, 2015

systems via Blockchain, thereby guaranteeing a high level of privacy and cryptographic security.

COLLATERIZED STABLECOINS

The price stabilization process of collateralized stablecoins is similar to that of tokenized ones. Unlike the latter, however, the assets that are placed to hedge the collateralized ones can have volatile values over time and, therefore, there may be problems of under-collateralization.

To ensure that each stablecoin is guaranteed by collateral worth at least equal to the reference currency it must be corrected through "Margin calls". Generally, in order to allow users to react to the margin call before the stablecoin becomes under-collateralized, these cryptocurrencies are over-collateralized *a-priori*.

According to the occasional paper n.230 commissioned by the ECB, empirical evidence shows how users operating with collateralized stablecoins are inclined to deposit excess collaterals for two reasons. Firstly, to avoid criminal commissions (due to default of the collateral position) and secondly to manage the revenues of cryptocurrency transactions without the need for services of external platforms for conversion into any currency.

Each stablecoin initiative differs from the others for the choice of the "eligible" assets that are accepted as collateral. Furthermore, previously exposed, a further classification is made between "on-chain" and "off-chain" collateralized. In the former the assets are registered and managed completely in a decentralized way in distributed ledger technology, whereas the latter requires the presence of a number of parts that act as safekeeping.

Off-chain collateralized stablecoins are characterized by the fact that as eligible assets they also admit traditional financial instruments (not crypto-assets), which implies the necessary presence of an entity responsible for the custody of collateral assets and for their return. If requested by the user. The process of issuing stablecoins against the deposit of an "off-chain" collateral is similar to that of fiat-collateralized stablecoins, the only difference is the request for overcollateralization against the management of fluctuations in the price of the collateral. A characteristic feature of these stablecoins is the redeeming process, which can be voluntary or mandatory. The first type consists in a reverse process from that of issuing, which takes place if the user requests it. While the mandatory redemption occurs in cases where the value of the collateral falls below the threshold Defined as the "over-collateralization ratio", expressed in the fundamental rules of the stablecoin initiative in use. If the user does not restore the ratio against a margin call, the issuer instructs the custodian to liquidate the collateral, the proceeds of which will be used to buy back from the market the equivalent

number of stablecoins issued against the contract and eliminate them from the system. In the event that the sale value of the collateral exceeds the value of the stablecoins eliminated from the system, this sum will be paid to the user minus the penalty fees.

The stability of the system is guaranteed as long as the liquidation of the collateral occurs before it falls below the value of the previously issued stablecoins.

On-chain collateralization refers to all those assets in digital form, for which the presence of an entity that manages their custody, return or eventual liquidation on the market is not necessary to restore the position compliant with the "overcollateralization ratio".

The management of this type of stablecoin initiatives is entrusted in a decentralized way to the execution of smart contracts between users and broadcasters. The issue of stablecoins in this case begins directly with the direct sending of the on-chain collateral to the address of the smart contract. After the deposit of the collateral, the stablecoin units will be delivered to the user according to the established proportion. The redeeming process remains identical to the previous one in the event of a voluntary request by the user. The case of mandatory redemption is different, as the smart contract has no power to dispose of the under-collateralized assets. The smart contract will therefore need to find the necessary funds for the repurchase of the stablecoins in order to be deleted. These funds may either come from the commission earnings accumulated so far by the issuer or from ad hoc funds raised for the correction of anomalous positions. The correction takes place through the issue of new stablecoins with a higher "overcollateralization ratio" than the ordinary ones. The greater over-collateralization required in this case is rewarded through rights on the future profits that will be generated by the initiative.

The last type of stablecoins differs from the others in that it does not require any type of collateralization. The key idea underlying algorithmic stablecoins is the self-regulation of the market price in the reference country by means of the adjustment of users' future expectations, which can be attained through two types of stabilization mechanisms. The issue of these takes place through an exchange between on-chain assets that the smart contract will maintain in the form of reserves and not collateral. In these stablecoins systems we cannot speak of "redemption" but of contraction of the supply, which is used to stabilize the price in the event of excess supply. Such operation is similar to the "compulsory redemption" for previous types of stablecoins. The repurchase of excess stablecoins can take place either through the sale of future rights to the platform's profits or through the sale of reserves related to the stablecoins themselves to be eliminated from the market.

TETHER – TOKENIZED FIAT

The first example of tokenized stablecoin came with the birth of Tether. Reading the Tether whitepaper, an introductory document that presents the creative project of this stablecoin to the world, it is possible to understand that the intent of the creators was to create, for the first time, a cryptocurrency that benefited from the same characteristics of bitcoin: anonymity, decentralization and internationality. The step forward proposed by the founders of Tether was to exempt their cryptocurrency from strong speculative attacks that make the price of bitcoin unstable and very volatile.

All Tethers were initially issued on the same Bitcoin Blockchain in the form of a Cryptocurrency token, via the Omni layer protocol. Each Unit of this cryptocurrency is backed in a one-to-one ratio to the US dollar. The collateralized dollars are held at Tether Limited's warehouse in Hong Kong. Once issued, each Tether can be used, transferred, or spent in the same way as bitcoins or other cryptocurrencies with the advantage of having the price set at the dollar.

Originally, the Tether was designed to be pegged only to the us dollar, but after the issuance of the EUR Tether on the Ethereum Blockchain in 2018, the Tether can be considered a multicollateralized stablecoin because it maintains parity with the euro (EURT) and the dollar (USDT). However, it is important to underline that Euro tether represents only one percent of the total capitalization of tether and amounts to approximately 40 million tokens in circulation¹³ at the time of writing. The U.S. Dollar tether, instead, is the absolute ruler of the stablecoin market, both in terms of capitalization and market volume, we are talking about a market capitalization of about 14 billion dollars and a daily trading volume of about 46 billion dollars¹⁴. These numbers not only make it the main stablecoin on the market but also the third most widespread cryptocurrency globally preceded only by Bitcoin and Ethereum.

However, being a tokenized stablecoin, Tether requires a third party that acts as a custodian for the funds deposited for its issue. The presence of a third party represents a source of limitation of the decentralization of the system, as a matter of fact, even the founders admit that their implementation of the Tether stablecoin is not perfectly decentralized, but rather based on the function of custodian of Tether limited. However, they claim that this centralized solution lays the foundations for building future innovations aimed at eliminating these weaknesses. As a matter of fact, users who decide to adopt Tether are exposed to counterparty risk, which however resides in any traditional financial intermediation service solution. Once

¹³ According to Etherscan.io

¹⁴ According to Coinmarketcap.com

this common pitfall has been overcome, Tether offers the indisputable peculiarities of Blockchain technology and the price stability characteristic of a fiat currency.

In my opinion the Tether project was the first example of synthesis between the Blockchain philosophy aimed at total monetary decentralization and the current financial system based on intermediation. I believe as an observer that from this moment on more and more "hybrid" projects will come to light until mechanisms of total algorithmic decentralization are ready and ripe (if they ever will be) to replace traditional financial intermediaries.

In any case, the fact that tether offers a system a system subjected to the counterparty risk that is not totally decentralized, has not compromised its wide diffusion and use in the following years. As a matter of fact, its success derives also from the collaboration with important companies in the cryptocurrency market, in particular in wallets and digital exchanges. In the long list of collaborations, we include the main partners such as Omni, Kraken, Poloniex, Epay etc ...

MAKER DAO AND THE COLLATERIZED DEBT POSITION

As seen in the previous paragraph, the tether project was the first that proposed a concrete solution to the problem of the strong volatility of the prices of cryptocurrencies existing up to that moment. The great incongruity of this project, which was also recognized by its founders, is precisely the strong centralization of the entity that acts as custodian on collateral assets denominated in US dollars or euros. This feature makes Tether very fungible as a medium of exchange but it puts it in contrast with the cardinal principles of cryptocurrencies, that is, total decentralization.

A step towards building a solid decentralized stablecoin system came with the presentation of the "The DAI stablecoin" whitepaper published by the Maker team.

The Maker team, better known as MakerDAO, is an open-source project based on the Ethereum Blockchain born in 2014. The Maker protocol which is built on Ethereum allows users to create currency, this is called DAI, and is built as an on-chain collateralized stablecoin.

The whitepaper, published in December 2017, gives a clear Definition of the Maker protocol and the DAI project: Maker is a decentralized platform, based on the Ethereum Blockchain, which allows the stipulation of specific "smart contracts". These work as sequences of commands based on algorithms that allow to stabilize the value of the DAI (name of the stablecoin of Maker) through a dynamic system of "Collateralized Debt Positions" or "CDPs". Maker allows users to leverage their Ether denominated funds by converting them into DAI

stable currency. Making a parallel with the previous case, DAI is to Tether as Ethereum is to Bitcoin.

COLLATERIZED DEBT POSITION AND TARGET RATE FEEDBACK MECHANISM

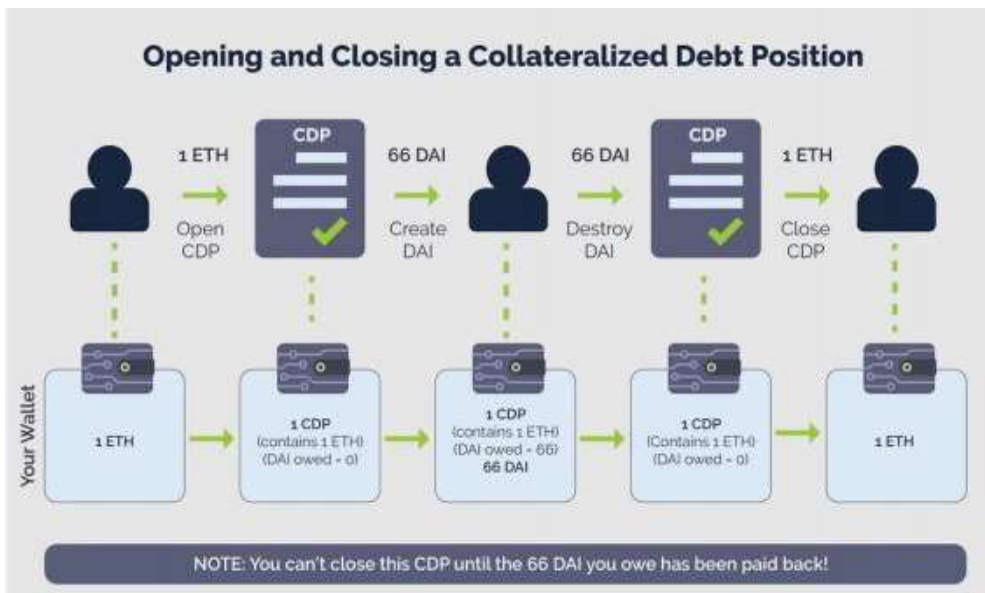
The stabilization mechanism of the DAI stablecoin price against the dollar takes place thanks to the execution of a series of computer operations dictated by an algorithm. Algorithms run on decentralized platforms such as Maker's are called smart contracts. Specifically, the object of my analysis is called Collateral Debt Position (CDP), a particular economic mechanism for the stabilization of the exchange rate. The stipulation of a CDP takes place when a subject decides to collateralise and block monetary sums against the issue of DAI stablecoins. Since the whole process rests on the Ethereum Blockchain, the blocked sums must necessarily be denominated in Ethers ("ETH"), the cryptocurrency that can be spent in this Blockchain.

The CDP provides a collateralization rate of 150%, that is, for each ETH of collateral deposited, the user will receive $0.66 \text{ DAI} \times \text{ETH/USD}$ ¹⁵ to be spent, in the Blockchain ecosystem, as a stable currency anchored to the dollar without risking any type of volatility that would occur by spending ETH. From an economic point of view, the overcollateralization rate of CDP is the opportunity cost of obtaining a currency without price fluctuations in the face of giving up a volatile currency.

If the user decides to close the CDP position, he will have to pay his debt in DAI and collect the proportional share of ETH initially given as collateral, net of "stability fees" required by the Maker platform for the service.

Figure 12 schematizes the process of opening and closing a CDP, the underlying assumptions in this particular case are that 1ETH is worth 100 USD both at the opening and the closing of the smart contract and that there are no stability fees required by the system:

¹⁵ Market exchange rate between Ether and US dollar.



**Figure 8: Process of Dai creation through CDP smart contract.
For the example 1 ETH=100 USD**

In all this, the key variable is the "DAI target price" or parity with the US dollar. For the Maker team, this target price has two fundamental functions, the first for calculating the collateral-to-debt ratio of a CDP and the second to give a value to the collateral asset that the user must receive in the event of a global settlement, that is the process of liquidation of last resort of the positions in case of system shutdown.

The price stability of DAI is managed through the so-called TRFM (target rate Feedback mechanism). This process modifies the target rate of interest on DAI to balance Demand and supply in the market, acting as an incentive to hold DAI (target rate positive) or to borrow DAI (target rate negative). The target rate is fixed at 0% when the price is pegged to 1 USD, and there's no need to change the demand or the supply.

At the moment DAI stablecoin is not as used as Tether but its popularity is rapidly increasing overtime. According to Coinmarketcap.com, DAI is the 23rd cryptocurrency in the world and its capitalisation is about US dollars 900 million with a daily volume of trading about 214 million. Although the DAI stablecoin has just exceeded half a billion dollars in capitalization, we will see its importance and relevance when in the fifth chapter we analyze the DeFI industry, in which many decentralized lending platforms use the DAI as a reference currency for its two main peculiarities: its stability and its compatibility with the Ethereum Blockchain, a feature that Tether does not enjoy.

NUBIT, AN ALGORITHMIC STABLECOINS

NuBits is the first algorithmic stablecoin created and it dates back to 2014. The Blockchain on which NuBits rests is called peercoin, in addition to having the primacy as the first development platform for an algorithmic stablecoin, it was also the first Blockchain that adopts the consensus protocol " proof of stake ". Each participant in the platform has the opportunity to participate in the vote regarding the decisions to reduce or increase the circulation of money in proportion to his NuBit Shares. Faced with excess supply in the NuBits market, which determines the reduction of the market price, the "Nubitshareholders" can mitigate this depreciation through the staking process, which in the specific case of this Blockchain, is called parking.

Parking consists of freezing a quantity of currency in circulation in order to rebalance the price to the target value. Participants in the parking are remunerated according to an algorithm that determines the amount of satoshi (ten thousandths of bitcoin) to be paid as a reward based on the "freezing" time.

The NuBits project was successful in maintaining parity with the US dollar until March 2018 with a maximum capitalization peak of 13 million dollars, from that moment on the value of the stablecoin has collapsed and today it stops at about forty dollars' cents.

The NuBit crash in March 2018 was caused by a shortage of currency reserves. This DeFIciency meant that the Nubit team was unable to prevent the panic selling generated by the depreciation of what was considered a stablecoin. A major criticism that was levelled at the peercoin platform and its project was that of holding the reserves in the form of bitcoin, which became a major problem during the Bitcoin bubble at the end of 2017.

Clearly, the case of the Nubit Crash brings about important economic reflections in the context of price stabilization mechanisms. First of all, the algorithmic stabilization mechanism without collateralization of assets (whether on or off-chain) tends to rely too much on the expectations of the economic agents who use it. When the expectations on price stability are low, a vicious downward circle is engaged, which inevitably causes the price of the currency to collapse. Such collapse is determined not only by bearish expectations due to the bursting of the Bitcoin bubble, but also due to the strong level of liquidity risk associated with the Nubit ecosystem. Liquidity risk strongly caused by the low level of market depth associated with this currency. Indeed, the Nubit market was unable to absorb large sales and redemption orders without causing a sharp drop in price. In the same period, the Nubit system had to face both a strong panic selling by users and a strong devaluation of the reserves held in bitcoin. The combination of these two factors caused the price to collapse and stability with

the dollar has not been maintained since then, currently the Nubit stands at 26 cents ¹⁶of a dollar.

EUR / USD STABLECOINS RANKING

RANK	NAME	MARKET CAPITALIZATION (Millions USD)	VOLUME (24h, Millions USD)	BLOCKCHAIN	PEGGED TO
1	Thether, USDT	15.518,100	36.028,746	Bitcoin	USD
2	USD Coin, USDC	2.460,374	433,123	Ethereum	USD
3	DAI	900,209	214,209	Ethereum	USD
4	TrueUSD, TUSD	508,356	63,098	Ethereum	USD
...					
10	STASIS EURO, EURS	37,543	0,946	Ethereum	EUR
...					
24	NUBITS, USNBT	2,851	0,016	Nubits Blockchain	USD
...					
26	EURBASE, EBASE	2,585	0,005	Ethereum	EUR

Table 3: Ranking of the most used stablecoins pegged to USD or EUR. According to Coinmarketcap.com

Quickly commenting on the data summarized in table number 3, it can be seen that many stablecoin projects are still in their infancy and involve truly negligible monetary masses.

As a matter of fact, it should be remembered that stablecoins are crypto assets born after ordinary cryptocurrencies. They have been designed, indeed, in order to reduce the uncertainty and volatility of the crypto market. Thether, USD coin and DAI are the real relevant projects to focus on. Another aspect to underline is the predominance of stablecoins anchored to the US dollar. As a matter of fact, given that the Euro is ranked tenth in the global ranking, there is no real virtuous project of issuing stablecoins anchored to such currency. Tether still remains the only major project to work on the Bitcoin Blockchain, while most

¹⁶ According to Coinmarketcap.com

stable currencies are built and designed on the Ethereum Blockchain, precisely because of its ease and universality of use, a feature that I will discuss in the dedicated chapter.

In conclusion, it is easy to believe that stablecoins are the most promising financial instruments for the future. Based on a decentralized distributed ledger, totally transparent and of stable value, they have all the best requirements for a future adoption in the economic systems all over the world. Furthermore, stablecoins have had so much resonance- even beyond the crypto world - that numerous financial institutions and central banks have set their sights on their mechanisms of stability and transparency. Nowadays it is therefore necessary to carry out a further categorization for this type of crypto-currencies: those seen so far are "private stablecoins" which differ from "sovereign stablecoins" in that they come to life from private and non-institutional initiatives, as we will see in the next chapter.

FROM PRIVATE TO SOVEREIGN STABLECOINS: CENTRAL BANK DIGITAL CURRENCY

During the inaugural speech of December 2019, the new president of the European central bank spoke on the topic of crypto currencies and the future of money. In my opinion, the speech given by Cristine Lagarde gives important food for thought regarding the position of institutional and regulatory bodies towards the so-called crypto-economy and in particular towards stablecoins. First of all, it highlights the increasing importance that the crypto-economy has reached over the years. And, as a consequence, the resonance that these new types of financial instruments have is no longer negligible on the part of the institutions. As a further proof of this, the governor stated that, in a scenario of strong economic and financial change, the central bank has the task not only of predicting future trends, but also of trying to modify and shape them. In her inauguration speech, she reiterated that an important debate on stablecoins is open at the institutional level, and that the European central bank is ready to collaborate with the most important global partners for the development of a stable institutional crypto-currency.

However, the ultimate goal of this project must not compromise the security of payment systems and the stability of the monetary and financial system. This type of digital currency would allow citizens to use central bank money directly. However, according to the Governor, the issue of "central bank digital currencies" needs further analysis and experimentation.

The still heated discussion on the convenience of adopting central banks digital currencies as stablecoins dates back to recent years, and the ECB joins the already long series of central banks that have begun to study and analyse these new types of monetary instruments.

The most reliable Definition of the CBDC¹⁷ is given by R. Houben and A. Snyers.

They Define stablecoins as:

- An innovative form of digital central bank money. This differs from reserves or settlement accounts that commercial banks keep with the central bank.
- A central bank money denominated in the reference currency for peer-to-peer exchange purposes by users in a decentralized way.
- A digital asset issued by the central bank for the purpose of serving as a means of payment for both retail and wholesale operations. "some form of central bank money handled through electronic means and accessible to the broad public";
- A central bank liability in digital and decentralized form through the use of a distributed ledger on the Blockchain.

¹⁷ Central Bank digital currency

According to a report prepared by the bank for international settlements¹⁸, published last January 2019, about 40 central banks from all over the world are currently carrying out studies and research for the experimentation of Central Bank digital currency. This institutional application of Blockchain technology and distributed ledger technology has attracted the attention and interest of the central banking community for its potential to interface with the future challenges of financial inclusion, efficiency in the payment system and cybernetic resilience. As reported by the World Economic Forum in its white paper of March 2019¹⁹, the first central banks to conduct research and publish articles in this area were the Bank of England and the Bank of Canada. In these articles, respectively titled "The Economics of Digital Currencies" and "Project Jasper", the two central institutes investigated how CBDCs could be used to improve performance, efficiency and resilience in domestic interbank payments.

The CBDCs hypothesized in these studies were tested as a pilot project on a narrow circle of subjects. These stablecoins, structured as payment tokens, represent liabilities directly held in central bank reserves. The operators in this system use these tokens to implement interbank transfers which are validated on the distributed ledger. The Blockchains that were used for these projects were structured as "permissioned" networks, in which only authorized participants were able to see the transactions recorded in the network.

In this system, the central bank that issues a certain amount of CBDC simultaneously removes the corresponding amount of currency from the money supply.

At the end of these articles, the pros and cons of central bank digital currencies were listed.

The benefits that would be obtained through the use of these official stablecoins would be:

- greater efficiency (greater speed at a lower cost) in domestic and foreign payments.
- The opportunity for savers to make safer deposits with the central bank and not subject to the risk characteristic of commercial banks
- The same competition with commercial banks could push them to increase the interest rate on deposits or the quality of the services offered.
- A potential increase in financial inclusion for "under-banked" individuals.
- A strong tool for the fight against tax evasion and financial crimes.
- a tool with greater resilience to cyberattacks due to the non-centralization of data and the benefits brought by Blockchain technology.

On the other hand, it is very important to focus on the direct or indirect costs that the company should pay by adopting these stablecoins:

¹⁸ report edited by C. Barontini and H. Holden

¹⁹ Central banks and distributed ledger technology: how are central banks exploring Blockchain today?

- Compared to physical cash, a lower level of consumer privacy could occur.
- Blockchain technology is under discussion about its actual scalability and speed of execution.
- the serious risk of exclusion from the financial system of subjects who do not use CBDCs because they are already foreign to digital payment systems.
- Institutions could have easier access to citizens' funds.

THE DIGITAL EURO: THE ECB'S CBDC

On October 2, 2020, the European Central Bank published an insightful report describing the process of issuing an innovative form of "Digital Euro" within the Eurosystem. In the document, the ECB highlights how, in the transition from the current payment system towards an electronic and digital one, the introduction of a EURO CBDC could be crucial for a greater inclusion of non-banked Europeans citizens in the financial circuit. It is important to underline that the term digital euro "denotes a liability of the Eurosystem recorded in digital form as a complement to cash and central bank deposits" (ECB, 2020), and not a public stablecoin brokered by the European Central Bank. Moreover, the ECB reiterates that, regardless of the type of IT infrastructure chosen for the construction the digital euro - blockchain included - the crypto-asset would still be considered a form of risk-free central bank money, that is, a digital representation of cash.

The substantial difference between the current forms of digital money and the digital euro lies in the fact that the former are liabilities of private supervised entities, i.e. commercial banks. The fact that they are issued by private entities makes them susceptible to the risk of default and a consequent negative impact on the economic and financial system. The digital euro, being issued directly by the Central Bank, would solve this problem, as the deposits of citizens would be made up directly with the ECB.

Against this background, the report provides an important analysis of the drawbacks that may result from the adoption of a digital Euro.

The most important of these is the effect on the banking sector, as it would create competition between commercial banks and central bank in terms of deposit supply and digital euro demand. The substantial increase in demand for the digital euro, resulting in the flight of deposits from commercial banks to the central bank, would increase the costs of financing for private intermediaries, which may have to deleverage and decrease the supply of credit, thus preventing an optimal level of investment and aggregate consumption. If this process ultimately implies higher costs for borrowers, economic activity could be hampered.

Furthermore, if their traditional business model were compromised, banks could decide to take more risks in an attempt to achieve higher (nominal) returns and offset the decline in profitability (ECB, 2020).

This hypothetical scenario underlines the need for the European central bank to construct and design the digital euro in a prudent way in order not to undermine the stability of the European banking system. According to the report, the digital euro project will be tested in the second half of 2021. The results and data collected during the test phase will drive future decisions concerning the formalization, if any, of the official ECB CBDC.

In these chapters I have tried to analyse in the best possible way the principles on which the concept of stablecoin is based, as well its various types, be it private or institutional, collateralized or uncollateralized. I consider it an important, if not fundamental, topic for a reflection on the next evolution of the currency. In my opinion it will be decisive how in the near future the large central monetary institutions will decide to move towards cryptocurrencies and stablecoins. It seems obvious that such important institutions in global economic systems cannot in any way decide to rely on a totally autonomous monetary system and decentralized. The key point will no longer be whether these distributed ledger technologies will also be adopted by central banks but will arguably be about how the trade-off between decentralization, privacy and universal accessibility and stable, secure and minimally controlled systems will be managed.

I believe this trade-off between decentralization and privacy optimization towards a secure and stable system will be the fundamental point for the mass diffusion of cryptocurrencies. It is logical to expect that Blockchain users of the first hour and the more "orthodox" of monetary decentralization, will not look favourably of central institutions and regulatory bodies into the sector. In the same way, however, all the early adopters themselves, could greatly benefit from the injection into the crypto market of large capital from millions of investors who are currently wary. For this reason, a formal legitimation guaranteed by an institutional body might be enough to put aside the mistrust and start operating in this growing market. Therefore, the meeting point between the needs of current users and potential new entrants will be in the hands of the central bodies. Returning to Lagarde's statements, the ECB's task is not only to find the right and optimal meeting point, but also to refer to such optimal meeting point for the development of a safe and innovative economic system.

A game is being played that will uniquely outline the future of money, monetary and financial systems. Many different interests of various parties are at stake, but if there is a meeting point

between traditional systems and the new crypto-economy, this is currently represented by the potential of stablecoins.

LIST OF ALL CRYPTO-ASSETS

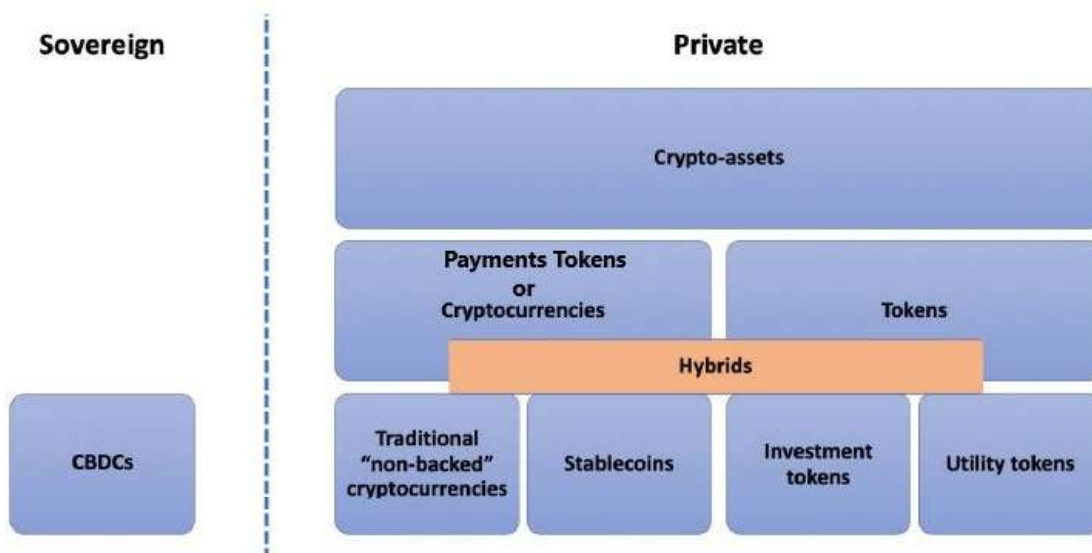


Figure 9: Taxonomy of Crypto-assets proposed by Policy Department for Economic, Scientific and Quality of Life Policies

THE PROJECT ETHEREUM

Like Bitcoin, “Ethereum is [a] public, distributed Blockchain based platform with a Proof of Work-based consensus algorithm coupled with rewards, which absolves the need for trusted intermediaries” (Bonneau, J. et Al.2015). The crucial difference between the two platforms lies in the fact that Ethereum is an open source Blockchain, which allow us to understand how Ethereum wants to overcome and evolve the use made so far by this technology. An additional difference can be found in the purpose for which Ethereum was created. Just as bitcoin was created to offer a digital cash p2p system that would allow digital payments to be made without the intervention of a central entity, Ethereum was designed to create a development platform for decentralized applications: Ethereum's most significant feature is the Ethereum Virtual Machine (EVM) - a stack-based runtime environment that can execute programs known as smart contracts (F. Victor and B.K. Luders, 2020). The EVM is essential for the Ethereum protocol, it is a virtual "computer" connected with all the nodes of the network. This allows anyone to run code in a trustless ecosystem where the result of an execution can be guaranteed and is completely deterministic. The Ethereum network is also based on the consensus protocol with which transactions are confirmed, which in this case are called "messages". The nodes that perform the function of miners are remunerated with the cryptocurrency that is the basis of the Ethereum ecosystem. Unlike Bitcoin, however, Ether (Ethereum's cryptocurrency) not only acts as a monetary medium of exchange for the purchase of goods or services but is also used as a currency for the purchase and management of the platform by all the developers who access it to promote their innovative realities.

ETHER MONETARY POLICY: “MINIMUM NECESSARY ISSUANCE”

Ether is the fundamental component for the existence of the Ethereum Blockchain, as bitcoin is a digital currency that can be spent and traded in different ways. Ether can also be considered as the opportunity cost of investing and developing platforms on the Ethereum network. The monetary policy underlying this cryptocurrency was decided in 2014 in the presale phase. The founders of the Ethereum monetary ecosystem chose not to set an *a priori* maximum amount of money in circulation. According to the official informative website of the Ethereum project "EthHub", the growth rate of the annual emission of Ether has been constantly decreasing over time and is currently equal to about 4.5% per year.²⁰ Specifically,

²⁰ The monetary policy in Ethereum framework is decided yearly by Ethereum Developers, community members and miners.
<https://docs.ethhub.io/ethereum-basics/monetary-policy/>

in this historical period 3.75 Ethers are issued for each block validated by the Blockchain plus the commissions that are paid to the miners.

To date, Ethereum enjoys a market capitalization of nearly \$ 40 billion, a daily volume of \$ 16 billion and the supply of circulating Ethers amounts to a total of 112 million coins²¹. Numbers that classify Ethereum as the second largest cryptocurrency by capitalization and use, after Bitcoin. Figure 18 shows us the annual issuance rate of growth of the money supply (RHS) and the current total money supply (LHS) and a future projection if the Proof of Work consensus system will be maintained.

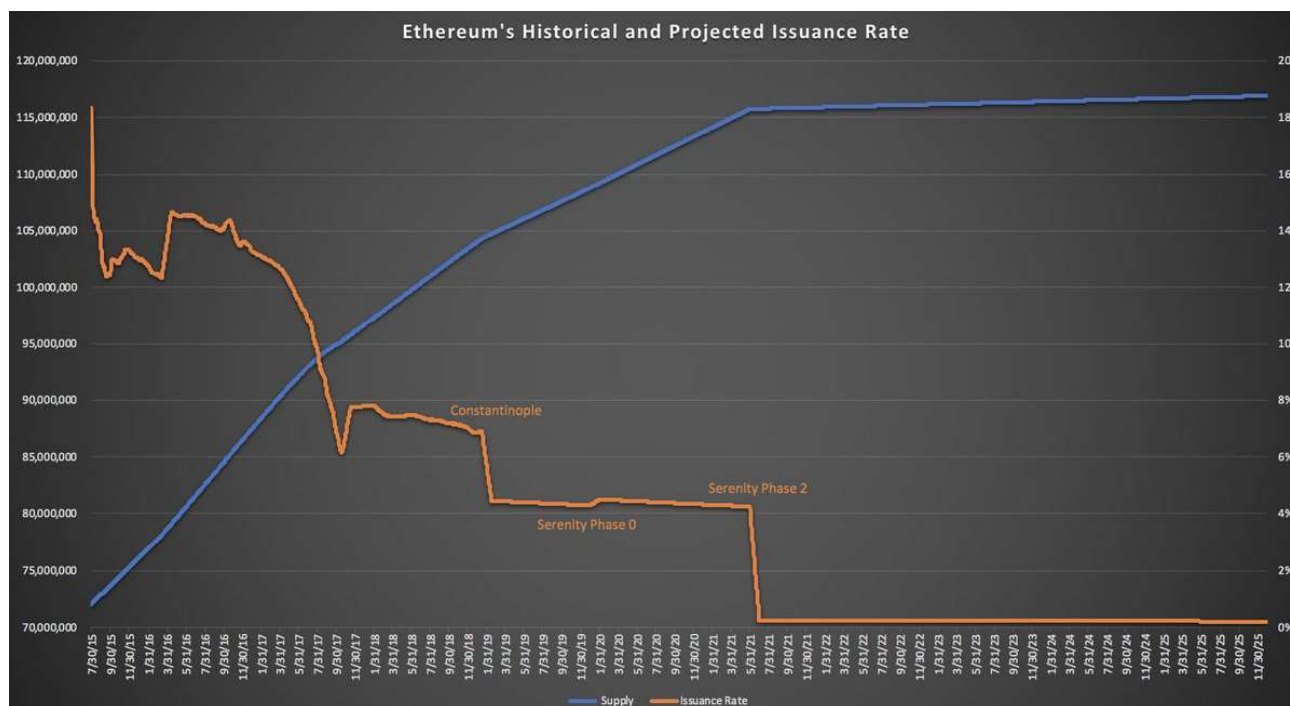


Figure 10: Supply and Issuance rate of Ethereum²²

The initial coin offering of Ethereum began on July 22, 2014 and was structured in a presale that lasted until September 2, 2014. The initial price of Ether was set at 2000 ETH²³ per BTC²⁴ and was fixed for two weeks, then the price linearly dropped to 1337 ETH per BTC. The ICO was structured in such a way as to create 60 million tokens of which 80% destined for sale on the market and 20% reserved for Ethereum foundations as a "development fund". The pre-sale of Ethereum ended in 42 days and a total of 31,000 BTC (equivalent to about 18 million USD) was raised by the foundation²⁵.

However, the genesis block of the Ethereum Blockchain was mined on July 30 of the following year, when the platform was officially launched.

²¹ According to Coinmarketcap.com

²² Taken from EthHub.io, estimated in the actual condition with Proof of Work consensus.

²³ Ether's code

²⁴ Bitcoin's code

²⁵ According to EthHub data

ETHEREUM NETWORK STRUCTURE

The Ethereum Blockchain is made up of two types of "nodes", namely, node operators and core developers. Node operators are the owners and managers of the nodes that operate the consensus protocol. Most of them do not deal with programming and writing applications based on the Blockchain, they have a purely computational role and provide for the maintenance of the network itself. The core developers of the Blockchain are those who develop and implement the network with new applications and services, making the most of the peculiarities of this open-source distributed ledger.

Both categories of miners have incentives that are paid in ether for their service, be it maintenance and validation, or development and innovation of applications on the Blockchain.

The remuneration system for the miners who deal with the validation and stability of the network is determined by the monetary policy directives we have seen previously, the rewards for developers are determined according to an On-chain governance mechanism.

On-chain governance is a system for administering and deciding on changes, modifications or innovations to be applied to the Blockchain. The on-chain name derives from the fact that the group of stakeholders (miners, developers and users) can propose changes through codes and each stakeholder can vote whether to accept them or not. In this case, the proposed changes are advertised by updating the computer codes, after which each node has the right to vote based on the quantity of tokens in its possession. The biggest change, voted in favour by the Ethereum network, was to migrate the Blockchain from a Casper "proof of work" consensus protocol to a "proof of stake" called the beacon coin in a new platform called Ethereum 2.0.

ECONOMICS OF ETHEREUM AND ETHEREUM 2.0

Currently, Ethereum is a Blockchain founded on the Proof of Work consensus, just like Bitcoin. The proof of work has a major influence on the economy of the system. The structural functioning of the Blockchain is guaranteed by the nodes (miners on bitcoin, validators on Ethereum) and their work. They perform a fundamental function, that is, validating the additional information and officially registering it in the Blockchain. This process, however, is not free of costs: as a matter of fact, it is the main weakness of the PoW consensus systems, as the miners / validators need a high computational power with which the data is encrypted and irrevocably recorded. Therefore, miners guarantee the functionality of

the system only as long as they have a higher remuneration than the energy costs necessary to guarantee ever greater computational power.

According to the studies carried out by the researchers of "Digiconomist" (a platform which has been studying innovations in the digital and crypto fields from an economic perspective for more than a decade) the annual electricity consumption of the Bitcoin Blockchain amounts to a total of about 70 TWh²⁶, while Ethereum would be around 10 TWh²⁷. In monetary terms this would translate into about 3.5 billion dollars a year in electricity costs for the maintenance of the Bitcoin platform and one billion a year for that Blockchain²⁸, without taking into account the environmental costs related to CO2 emissions.

It is evident that the resistance of Blockchains based on proof of work is subject to the fact that miners obtain remuneration which is greater than these already enormous figures, and still destined to grow due to the intrinsic nature of the cryptographic algorithm. Consequently, it can be said that the scalability of these technologies also partly depends on the cost-effectiveness of their operation as it is foreseeable that if the costs for miners increase, higher commissions will be required for users of Blockchains, thus discouraging them to use these systems. in favour of traditional financial services.

It is precisely in relation to these issues that the Ethereum developer team has decided to migrate to a consensus system that does not require exaggerated computational power and does not require such worrying energy costs. The chosen alternative was the Proof of stake system, in which the validators no longer have to compete at a computational level but can collaborate and validate transactions in proportion to the share of "staking tokens" they own. The staking process, or PoS mining, is the practice with which users in possession of tokens can decide to "stake" (staking) their assets. This system implies that locked tokens are momentarily unfungible until the end of the staking process. The remuneration provided for those who point and temporarily deprive themselves of a quantity of tokens, consists of the right to confirm and register the new blocks in the Blockchain, thus being able to obtain commissions for this service. The staking process is also used to decide how the transactions to be verified should be distributed among the participating nodes. The percentage of tokens staked by each node on the total staking tokens determines the percentage of transactions to be verified for each validator. The proof of stake, in addition to having greater energy efficiency, overcomes a weakness of the proof of work system, that of vulnerability at 51%. In a proof of work system, a node with a computing power of 51% of the total could

²⁶ <https://digiconomist.net/Bitcoin-energy-consumption>

²⁷ <https://digiconomist.net/ethereum-energy-consumption>

²⁸ Digiconomist's researcher estimated a cost of 5 cents per KWh for Bitcoin's miners and 10 cents per KWh for Ethereum's validators. The difference price is due to the different economies of scale of the two Blockchains

compromise the stability of the network, while the proof of stake guarantees the security of the system itself as a potential owner of 51% of the total tokens of a system. It would have no incentive to bring down the network for which it holds the absolute majority of the assets.

As reported by EthHub, the official website of the Ethereum platform, during the migration period (from the beginning of 2019 late 2021 and beyond²⁹), any node or participant in the Ethereum Blockchain can apply to become an Ethereum 2.0 validator node through the Staking process. The requirements for becoming an Eth2³⁰ validator consist in having a minimum of 32 ETH and guaranteeing a minimum level of computational power bigger than 500W³¹.

The staking process requires that each validator candidate deposits an amount of Ether through a "smart contract", on the basis of which the validation percentage will then be calculated based on the total ETH deposited for staking³².

The remuneration system for Eth2 validators is inversely proportional to the increase in the Ethers deposited for staking.

SMART CONTRACTS AND TRANSACTIONAL COSTS

The great innovation brought by Ethereum to the crypto world was the creation of an infrastructure on which financial transactions could be performed through automated orders such as smart contracts. The digital environment that has been created between the interaction of operators who offer different smart contract services in the financial field and beyond, takes the name of DeFI or Decentralized Finance (which will be analyzed in a further dedicated chapter). Before moving to in-depth analysis, it is important to understand how Ethereum manages smart contracts.

Smart contracts are programs that encapsulate the logic for governing funds. As these contracts have to be executed by all participating nodes in the Ethereum network, the sender of a transaction has to pay for the computational cost of execution in units of gas (a virtual unit of account used to measure the computational cost of executing a transaction). The amount of gas to be paid by the sender of a transaction depends on the complexity of a smart contract's logic. Additionally, the sender is required to specify the gas price, which he will have to pay per unit of consumed gas. The product of the gas cost and price determines the

²⁹ According to the official roadmap of Ethereum.org

³⁰ Node involved Ethereum 2.0 validating process.

³¹ The same for running an archive node of Ethereum 1.0.

³² Assuming that 100 ETH have been deposited for staking, a validator in possession of 32 ETH will have guaranteed the validation of 32% of the transactions with the related remuneration.

transaction fee, which is received by the miner who includes the transaction in a block (Sam M. Werner et Al, 2020).

Ethereum smart contracts can serve as a back-end for decentralized applications. The benefits of using an Ethereum smart contract instead of a new Blockchain include faster and easier development, bootstrapped security, and being able to communicate with other decentralized applications deployed in the Ethereum Blockchain (B.V. Buterin, 2013).

SMART CONTRACTS AND NEW KINDS OF GOVERNANCE MODELS: THE DAOs

Ethereum has brought many innovations to the Blockchain world. Many mistakenly believe that the only sector born from the use of these innovations is decentralized financial services with the advent of the DeFI industry. Actually, Ethereum and the unique peculiarities of its Blockchain has given development impulses even beyond the economic-financial perimeter. To provide an example, the application of refined smart contracts in the management field has given birth to the current that takes the name of "Decentralized Autonomous Organization (DAO). A DAO can be Defined as an organization governed by computer codes and algorithms (smart contracts). Given these characteristics, it has the ability to function autonomously, without the need for central authorities or managerial subjects.

The operation of a DAO consists in processing external data and executing specific commands without human intervention. These organizations are participated by a community of subjects who regulate their activities and objectives through a system of utility tokens. The directives of the DAO, its purposes of the same and the construction of smart contracts are managed by an "on-chain" governance system, where the decision-making weight of the members is based on their share of (possessed) tokens.

Unlike traditional organizations, which run on hierarchical structure and different levels of bureaucracy, DAOs have no hierarchy. Instead, they make use of economic mechanisms - which are translated into computer codes (i.e. algorithms) - to align the interests of the organization with the interests of its members. Fundamental smart contracts make extensive use of game theory.

Basically, DAOs provide an operating and management system for the open collaboration of individuals. This system allows various individuals and institutions to collaborate without necessarily having to know or trust each other.

The main economic dilemma that these types of organizations face and to which they propose a solution is the well-known "Principal - Agent". Being autonomous, the DAO (relationship

agent) has the ability to make decisions and take actions on behalf of other members (the principal) in a totally automated and decentralized way.

Through the greater transparency offered by the Blockchain and the management method through smart contracts, the problems of information asymmetry affecting traditional centralized systems are practically eliminated. All the transactions that the DAO executes on the basis of smart contracts are recorded in an immutable and transparent way on the distributed ledger. In this way, each member of the organization can verify the correct functioning of the organization and possibly propose the correction of the basic algorithm through the on-chain voting system.

Currently, the most important DAO in the Ethereum ecosystem is MakerDAO, founded in 2014. Its popularity derives from the creation of the Stablecoin DAI, as previously exposed. In addition to that, it is interesting to analyse that, from a management point of view, Maker is an open-source project included in the Ethereum Blockchain developed by a decentralized autonomous organization. The project is managed by people around the globe who hold its "utility" - governance-token called MKR. According to the official website MakerDao.com, the founders chose to adopt a "scientific-governance", based on executive voting mechanisms dependent on the share of MKR owned by each voter. The voting process is transparent, efficient and publicly available on the Blockchain.

According to official information released by the organization, the Maker governance is currently studying an expansion of the crypto-assets eligible as collateral for the issuance of the DAI stablecoin. The purpose of this analysis is to be able to bring more options to DAI users and, in doing so, to make the market for this stablecoin even more liquid.

The most recent decision by Maker's governance on the adoption of crypto-assets as collateral for the issuance of DAI dates back to 3 May 2020³³. On this date, it was established that even bitcoins (in the form of ERC-20 tokens, which I will cover in the next paragraph) could act as collateral for the DAI stablecoin, until then collateralized only through the deposit of ETH.

ERC20 TOKENS AND WRAPPED BITCOIN

Ethereum is more than just a Blockchain or a cryptocurrency: as a matter of fact, it primarily consists in a platform upon which it is possible to build and implement different Dapps (Decentralized Applications), each working through its own crypto-tokens. The tokens operating on Ethereum are computerized with the structure "ERC-20", and, therefore, belong to the category of "utility tokens" listed in the third chapter. On the contrary, the "investment

³³ <https://cryptonomist.ch/2020/05/04/wbtc-collaterale-dai/>

tokens" are based on the "ERC-1400" structure, which does not allow them to rely on the Ethereum platform.

For the purpose of this paragraph, it is crucial to dwell on the functioning and importance of ERC-20 tokens as they are the basis of the functioning of any application on Ethereum.

Since its inception, Ethereum has been highly regarded by the market and Blockchain developers for its versatility.

Despite representing the most important global cryptocurrencies, the Ethereum and Bitcoin ecosystems have been completely separate and non-communicating worlds up until 2019, and the claim of the Ethereum developers to give life to a global and universal Blockchain platform collided with this clear separation. As a matter of fact, most of the liquidity, demand and trading volume in the crypto market lay and still lies in Bitcoin. In order to remove this barrier between the two ecosystems and to inject a large amount of liquidity ³⁴ into the Ethereum world, in January 2019, the "ERC-20 token" Wrapped bitcoin or WBTC was created³⁵.

Wrapped BTC was the first ERC-20 wrapped token and the first working on proof of reserves protocol on Bitcoin Blockchain (Kyber Network, 2019).

The act of "wrapping" bitcoins can:

- Increase speed of transactions: Ethereum blocks are created every ~15 seconds and it is possible to have a fair deal of confidence in the irrevocability of a transaction in less than 5 minutes. This speed is faster than the original Bitcoin's transactional speed.
- Reduce the number of intermediaries: one of the key benefits of assets on a Blockchain is their ability to be transacted without intermediaries. This can be done through, decentralized exchange protocols.
- Enhance security: tokenization enables users to have full control of private keys of the asset. Users who do not want to hold keys can reduce counterparty risk by moving it from exchanges to a security-focused custodian.
- Usability: The ERC20 standard has been adopted by a large number of institutions and products. This provides users with a variety of exchanges, wallets, and Dapps to use while handling their tokenized asset. They also have the ability to move tokens quickly, 24/7.
- Improve Transparency: The total number of tokens, token creation transactions, token removal transactions, number of token holders, and rules for transfers can be seen on a

³⁴ <https://decrypt.co/resources/what-is-wbtc-explained-Bitcoin-ethereum-DeFi>

³⁵ Wrapped Bitcoin was brought to the world as a collaborative project between major players in the DeFi ecosystem such as BitGo, Ren, Dharma, Kyber, Compound, MakerDAO, and Set Protocol in an effort to bring more liquidity into the Ethereum network by dipping into Bitcoin. The project is now controlled by a Decentralized Autonomous Organization (DAO) called the WBTC DAO.

public block explorer by anyone. This level of transparency is not usually available for assets like fiat currencies, commodities, and stock (Kyber Network, 2019).

The fundamental characteristic of Wrapped Bitcoins lies in the fact that their exchange rate towards ordinary bitcoin is always stable and fixed at one. As a matter of fact, the wBTC³⁶ indeed, can be considered as a tokenized stablecoin anchored to bitcoin. From an economic point of view, it is interesting to study how exchange rate parity is maintained and which subjects come into play in the tokenization process. In the process of issuing the wBTC, three categories of subjects come into play in addition to the authorizing wBTC DAO, which certifies and authorizes DeFI operators to play the roles of Custodian and Merchant through the process. WBTC DAO As a matter of fact certifies and authorizes DeFI operators to play the role of "Custodian" and "Merchant" in the process. The role of custodian consists in keeping the assets that are tokenized (in this case bitcoins) and issuing wBTCs according to the established exchange rate (1: 1 in this particular case). The merchant, on the other hand, covers the role of intermediary between the custodian issuing the tokens and the user requesting their use.

The merchant is the subject (always enabled by wBTC DAO) who stipulates the smart contract with the end user, it establishes the amount of BTC that the user wishes to convert and the sum in wBTC that he will receive against the contract. It is important to underline that the subjects identified as Merchants must carry out the customer due diligence as prescribed by the Know your Customer and Anti-money laundering directives which will be examined in Chapter 6.

Basically, the minting process of wBTC takes place when a bitcoin user decides to appeal to a "Merchant" enabled for the conversion of his BTC. The signing of the smart contract triggers the withdrawal from the market of a BTC, deposited at the custodian, and the issue of a compliant wBTC for use on the Blockchain platform. The opposite process, called "burning", takes place in reverse and is necessary for the financial stability of the system itself³⁷. Only in the event of the elimination from the market of wBTCs the Custodian can return the corresponding number of BTC to the user.

The issue of wBTC and the process just described, however, is not exempt from transactional costs present as remuneration for the parties that are part of it. As a matter of fact, in the smart contract for the issue of wBTC there are commission costs for the custody of tokenized assets and brokerage fees in favour of the merchant who stipulates the contract. In light of this the real exchange rate between wBTC and BTC for the user will

³⁶ Wrapped Bitcoin's code

³⁷ <https://medium.com/chainsecurity/wrapped-bitcoin-wbtc-audit-completed-1025463a88c5>

never be totally at par but slightly lower due to the conversion fees. The actual presence in the market of a greater quantity of Bitcoin than the quantity of wBTC issued gives the custodian and the system itself greater financial stability in situations of high volatility and high market volumes. In any case, given the volumes of tokenized bitcoins from January 2019 onwards, it can be said that the cost of the tokenization of bitcoins by users is amply repaid by all the services that can be used within the Ethereum platform.

Despite the costs, the tokenization of bitcoins, in my opinion, is a fundamental process for the development of an interoperable system between the two main global cryptocurrencies as both Blockchains and their respective users can obtain important benefits.

Ethereum as a platform can undoubtedly benefit from the huge amount of liquidity present in the bitcoin market³⁸ and, vice versa, bitcoin users can take advantage of the most advanced Decentralized Finance services operating only on Ethereum, not to mention the greater efficiency and transaction speed of the latter towards Bitcoin.

Furthermore, the greatest efficiency gain in the energy field will arguably be obtained with the migration of the Ethereum platform to Eth2, which will expand the proof of stake consensus protocol not only to the mining of Ether, but also to the tokenized form of Bitcoin. This, in turn, would lighten the wasteful Bitcoin mining process based on very inefficient forms of proof of work.

ETHEREUM'S MARKETS

In the first five years of its existence, Ethereum revolutionized the world of Blockchain and crypto-assets, giving life to an open-source platform on which to develop different types of economic activity through organizations that exploit decentralized governance models.

There are numerous projects and organizations operating in this ecosystem. In recent years, computer programming activities specialized in Blockchain, decentralized marketplaces, decentralized gaming platforms and organizations offering financial services have been developed on Ethereum by exploiting the decentralization of the public distributed ledger. For the purposes of my work, in the next chapter, I will deal with the decentralized financial sector that is occupying the fintech market, this economic environment is called DeFI or Decentralized Finance. The DeFI is not only the set of operators who offer financial services through Blockchain technology: in fact, it could prove to be the digital

³⁸ According to Coinmarketcap.com Bitcoin has a market capitalization about 200 USD billion, 285 times higher the Wrapped Bitcoin one (700 USD millions).

evolution of the banking and credit world, shifting the balance of the entire sector we are used to.

DECENTRALIZED FINANCE

In light of what has been discussed so far, we can say that distributed ledger technology integrated with a Blockchain network has led to the emergence of the world of crypto-assets, a world in which some fundamental paradigms of traditional finance have been questioned or even upset. One of the main paradigms of economics and finance that has been upset is certainly that of intermediation between economic operators. Intermediaries often play essential roles in expanding transaction possibilities. In economic transactions, intermediaries often help transacting parties find each other, establish trust, and settle transactions (Roth, A.E., 2015) Without intermediaries, transacting parties may not be able to establish connections, negotiate contracts, or enforce agreements. Nevertheless, Intermediaries often enjoy substantial power in shaping economic transactions, and they can leverage their power to maximize self-interests, raising concerns over their monopoly power (Cohen, J.E., 2019). The tension between the need for efficient transactions and the concern over monopoly power characterizes how human society approaches dominant intermediaries in economic transactions. This tension is especially pronounced in the financial system, where financial transactions are facilitated and controlled by large financial institutions (Y. Chen and, C. Bellavitis, 2020).

In the previous chapter, I have always dealt with single cryptocurrencies, tokens or other crypto-assets describing their individual technical characteristics, the Blockchains on which they are based and monetary policies in their ecosystem.

I have decided to proceed in this way in order to give the reader all the tools to understand both the main characteristics of cryptocurrencies, the purpose for which they were created, and the changes and evolutions that have occurred in this rapidly growing sector, which is still little known and studied at an academic level.

After having provided such theoretical tools and practical case studies, I will now move to the core of my work, that is, the comparison of the characteristics of the traditional financial world with those of the emerging DeFI. This topic will not be examined at the specific level of individual Blockchain projects, but rather by adopting a more general and organic view that might help in forecasting the macro trends of the crypto world, which will be destined to change the habits of all economic operators in the market in the coming years.

In order to underline the emerging importance of the crypto world, I will proceed with an analysis of the opinion and positions on the subjects taken by the largest central regulatory institutions in the world. The active interests on these innovative technologies from these bodies tests for the relevance of the phenomenon. And it is precisely about decentralized

finance that the Financial Stability Board stated that, with distributed trust and decentralized platforms enabled by Blockchain technology, entrepreneurs and innovators have recognized the possibilities of creating an open financial system that has limited or no involvement from financial institutions. By doing so, they intend to reduce transaction cost, broaden financial inclusion, empower open access, encourage permissionless innovation, and create new business opportunities (Financial Stability Board, 2019).

INTRODUCTION TO DECENTRALIZED FINANCE

Decentralized Finance (DeFI) is a movement in the Blockchain space that has recently gained a lot of traction, this term refers to open financial infrastructures built upon public smart contract platforms, such as the Ethereum Blockchain (Fabian Schar, 2020). DeFI does not rely on centralized intermediaries and institutions. Unlike traditional finance, it is built on open protocols and decentralized applications (DApps). Transactions and contracts are managed by smart contracts, algorithms built in a secure and deterministic way. Every change of state and transaction persist on a public Blockchain and are openly available. Thus, this architecture is capable of creating an immutable and highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses or escrow services, as most of these functions can be performed by smart contracts.

THE PROS OF DECENTRALIZED FINANCIAL SYSTEM

According to Yan Chen and Cristiano Bellavitis, the emerging decentralized finance model, promises significant advantages and challenges for the future. The authors list them in five points:

1. Decentralization;
2. Innovativeness;
3. Interoperability;
4. Borderlessness;
5. Transparency.

1 Decentralization

In a decentralized financial system, financial transactions are facilitated not by centralized institutions but by decentralized peer-to-peer networks. By reducing the involvement of centralized institutions, decentralized networks can reduce transaction costs and create network effects without incurring monopoly costs (Catalini, C., Gans, J.S., 2019). When a decentralized peer-to-peer network rises to dominance, no single entity can accumulate sufficient monopoly power to monopolize the network and exclude others from participating, allowing everybody to benefit from the network effects to enlarge transaction possibilities (Huberman, G et Al., 2019).

2 Innovativeness

Decentralized finance promotes permissionless and combinatorial innovation, indeed decentralized platforms do not have a controlling party and, therefore, allows for open access and permissionless innovation—that is, developers can freely build and experiment with new applications without asking for permission (Cerf, V., 2012). These kinds of platforms can also facilitate combinatorial innovation. In a decentralized finance ecosystem, new financial technologies can become the building blocks for future innovations, promoting new combinations and new products (Brynjolfsson, E., McAfee, A., 2014).

3 – Interoperability

Traditional finance is more inclined to work in silos, each financial institution has always maintained its own database, services and IT systems. In this context it was natural that barriers had been raised that prevented the birth of an integrated system. Conversely, decentralized finance is built on public and often open source Blockchains, dramatically increasing the interoperability of the services offered. At the moment, the only limit hindering total interoperability is the non-integration between the various Blockchains. In the near future, operators in the sector will have to choose between two alternative paths to achieve the goal of total integration: either pushing and investing for the emergence of a dominant decentralized platform or pursuing intercompatibility between different Blockchains, in order to be able to interchange projects at the time of need. The latter would, moreover, avoid the chance of a single Blockchain monopoly. (Y. Chen and, C. Bellavitis, 2020).

4 – *Borderlessness*

In a centralized financial system, the biggest limitation consists in being tied to a specific geographic area and consequently having to adopt one - and only one - fiat currency for transactions. Any transfer of value between different geographical areas in different currencies is subject to transactional exchange costs and deferred operational deadlines. In contrast, decentralized finance is inherently borderless and thus allows for borderless finance, as it is not tied to geographic locations or fiat currencies. Moreover, it does not rely on any specific central bank or government (Ammous, S., 2018). With the new systems of decentralized finance, the transfer of value between individuals across the world could take place very quickly with practically negligible costs.

5 – *Transparency*

The most delicate issue in which distributed ledger technology has the greatest advantage compared to any traditional data archiving and recording system, is that of transparency. Each transaction is recorded on public ledgers which can be checked and verified by anyone at any time. With public ledgers, decentralized finance generates distributed trust, so transacting parties can transact with each other without pre-existing relationships or trusted intermediary, expanding the scale and scope of potential transactions (Seidel, M.-D.L., 2018).

DEFI STRUCTURE

The foundation of any DeFI protocol and application are the aforementioned smart contracts, small applications stored on a Blockchain and executed by a large computer network. Smart contracts are highly transparent and minimize the risk of manipulation and arbitrary intervention by third parties.

DeFI is built on "multi-layered" architecture composed of 5 purpose-specific levels, namely, settlement, asset, protocol, application, and aggregation.

The *settlement layer* (1) consists of the Blockchain and its native protocol asset. It allows the network to securely store ownership information and ensures that any of the state changes adhere to the network's rule set. As such, the Blockchain can be seen as the foundation for trustless execution and serves as a settlement and dispute resolution layer.

The *asset layer* (2) consists of all tokens that are issued on top of the settlement layer. This includes the native protocol asset as well as any additional tokens that are based on token standards supported by the Blockchain.

The *protocol layer* (3) provides standards for specific use-cases such as decentralized exchanges, debt markets, derivatives and on-chain asset management. These standards are usually implemented as a set of smart contracts and can be accessed by any user (or DeFI application). As such, these protocols are highly interoperable.

The *application layer* (4) creates user-oriented applications that connect to individual protocols. The smart contract interaction is usually abstracted by a web browser-based front end, making the protocols easier to use.

The *aggregation layer* (5) is an extension of the application layer. Aggregators create user-centric platforms that connect to several applications and protocols. They usually provide tools to compare and rate and services, allow users to easily perform otherwise complex tasks by connecting to several protocols simultaneously, and finally combine relevant information in a clear and concise manner (Fabian Schar, 2020).

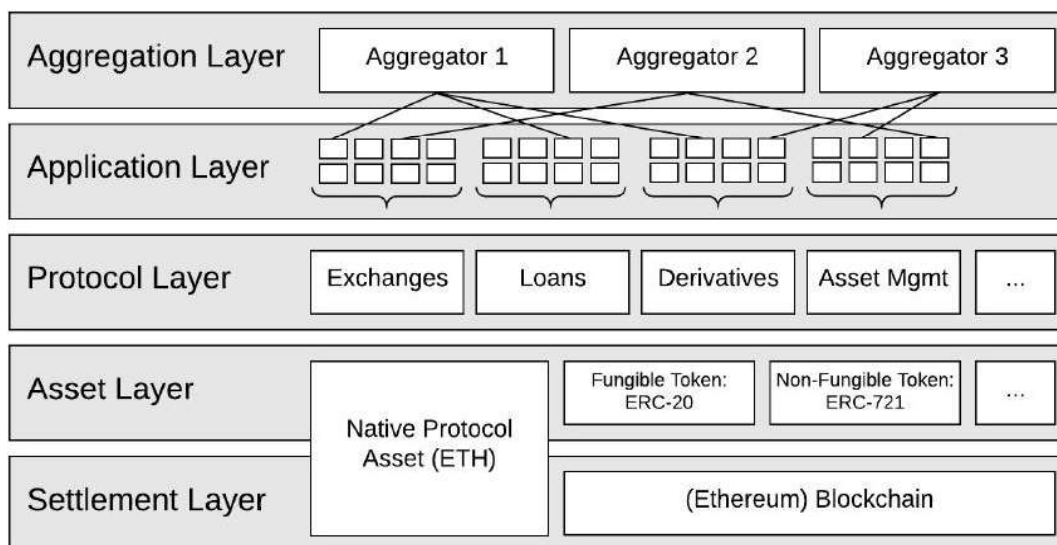


Figure 11: Scheme of the Multi-layer DeFI Architecture

In my opinion, an analysis of the evolution and spread of "DeFI" cannot ignore the architecture of Ethereum DeFI world, since, to date, most of the "DeFI" programmers and developers on Blockchain prefer this ecosystem for its openness and universality, as we can see in figure n.18 below. At the beginning of 2020, it was officially registered that 87% of DeFI projects were founded on the Ethereum network and that the remaining share was divided between Stellar, Waves, Neo (Blockchain platforms on which decentralized monetary systems based on privacy and speed of transactions are proposed) and other independent ones of marginal importance.

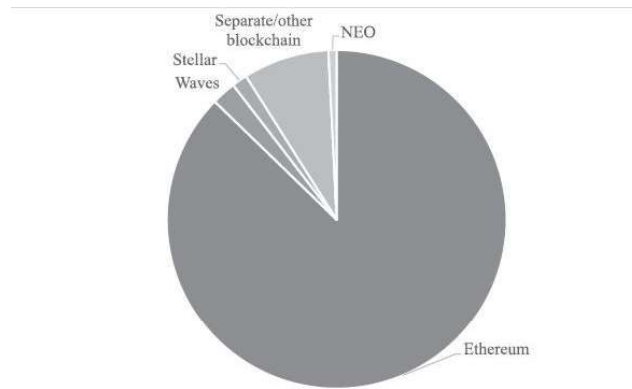


Figure 12: 87 % of all publicly funded projects are built on Ethereum Blockchain³⁹

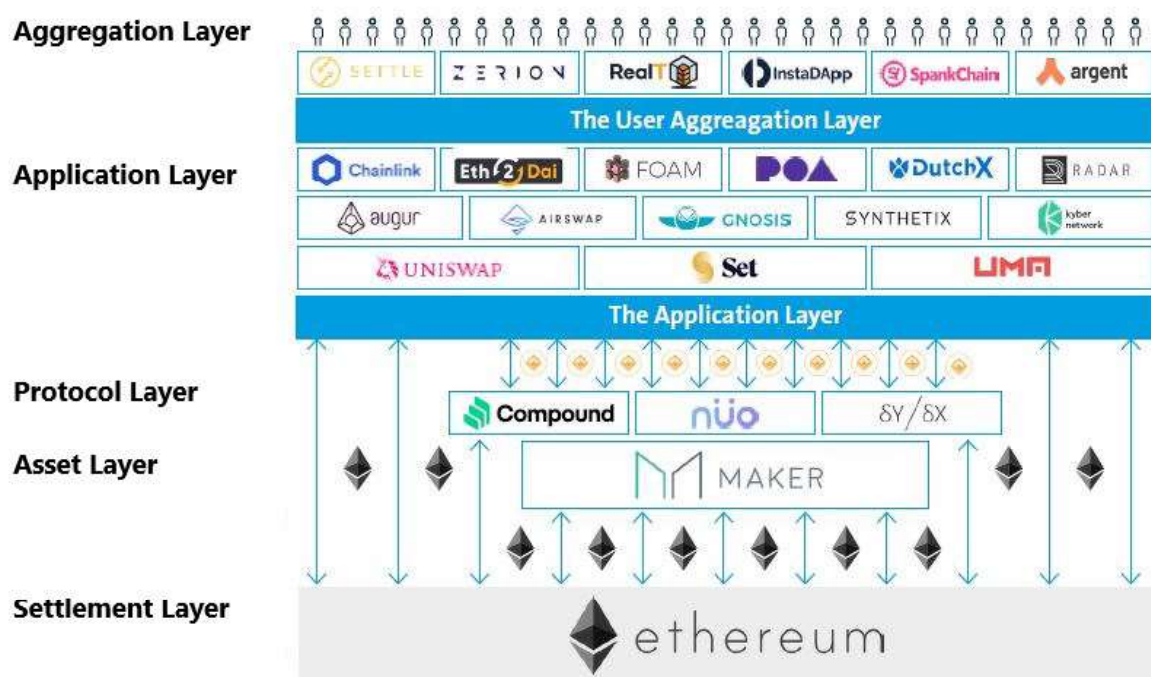


Figure 13: The Actual DeFI Ethereum Ecosystem, medium.com

Figure 19 shows how the decentralized financial system is declined on the Ethereum Blockchain. The various boxes show the names of the "companies" operating in the Ethereum DeFI market. Each of them offers their users a range of payment, credit and financial services. The common variable of these platforms is the Ethereum Blockchain and the Ether exchange currency. Often, all these platforms are able to communicate with each other thanks to the universality of the reference currency in this system. In order to access these services, the end user must open a digital "wallet" that is able to communicate with the Ethereum Blockchain. This wallet acts as a real wallet in which the sums denominated in ETH will be deposited. Therefore, the first step to access DeFI services is that of an "exchange" in which crypto-

³⁹Y. Chen, C. Bellavitis, 2020.

assets can be acquired by selling fiat currencies. Once the wallet has been created, users will be able to access one or more services offered by these companies simply by "logging in" through their wallet. Each Wallet, in addition to having a public address with which to receive or send funds, can be managed in digital format online or can be backed up off-line on special devices.

Going through the scheme from the bottom up, the various players offer ever greater and "all-round" services. As a matter of fact, if Ethereum is the basis of the whole architecture at the settlement layer, Maker (as seen in the 4th chapter) is the protocol that allows all Ethereum users to spend a stablecoin accepted throughout the system and the MakerDao platform represents the Asset layer. Once in possession of DAI, the user can not only use it as a means of exchange and payment, but also "sell" their liquidity at market prices through platforms such as Compound⁴⁰, Nuo⁴¹ and Dy/dx⁴².

Moreover, the protocol layer acts as a decentralized lending / borrowing system where liquidity shares are requested and offered at market interest rate that is instantly liquidated.

All the decentralized applications listed in the application layer offer greater and more complex financial services based on the crypto-assets. For example, "Uniswap⁴³" provides special smart contracts that allow to open derivatives positions on crypto-assets such as "tokens-swaps" and many others.

In the fifth level, the aggregation layer, integrated service providers are listed, which allow the end user to directly connect a wallet and access all types of DeFI services through the use of a single platform.

MAIN BUSINESS MODELS IN DECENTRALIZED FINANCE

In the light of these considerations, it can be said that the peculiarities of a decentralized financial system have boosted the birth and development of innovative business models, which offer traditional financial services, declined through "smart contracts", algorithms running on Blockchain without the need for human intervention.

My intent in this section is to run through the characteristics of these DeFI business models in more detail. We can group them into three sections: the decentralized credit market, the decentralized exchange market and the Decentralized Fundraising and capital market.

The Decentralized Credit market are an essential part of the DeFI ecosystem. There is a large variety of protocols that allow people to lend and borrow crypto-assets. Decentralized loan

⁴⁰ <https://compound.finance/>

⁴¹ <https://app.nuo.network/>

⁴² <https://dydx.exchange/>

⁴³ <https://uniswap.org/>

platforms are special in the sense that they require no identification from neither the borrower nor the lender. Everyone has access to the platform and can potentially borrow money or provide liquidity to earn interest. As such, DeFI loans are completely permissionless and not reliant on trusted relationships. In order to protect the lender and stop the borrower from running away with the funds, there are two distinct approaches: First, credit can be provided under the condition that the loan must be repaid automatically, meaning that the borrower receives, uses and repays the funds, all within the same Blockchain transaction. If the borrower has not returned the funds (plus interest) at the end of the transaction's execution cycle, the transaction will be invalid and any of its results (including the loan itself) reverted. These are the so-called flash loans (Wolff, Max, 2018). Flash loans are a very innovative and experimental application for crypto-based credit. As a matter of fact, in the traditional context they could not even be thought of. The transactions that are part of this contract are held in abeyance from the transcription of the new block into the Blockchain until the funds are returned by the borrower. If the return does not take place, the set of transactions and transfer of funds is immediately reversed and not transcribed in the Blockchain, reporting the *ex-ante* balance sheet positions. Although this type of digital lending can minimize, if not eliminate, credit risk, it opens up to other types of risk, both IT and cryptographic. If the block of an unpaid loan was mistakenly closed and reported on the ledger, this would lead to a big problem of double spending in the entire Blockchain which, at this point, would be irremediable.

Second, loans can be fully secured with collateral. The collateral is locked in a smart contract and only released once the debt is repaid. Collateralized loan platforms exist in three variations: Collateralized debt positions, pooled collateralized debt markets and P2P collateralized debt markets. Collateralized debt positions are loans that use newly created tokens while debt markets use existing tokens and require a match between a borrowing and a lending party (B. Ernesto, 2020).

More than 2800 out of the 5100 existing cryptocurrencies are listed on official exchanges. These numbers immediately highlight the fact that there is a demand for exchange services that cannot be ignored. Since the birth of Bitcoin, many exchange platforms have been born, in which the user could deposit sums also denominated in fiat and exchange them in the major cryptocurrencies on the market. The biggest shortcoming of these exchange platforms has always been centralization itself, which clashed with the central philosophy of Blockchain technology. It is only in recent years, starting from 2018, that Decentralized exchange platforms have developed, and, as mentioned earlier, those have become one of the main businesses in the DeFI ecosystem. Since 2018, there has been a move towards open exchange

protocols. These projects try to streamline the architecture of decentralized exchanges by providing standards on how asset exchange can be conducted, and allowing any exchange that is built on top of the protocol to use shared liquidity pools and other protocol features. Most importantly, other DeFI protocols can make use of these marketplaces and exchange or liquidate tokens when needed (Fabian Schar, 2020). According to Defirate, 2020 is quickly shaping up to be the year for decentralized exchanges to take the mainstage. With optimized usability, deeper liquidity, and emerging composability, the DEX⁴⁴ ecosystem is getting stronger by each day. When it comes to exchanging crypto, many have long been focused on centralized players due to their fiat on boarding and ease of use. Despite these notions, many have been quick to point out that centralized exchanges come with their own inherent risks – namely those of custody. In the past year alone, DEXes have made serious improvements in both usability and liquidity – signalling that they are ready to compete with their goliath counterparts (DeFirate.com, 2020).

Traditional venture financing often involves substantial friction in the fundraising process, as investors may only trust and invest in projects with strong network ties (Hallen, B.L., Eisenhardt, K.M., 2012). Blockchain technology is reshaping the fundraising landscape (Fisch, C., 2019). One primary form of decentralized fundraising is an initial coin offering (ICO). In an ICO, a project would create a project-specific token on a public Blockchain and sell the token to potential investors to raise funds for early-stage developments. Over the past few years, ICOs have emerged as an innovative funding mechanism for early-stage ventures, enabling entrepreneurs and innovators to raise billions of dollars from global investors (Martino, P et Al, 2019).

An ICO is a potentially powerful way for a project to raise funds and create network effects. By relying on distributed trust created by Blockchains, decentralized fundraising can reduce the friction in the gathering of funds, ease access to capital, and thereby promote entrepreneurship and innovation. Furthermore, an ICO is a new way for a project to co-opt stakeholders to bootstrap the creation of a new ecosystem (Chen, Y., 2018). Often, an ICO can be especially valuable when a token has inherent utility in the project's products or platforms. Such a token is often referred to as a utility token—it can either be redeemed for certain services or function as the primary medium of exchange. Some projects may issue security tokens, which represent direct ownership or claims on cash flows. A new variant—initial exchange offerings (IEOs)—have recently emerged. Unlike ICOs, IEOs rely on cryptocurrency exchanges to ensure the trustworthiness of potential projects and to connect high-quality projects to potential investors. In IEOs, cryptocurrency exchanges often examine

⁴⁴ Acronym used in crypto jargon to indicate the words "Decentralized Exchange".

potential projects, provide detailed information on promising ones, and endorse high-quality ones with their own reputation. Fig. 14 shows ICOs and IEOs in 2019 (Fabian Schar, 2020).

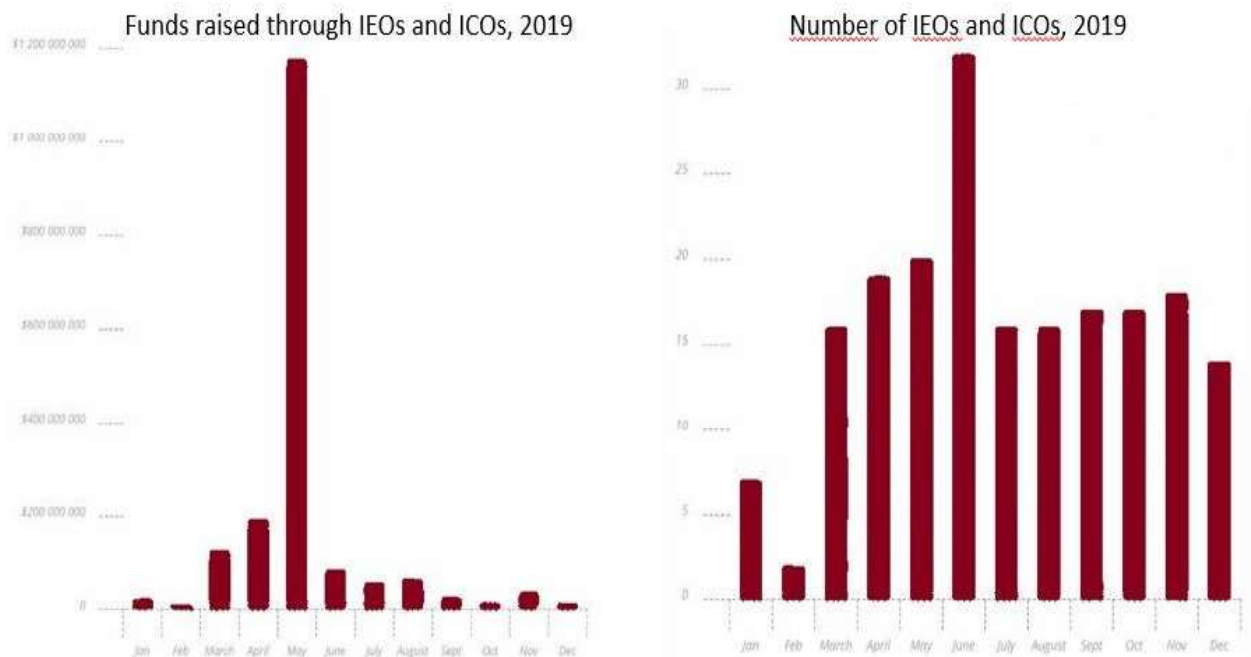


Figure 14 ICOs and IEOs in 2019

The figure shows us how numerous DeFI projects were financed through IEOs and ICOs in 2019, with a record of over 30 initiatives in June 2019 and a record of almost one billion and two hundred million dollars raised in May 2019: this proves the fact that, within this market, these innovative fundraising systems are preferred to canonical methods of crowdfunding or capital raising by new companies that want to enter the sector.

NUMBERS OF DEFI TODAY

In this short paragraph, after having listed the characteristics, the functioning and main business models of the DeFI world, I will list some figures on the DeFI market and ecosystem to date.

The most authoritative and reliable platform regarding data analysis in the DeFI market is currently Defipulse.com, where data on all existing DeFI operators is catalogued and updated daily. According to the latest available information on the platform, at the time of writing, the locked value in smart contracts amounts to a total of about seven and a half billion USD. This is a fundamental data not as an absolute figure (which is negligible compared to the values existing in traditional finance) but as a relative figure, as it represents a value fourteen times greater the record from the previous year. It is important to understand that these are not

transaction volumes or market cap numbers; the value refers to reserves that are locked in smart contracts (Fabian Schar, 2020).

Funds locked on smart contracts are a fundamental benchmark for the DeFi industry. This parameter shows investor confidence in the decentralized financial market: with the growth of funds for smart contracts the system tends to increase its stability and its available liquidity. In the last year, as can be seen from the image, a virtuous circle has been created with which numerous investments and capital have been brought into the DeFi market.



Figure 15: Total Value locked (USD) in DeFi - 09/2019-09/2020

DeFIPulse also offers a ranking of the best platforms by quantity of locked value and quality of services offered. Figure 16, as a matter of fact, shows the ranking of the best 10 platforms to join DeFi services. This table, in addition to showing us that all the 10 largest platforms in the market are based on the Ethereum Blockchain, also lists the type of provided services (lending, Assets Management, Crypto-derivatives, Dex or Decentralized Exchanges), the locked value in their smart contracts and the average daily interest rate of your contracts.

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Aave	Ethereum	Lending	\$1.54B	10.84%
2.	Maker	Ethereum	Lending	\$1.26B	3.86%
3.	Curve Finance	Ethereum	DEXes	\$1.05B	3.57%
4.	yearn.finance	Ethereum	Assets	\$806.1M	3.18%
5.	Synthetix	Ethereum	Derivatives	\$715.6M	10.06%
6.	Compound	Ethereum	Lending	\$612.6M	2.43%
7.	Balancer	Ethereum	DEXes	\$564.9M	-1.13%
8.	WBTC	Ethereum	Assets	\$514.4M	2.60%
9.	Uniswap	Ethereum	DEXes	\$450.1M	-69.30%
10.	RenVM	Ethereum	Assets	\$235.6M	13.83%

Figure 16: Defipulse ranking of the top 10 DeFI platforms⁴⁵

**THE CONS OF DECENTRALIZED FINANCIAL SYSTEMS:
TECHNICAL, CENTRALIZATION, LIQUIDITY AND REGULATORY RISKS.**

On a technical level, all transactions recorded on the Blockchain are irreversible. This determines the risk of incorrect or fraudulent operations within the system. Because of the fact that DeFI is primarily based on the integrity of smart contracts and the Blockchain protocol on which it rests, any failure in the programming code could lead to computer fraud or massive data loss for Dapps users. The correction of errors and frauds in these IT protocols is not as immediate and simple as the cancellation of financial transactions in the traditional system could be. The existence of an infinite number of possible combinations for smart contracts means that there are no standard situations and uniform procedures for the settlement of any errors.

There have been a wide range of DeFI hacks where several million “in USD value” have been stolen or lost. Potential remedies for code bugs and technical failures could be third party audits and insurance schemes, regulation in the form of necessary risk management procedures, capital buffers, and consumer protection. Alternatively, transparent and formalized processes of “good governance” within the DeFI protocols could be adopted,

⁴⁵ DeFipulse.com last accessed August 2020.

which can quickly freeze the smart contract, update the code, or even undo certain transactions in extreme cases, such as the DAO fork refund 2018⁴⁶.

Moving beyond all the technical risks involved in the settlement layer of the DeFI architecture, as seen in the previous paragraphs, most DeFI protocols rely on Ethereum, which, in periods of high usage, has suffered from many slowdowns and congestion, making the market inefficient and harmful to users.

Another type of risk that the DeFI ecosystem suffers from is that of usability. The user experience of these platforms are often complicated, not very intuitive and created for users who are already experts in the sector (J. Grigo and P. Hansen, 2020).

The great effort of the DeFI developers will consist in making the use of the various platforms more accessible and intuitive. Each platform is often based on the use of its own token that serves as a currency to access the services offered. The large number of tokens and different platforms is a limit to the DeFI ecosystem as it requires different "units of measurement" and it is not provided with a single and universal *passpartout*.

The DeFI world is not totally exempt from what is called counterparty risk in finance. Many Dapps have been founded by teams or companies of investors and developers and this makes them very far from being completely decentralized, at least in their initial phase of stabilization in the market.

For example, Compound - the second most prominent DeFI lending protocol - was designed with the ability to be upgraded in place by a central administrator. Only recently, the platform launched its COMP token and started decentralizing its governance, openly stating that this shift would be conducted over a period of time⁴⁷.

In these cases, the counterparty risk could arise since the intermediary managing the DeFI platform under consolidation could use users' funds and assets in an improper and fraudulent way.

The risk of centralization mainly derives from the fact that, in most projects, they are equipped with a "master key" owned by the team developers that allows them not only to turn off or deactivate the Dapp⁴⁸, but also to easily provide system updates or emergency shut off in case of technical problems. While it is expected that with the evolution of a totally decentralized governance system the problem of centralization will be reduced over time, at the moment it cannot be neglected.

⁴⁶ https://www.google.com/search?q=dao+fork+undone&rlz=1C1GGRV_enDE781DE781&oq=dao+fork+undone&aqs=chrome..69i57.7322j0j7&sourceid=chrome&ie=UTF-8

⁴⁷ <https://www.theblockcrypto.com/post/62126/DeFI-compound-decentralized-governance-token-coinbase-live>

⁴⁸ Decentralized Application

In the financial industry, liquidity is essential to ensure that an efficient pricing system exists. In the DeFI world, liquidity risk is not only due to the fact that there is no body of last resort in the system whose purpose is to safeguard the system, but also from the fact that technical congestion and Blockchain slowdowns can lead to large market inefficiencies with serious effects on the liquidity of the system itself. For example, on March 12, 2020, the crypto-assets market fell by about 40%, coinciding with the collapse of the global stock market due to the Covid-19 virus. When volatility picks up and markets drop, a few things happen concurrently: liquidations in DeFI projects such as in Maker's smart contracts accelerate, arbitrageurs that don't have enough capital on each venue begin shuttling assets between the exchanges in order to arbitrage the price discrepancies, and demand for block space explodes upwards. Transaction fees on Ethereum skyrocket, and transactions don't get included in a block for minutes, or even hours (J. Grigo and P. Hansen, 2020).

At the same time, as prices collapse, miners start turning off their machines because mining revenues fall below the cost of electricity, which in turn further slows the rate at which new blocks are produced, increasing latency and decreasing aggregate throughput⁴⁹.

The crypto market suffered a lot from this sharp decline but the DeFI world was much more affected much more. The Maker platform on which much of the decentralized system rests was close to default. The principle that brought Maker and all Ethereum DeFI to its knees was that many collateralized debt positions were liquidated in short intervals, but with the congested Ethereum network, many of these transactions were not included in the blocks of the Blockchain. The price of Ethereum plummeted thus uncovering all collateralized positions.

Regulation risk represents the uncertainty about the future regulation that a legislator will be able to enact regarding the DeFI sector. In many jurisdictions, decentralized projects operate unlicensed regardless of their location. As we will see in the next chapter, institutions have just begun to give directives in the crypto world, but as far as the regulation of the DeFI sector is concerned (around 1% of the crypto world at the time of writing)⁵⁰, there is still no regulatory certainty. At the fiscal level, there is still no legislation that clearly defines how to allocate the income deriving from DeFI assets. However, the critical point for this sector is that Financial regulation necessarily requires some sort of responsible counterpart figure that would clash with the nature of decentralized projects. One possible solution to this dilemma might be a new way of supervising and regulating financial risks, called “embedded supervision” by the Bank for International Settlement⁵¹. Embedded supervision is a regulatory framework that provides for compliance with regulatory standards in DLT based markets to

⁴⁹ <https://multico.in.capital/2020/03/17/march-12-the-day-crypto-market-structure-broke/>

⁵⁰ According to <https://www.coindesk.com/learn>

⁵¹ <https://www.bis.org/publ/work811.html>

be automatically monitored by reading the market's ledger. It would reduce the administrative burden for firms, while increasing the quality of data available to the supervisor (R. Auer, 2019).

In any case, the issues concerning the anti-money laundering regulations and the fight against terrorist financing, on the identification of the beneficial owner of the assets, the origin and destination of funds on decentralized platforms are still critical.

As in any type of revolutionary technological innovation, the legislative gap that is created will only be filled in the medium to long term, when the intervention of the main financial and regulatory institution will be inevitable and necessary.

CRYPTO WORLD REGULATION:

HOW CRYPTOCURRENCIES AND DECENTRALIZED FINANCE RELATE TO THE EU DIRECTIVES.

My intention to develop a comparison between traditional finance and decentralized finance, which is based on Blockchain technology, cannot disregard the analysis of an important issue such as the current regulation for all financial intermediaries that provide investment, financing and payment instruments. My aim is to dwell on the main European directives that regulate the credit and financial sector, and to analyse step by step the course of action pursued by the regulators with the adaptation of the regulatory framework to the growth of the crypto and Blockchain sector. At the end of this section I will dedicate short space to personal judgments on whether these directives can be interpreted as a sign of openness or, alternatively, as a display of rejection from the regulator towards the crypto world.

The main directives that I want to review are on anti-money laundering and countering the financing of terrorism.

ANTY MONEY LAUDERING: 4TH AND 5TH DIRECTIVE

The greatest strength of Blockchain technology is complete anonymity, albeit contextualized in the total advertising of each transaction recorded in the distributed ledger. In order to analyse this issue, as well as to compare centralized and decentralized financial systems, it is necessary to frame the current legislative plan establishing the rules for financial intermediaries.

Within the European context, the directives governing anti-money laundering and countering the financing of terrorism are the EU directive 2015/849 of the European parliament and of the council, issued on 20 May 2015 (also known as Know your customer (KYC) or AML directive 4th) and the EU directive 2018/843 of the Parliament and the Council, called Anti-money laundering directive 5th (AMLD5) of 30 May 2018. The latter directive integrates and amends the former. For the purpose of my thesis, I will focus on the integrations that have been introduced with regards to the field of digital currencies. At the European level, the current regulation on anti-money laundering and countering the financing of illegal activities, were issued by the Council and the European Parliament with the prior approval of the European central bank, indeed as reported in the official gazette of the European Union, published on 12 June 2013, the European Central Bank supports the development of an

economic union that gives the member states the necessary tools to combat terrorist financing and money laundering.

On 10 June 1991, the first European directive on anti-money laundering (CD 91/308/ EEC) on the "prevention of the use of the financial system for the purpose of money laundering⁵²" was issued, and with the subsequent amendments and additions disclosed in 2001, 2005 and 2006, the European Union embarked on an important regulatory path against the illicit and fraudulent use of capital which led to the already mentioned AMLD4 and AMLD5. The Council of the European Union and the European Parliament list the reasons behind the necessity of a strong focus on anti-money laundering and the fraudulent use of capital by all financial operators:

- First, it is essential to limit illicit cash flows as they damage the integrity, stability and reputation of the financial sector itself. With worrying consequences for civil society.
- Secondly, supranational cooperation is needed since money laundering and terrorist financing are often carried out by international associations, and regulation by member states alone could have very limited effects.
- The third fundamental point is that the European banking system could be jeopardized by the very freedom of movement of capital existing within the Union. It is necessary to coordinate anti-money laundering and counter terrorist financing operations at a European level to prevent illicit capital from being moved between the various member states without supranational monitoring.

After introducing the reasons as to why it is essential to combat financial crimes, and underlining the importance of combating them at EU level and not only at national level, Article 1 of the KYC directive provides a clear definition of money laundering and terrorist financing. The third comma of article 1 defines money laundering as the transfer of assets, deriving from criminal activities, with the aim of concealing their illegal origin and in order to avoid any legal consequences for the subjects involved in the transaction.

Subsequently, in the following paragraphs, the directive specifies that the concealment or camouflage of the true nature, source, location, arrangement, movement, rights with respect to, or ownership of, ownership, knowing that such ownership arises from a criminal activity or an act of participation in such an activity; the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from a criminal activity or from an act of participation in such activity; participation, association to be engaged, attempts to engage and help, aiding, facilitating and consulting a commission of one of the actions mentioned above.

⁵² Official Journal of the European Union L141 / 74 5 / 6/2015

Financing of terrorism is defined as the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning⁵³

The second article lists the entities that are bound by the provisions of the directive. It is important to point out that regulations concerning the world of cryptocurrencies have been introduced from 2015 to 2018: this highlights the fact that the regulator can no longer ignore the strong rise of cryptocurrencies and their impact on the financial system. With the 2015 legislation, the subjects required to comply with the requirements laid down by the directive were:

- Credit and financial institutions.
- Legal or natural persons acting in the exercise of their professional activity such as statutory auditors, auditors and tax consultants.
- Notaries and other legal professionals if independent, if they participate in their professional activity in financial securities or real estate transactions.
- Trust or fiduciaries.
- Real estate agents.
- Betting service providers.
- Other subjects who exchange goods settled in cash for a sum greater than or equal to 10 thousand euros, in a single or in more related transactions⁵⁴.

I would also like to underline the fact that, in the 2018 directive, the following definition of cryptocurrency was introduced for the first time:

“virtual currencies” means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”⁵⁵

Subsequently, the directive broadens the scope of application of the rules in question to new entities that deal with providing exchange services between fiat currencies and cryptocurrencies. These entities are defined as follows:

⁵³ *Article 1 – General Provisions* KYC Directive (EU) 2015/849 of the European parliament and of the council of 20 May 2015 – Official journal of the European Union

⁵⁴ *Article 2 – General Provisions* KYC Directive (EU) 2015/849 of the European parliament and of the council of 20 May 2015 – Official journal of the European Union

⁵⁵ AML Directive (EU) 2018/843 of the European parliament and of the council of 30 May 2015 – Official journal of the European Union

“... entities that provide services to exchange cryptocurrencies in fiat currencies, safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.”⁵⁶

The regulatory provisions of the Directive are expressed in Articles 10 and 11. Specifically, Article 10 prescribes that member states prohibit the holding of anonymous current accounts or deposit books with their financial and credit institutions. In addition to the documentary collection necessary to establish continuous relationships with customers, it is also necessary to carry out customer due diligence, that is, an in-depth fact-finding questionnaire with which the most important information of the account holders holding contractual relationships is collected.

Article 11 lists the occasions the observance of the "customer's due diligence" procedure is mandatory:

- Whenever a business relationship is established with a new customer.
- Whenever an occasional transaction exceeding EUR 15 000 is concluded.
- Whenever a transfer of funds between parties is made using bearer payment methods.
- When there is a proven suspicion of money laundering or terrorist financing without any kind of lower limit.
- When there is a proven suspicion of fraud of the information released by the customer during the customer due diligence.

Finally, the following articles, (12, 13 and 14) reiterate the mandatory procedure for financial intermediaries and all the other subjects listed above, that is, the precautionary verification of the identity of the customers in the commercial relationship, which can rely on any public information available on the subjects.

AMLD5 GAPS AND NEXT STEPS.

As a result of AML5D, obliged entities, providers of custodian portfolios and providers engaged in exchange services between virtual currencies and fiat currencies must comply with the same AML/CFT requirements as banks and other financial institutions. They must register with national anti-money laundering authorities, implement customer due diligence checks (so-called "know your customer" checks), monitor virtual currency transactions, and report suspicious activity to government agencies. Furthermore, only fit and appropriate people can become their managers and / or beneficial owners (R. Houben & A. Snyers, 2020).

⁵⁶ Article 1 Amendments to Directive (EU) 2015/849 AML Directive (EU) 2018/843 of the European parliament and of the council of 30 May 2015 – Official journal of the European Union

Nevertheless, a large number of legislative gaps, mostly due to the fast evolution of the crypto-world, can still be found in EU law (L. Cancelli, 2020).

As a matter of fact, according to Cancelli, the first problem of this directive is that cryptocurrencies are considered as a means of payment, as a store of value but not as a financial investment instrument. The other major deficiency of the directive is the regulation towards crypto-crypto service providers. As a matter of fact, all platforms that rely solely on cryptocurrencies provide the user with the user with a private and a public key, guaranteeing the anonymity of the same. In these areas, there's no possible way to know the true identity of the user, a problem which still leaves large margins for the fraudulent use of capital.

Indeed, according to the aforementioned document commissioned by the Committee on Economic and Monetary Affairs, it has been recorded that the most recurrent illegal activities carried out through the use of cryptocurrencies, include the purchase and sale of illegal goods or services online in the darknet markets, money laundering, circumvention of capital controls and stealth ransomware attacks. In this type of transactions, cryptocurrencies take on the role of payment instruments between anonymous addresses on platforms exempt from the AMLD5 directive, as they do not require exchange operations between fiat and cryptocurrencies. According to the commission, one of the first regulatory actions to be considered is the expansion of the Definition of virtual currencies towards the inclusion of crypto-tokens or other crypto-assets, the use of which has been increasing use in recent years and which have not been considered within the regulatory scope of the AMLD5. Secondly, the list of obliged entities should be expanded. The critical points concern cryptocurrency exchange activities in cryptocurrencies; financial service providers active in holding and raising funds related to an issuer's offer (ICO); and decentralized finance platforms that operate directly on the Blockchain.

In my opinion, the answer that the regulator will give to these regulatory gaps will be decisive, as a matter of fact, in addition to financial fraud itself, the damage on the financial system is also due to the large regulatory uncertainty affecting the cryptocurrency sector. An increasing number of institutional financial operators (and in part also retail) are actively following the growth of the crypto-assets phenomenon, but the regulatory uncertainty often acts as a deterrent in the choice of resource allocation, thus determining a slowdown in the scalability and diffusion of these technologies between people, entrepreneurs and financial operators.

CONCLUSIONS

CRYPTO-ASSETS: DYNAMICS OF THE LAST YEARS

Blockchain technology appeared with the advent of Bitcoin 12 years ago, and while it may seem like a paltry time period, many aspects of this industry have changed. Satoshi Nakamoto's noble purpose of creating an inclusive, universal and decentralized payment system has been denatured over time. The cause of this outcome was the great speculation induced by the volatility of an asset that was initially supposed to act as a trading currency. Because of this, Bitcoin has always divided the general opinion between avid supporters and sceptical detractors. Regardless of this, the path of diffusion and development of this cryptocurrency has been incessant and objective. Despite all the inherent flaws that have been pointed out throughout the thesis, the merit of Bitcoin has been that of attracting developers, investors and analysts to the Blockchain sector. Since the introduction of Bitcoin, many other cryptocurrencies were born and flooded the market to such an extent that the term crypto-asset was coined, which reflects the need to differentiate and distinguish the function and purpose of different financial instrument.

The masses and volumes of money on the crypto market are negligible when compared with those of traditional financial instruments and deposits denominated in fiat currencies, but it is crucial to bear in mind that the whole phenomenon is no older than twelve years. In my opinion it is much more explanatory to analyse the phenomenon from a relative point of view and in terms of growth.

To give an idea, the growth that has taken place in the crypto sector from the beginning of 2017 has been incessant and impressive. If in 2017 the market capitalization of crypto-assets was equal to 18 billion dollars, with daily transactional volumes of about 190 million dollars, today the capitalization of the crypto market has grown 18 times and amounts to 332 billion dollars with trading volumes intraday that touch almost 100 billion dollars⁵⁷. 85 percent of this share is covered by the 10 largest cryptocurrencies by capitalization and use. These ten alone boast a capitalization of at least one billion dollars each, which makes us deduce that although there are thousands of projects and cryptocurrencies listed on the market, the vast majority of them can be considered projects of little objective relevance.

Table number 4 summarizes the main data of the major Crypto-assets on the market:

⁵⁷ According to Coinmarketcap.com data.

RANK	NAME	MARKET CAPITALIZATION (Millions USD)	VOLUME (24h, Millions USD)	CIRCULATING SUPPLY (in its own currency)
1	Bitcoin	199.570,97	35.672,711	18.497.606 BTC
2	Ethereum	40.452,794	10.502,996	112.720.935 ETH
3	Tether	15.518,100	36.028,746	15.204.746.688 USDT
4	Ripple	10.920,933	1.573,420	45.097.364.449 XRP
5	Bitcoin Cash	4.241,613	1.378,162	18.525.469 BCH
6	Polkadot	3.703,626	393,470	852.647.705 DOT
7	Binance Coin	4.174,901	515,983	144.406.560 BNB
8	Crypto.com Coin	3.121,270	61.178,343	20.215.525.114 CRO
9	Chainlink	2.943,132	1.274,254	350.000.000 LINK
10	Litecoin	2.940,341	1.676,453	65.519.157 LTC

**Table 4: Ranking of the 10 most important Crypto-assets on the Market.
According to Coinmarketcap.com**

Reflecting on capitalization data and transactional volumes, a fact that I really care to highlight is the decline in the dominance of bitcoin in the crypto world. As previously exposed, the term Bitcoin dominance refers to the percentage of capitalization of Bitcoin relative to the total crypto-assets capitalization. Today this value stands at around 57 percent, which still makes Bitcoin “the king” of cryptos, but is important to note that this value has not always been at these levels. As a matter of fact, if we consider the data from the beginning of 2017, the monopoly of the most noble global cryptocurrency would seem to have weakened considerably, given that at the beginning of that year the dominance of bitcoin was equal to 87%. In my opinion, the loss of almost 30% percentage points over four years opens up interesting food for thought. As an observer of this sector, I would say that such this decrease in relevance can be explained through two processes that have occurred in recent years, one directly dependent on Bitcoin, while the other referring to the growth of all other cryptocurrencies, in particular Ethereum. It is reasonable to think that the largest Bitcoin investors, perfectly aware of the structural limitations and high management costs of this Blockchain, have begun to differentiate their portfolios over time by entering relevant positions on other cryptocurrencies (G.Brown and R.Whittle, 2020). Another factor that

cannot be overlooked is the growth of Ethereum and of the entire ecosystem that orbits it. The dominance of Ethereum as opposed to Bitcoin has grown from 3.90% to 12% in the past four years. Furthermore, almost all of the DeFI market rests on the Ethereum platform and it is therefore foreseeable the future influence of this cryptocurrency will grow in absolute terms and also in relation to Bitcoin. Furthermore, the advent of Ethereum 2.0 and its state-of-the-art proof of stake system from an energy point of view, will give an important turning point to the entire crypto-assets sector.

REGULATION AND PUBLIC OPINION

As previously analyzed in the sixth chapter, the big problem that has accompanied the crypto world from the very beginning concerns its regulation and the relationship with institutional bodies around the world. The fate of crypto assets and of all operators working in the decentralized finance market strongly depends on how regulation in this sector will be managed. In my opinion this will be a decisive step for the transformation of the sector from a niche to a "mass" sector. I use the word "niche" in its most positive meaning, that is "destined for greater potential growth": as the majority of newly-born technologies in recent years, the intrinsic potential of DeFI is not clearly Defined and can be the object of further investigation in the coming years.

According to an international survey carried out in June 2018 by ING⁵⁸, 66% of the population is aware the existence of cryptocurrencies but only 9% of citizens own some. In spite of this, 35% of respondents say the future of payments will be made in cryptocurrencies⁵⁹.

Among the various results that emerge from the survey, there is a particular aspect that I personally found worthy of interest. The interviewed subjects who declared themselves regular users of mobile banking apps are the individuals who, in a higher percentage, declare they want to enter the crypto market in the coming years. I think that this hint may constitute an interesting point of contact between traditional banking and the crypto world, as the most confident users of digital versions of the banking world are also the most predisposed to try the new financial market based on crypto and digital assets. In my opinion, as an operator in the banking sector, traditional banks should further dig out the potential interest that customers could have in the crypto world, in view of a future turning point with reference to a potential new offer of dedicated services. The numbers seen above clearly indicate that a

⁵⁸ Ing International Survey, 2018

⁵⁹ Survey conducted on a sample of 14 828 people from 15 European countries, the United States and Australia.

demand for services related to crypto-assets is not only present on the market, but is also strongly on the rise.

Despite the growth in market demand in the crypto sector, and therefore to a potential sale of innovative high-margin services, banking institutions around the world have always had a great distrust of this new type of financial instruments due to the large legislative gap that surrounded them.

Given this legislative problem, on 22 July 2020, the American regulator - the government office responsible for currency control (OCC) - authorized federal banks to provide their customers with the custody service of listed cryptocurrencies. The OCC's official press release states that " providing cryptocurrency custody services, including holding unique cryptographic keys associated with cryptocurrency, is a modern form of traditional bank activities related to custody services".⁶⁰

With a view to a transition process towards innovative finance, also based on crypto-assets, this statement by the OCC is a fundamental step towards regulating the sector.

As we have seen above, the interest of several central banks in CBDCs, the anti-money laundering inclusion of cryptocurrency operators, and the authorization for US federal banks to offer crypto custody services to clients, are small signals that demonstrate the direction taken (in small steps) by the economic-financial world towards that of the crypto economy and Blockchain technology.

Moving from the United States to the EU, on 24 September 2020, a first real legislative turning point took place thanks to a regulatory proposal by the European Commission⁶¹. According to this legislative draft, all operators in the crypto-currency market will have to directly receive authorization to operate from the member states. This authorization can only be granted if the companies are compliant with the capital requirements necessary for the management of highly volatile assets and adequate IT security that protects customers. Furthermore, all crypto operators will necessarily have to offer a service for handling complaints, like normal banking institutions.

The commission also established that companies that decide to offer their services to crypto-investors must necessarily have a physical registered office within the European Union.

All entities issuing stablecoins will be obliged to redeem customers with an exchange rate of 1 to 1 at any time.

Despite the bill still needing to undergo the legislative procedure by the European institutions (that is, being approved by the European Parliament and the European Council), it seems that

⁶⁰ OCC's official press, News Release 2020-98|July 22, 2020

⁶¹ <https://www.ilsole24ore.com/art/ue-nuove-regole-criptovalute-misure-salvaguardia-patrimonio-e-diritti-investitori-ADYtrPr>

the direction taken is that of an opening towards the crypto-economy from the part of the European Institutions.

In my opinion, it is also important to reflect on how the crypto industry will react. How will the more orthodox current, devoted to a total decentralization of the monetary system, react? It is not unlikely to think that the more this sector is institutionalized, with regulation and openness to the traditional banking world, the more decentralized platforms will be researched, studied and created that are exempt from institutional control. As a matter of fact, we must bear in mind that the primary purpose of Bitcoin, and of all the following cryptocurrencies, originally was to establish a universal, democratic monetary and payment circuit with no institutional barriers.

It will be crucial to follow how events will evolve in the coming years, as well as how cryptocurrencies will be regulated in Europe and, therefore, how the banking and financial players of the old continent will move. In this last section of the thesis I wanted to express many personal opinions because I believe it is essential to observe, know and debate what is happening today in alternative financial markets to the traditional ones. I do not want to express a clear favourable or unfavourable opinion regarding the benefits that can be gained from crypto-assets in all their forms. However, I believe it is very useful - if not even necessary - for those involved in the financial sector, to be aware of the evolution of the crypto economy sector in spite of the almost total silence of the media, as well as of the role that these technologies will play in changing our investment habits and allocation of economic resources in the future.

BIBLIOGRAFY:

1. Harari, Y.N. (2011). Sapiens, a brief history of humankind.
2. Houben, R. and Snyers, A. (2018). Cryptocurrencies and Blockchain, legal context and implications for financial crime, money laundering and tax evasion, requested study by the tax3 committee of the European Parliament.
3. H. Natarajan, S. Krause, and H. Gradstein, World Bank Group (2017). Distributed Ledger Technology (Dlt) And Blockchain. Fintech Note, No. 1. Washington, D.C.
4. Committee on payment and markets infrastructures (2015). Digital currencies.
5. European central bank (2015). Virtual Currency Schemes – a further analysis.
6. Ernst & Young (2018). IFRS – Accounting for crypto-assets.
7. s.lee 2018
8. Bianchi, R., Chiap, G. and Ranalli, J. (2019). Blockchain - tecnologia e applicazioni per il business.
9. Houben, R. and Snyers, A. (2020). Crypto-assets – Key developments, regulatory concerns and responses, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies Authors: study Requested by the ECON committee.
10. Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System.
11. Popescu, A.D. (2020). Decentralized Finance (DEFI) – The Lego of Finance, Social Sciences and Education Reserch Review.
12. Popper, N. (2016).
13. Gervais, A., Ghassan, O. K., Wust, K., Glykantzis, V., Ritzdorf, H., Čapkun, S., (2016). On the Security and Performance of Proof of Work Blockchains.
14. Redman, J. (2018). 80% of the 21 Million Bitcoins Have Been Mined Into Existence.
15. Ari, P. (2017). Forbes.
16. Dennin, T. (2019). From Tulips to Bitcoins, a history of fortunes made and lost in commodity markets.
17. Zeller M. (2019).
18. European banking authority (2019). Report with advice for the European Commission on crypto-assets.
19. Blemus, S. and Guegan, D. (2019). Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance.
20. Nannings, M. (2019). Kwalificatie van crypto-assets als effect, *TFR* 2019/12, (623) 624.
21. Bullmann, D., Klemm, J. and Pinna, A. (2019). In search for stability in crypto-assets: are stablecoins the solution?, European Central Bank.
22. Mita, M., Ito, K., Ohsawa, S. and Tanaka, H. (2015). What is Stablecoin? A Survey on Its Mechanism and Potential as Decentralized Payment Systems.
23. Barontini, C. and Holden, H. (2019). Proceeding with caution – a survey on central bank digital currency. Bank for International Settlement paper n.101.
24. Lannquist, A. - World Economic Forum, (2019). Central Banks and Distributed Ledger Technology: How are central banks exploring Blockchain today?
25. ECB, (2020). Report on a Digital Euro.
26. Lagarde, C. (2019). Introductory speech statement at the ECON committee of the European Parliament.
27. Bonneau, J et al. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.
28. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.Sok, (2015). Research perspectives and challenges for bitcoin and cryptocurrencies. In:2015 IEEE Symposium on Security and Privacy. pp. 104-121.
29. Viktor, F. and Luders, B.K. (2020). Measuring ethereum-based erc20 token networks.

30. Werner, S.M., Pritz, P.J. and Perez, D. (2020). Step on the Gas? A Better Approach for Recommending the Ethereum Gas Price.
31. Buterin, B.V. (2013). Ethereum White Paper - A Next Generation Smart Contract and Decentralized Application Platform.
32. Kyber Network (2019). Whitepaper.
33. Roth, A.E., (2015). Who Gets What—and Why: the New Economics of Matchmaking and Market Design.
34. Cohen, J.E. (2019). Between Truth and Power: the Legal Constructions of Informational Capitalism.
35. Chen, Y., (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation.
36. Financial Stability Board, (2019). Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications.
37. Schar, F. (2020). Decentralized finance; On Blockchain-and Smart contract- based financial markets.
38. Makerdao (2019). The Day stablecoin whitepaper.
39. Catalini, C., Gans, J.S., (2019). Some simple economics of the Blockchain.
40. Huberman, G., Leshno, J.D., Moallemi, C., (2019). An economist's perspective on the bitcoin payment system.
41. Cerf, V., (2012). The dynamics of disruptive innovation: internet speculations.
42. Brynjolfsson, E., McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.
43. Chen, Y. and Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*.
44. Ammous, S., (2018). *The Bitcoin Standard: the Decentralized Alternative to Central Banking*. John Wiley & Sons, Hoboken, NJ.
45. Seidel, M.-D.L., (2018). Questioning centralized organizations in a time of distributed trust. *J. Manag. Inq.* 27 (1), 40–44
46. Wolff, M. (2018). *Introducing Marble: A Smart Contract Bank*.
47. Boado, E. (2020). *Aave Protocol Whitepaper v1.0*.
48. Hallen, B.L., Eisenhardt, K.M., (2012). Catalyzing strategies and efficient tie formation: how entrepreneurial firms obtain investment ties. *Acad. Manag. J.* 55 (1), 35–70.
49. Fisch, C., (2019). Initial coin offerings (ICOs) to finance new ventures. *J. Bus. Ventur.* 34 (1), 1–22.
50. Martino, P., Wang, K.J., Bellavitis, C., DaSilva, C.M., (2019). An introduction to Blockchain, cryptocurrency and initial coin offerings. *New Frontiers in Entrepreneurial Finance Research*, pp. 181–206
51. Grigo, J. and Hansen, P. (2020). Decentralized Finance (DeFI) –A new Fintech Revolution? *The Blockchain Trend explained*. Bitkom, federal association for information technology, telecommunications and new media e.V.
52. Auer, R. (2019). *Beyond the Doomsday Economics of 'Proof-of-Work' in Cryptocurrencies*.
53. European parliament (2015). *AMLD4 - Know your customer (KYC) EU directive 2015/849*.
54. European parliament (2018). *AMLD5 - Anti money laundering Directive (EU) 2018/843*.
55. Cancelli, L. (2020). *The Growing crypto-assets threat to anti-money laundering: How institutions are coping with this phenomenon*.
56. ING International (2018). *International Survey Mobile Banking. Cracking the code on cryptocurrency. Bitcoin buy-in across Europe, the USA and Australia*.

SITOGRAPHY:

1. <http://Documents.Worldbank.Org/Curated/En/177911513714062215/Pdf/122140-Wp-Public-Distributed-Ledger-Technology-And-Blockchain-Fintech-Notes.Pdf>
2. <https://academy.binance.com/it/Blockchain/decentralized-autonomous-organizations-daos-explained>
3. <https://app.nuo.network/>
4. <https://bitcoinaverage.com/en/bitcoin-price/btc-to-eur> last accessed August 2020
5. <https://bitcoinaverage.com/en/bitcoin-price/btc-to-eur> last accessed August 2020
6. <https://Blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network/>, last accessed August 2020
7. <https://Blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network/>,last accessed august 2020
8. <https://Blockchainwhispers.com/Maker-Price.pdf>
9. <https://blog.trendmicro.com/wp-content/uploads/2018/03/blog-1024x349.png>
10. <https://blogs.airdralert.com/free-crypto-masternodes/>, last accessed August 2020
11. <https://blogs.airdralert.com/free-crypto-masternodes/>, last accessed august 2020
12. <https://coinmarketcap.com/> Last accessed August 2020 AMLD4 or KYC Directive (EU) 2015/849 of the european parliament and of the council of 20 May 2015 – Official journal of the European Union
13. <https://coinmarketcap.com/> Last accessed September 2020
14. <https://compound.finance/>
15. <https://cryptonzy.b-cdn.net/wp-content/uploads/2018/03/Bitcoin-quantity-chart1.jpg>, last accessed August 2020
16. <https://cryptonzy.b-cdn.net/wp-content/uploads/2018/03/Bitcoin-quantity-chart1.jpg>, last accessed August 2020
17. <https://DeFipulse.com/>
18. <https://DeFIrate.com/dex>
19. <https://doi.org/10.1109/SP.2015.14>
20. <https://doi.org/10.2139/ssrn.2874598>.
21. <https://dydx.exchange/>
22. <https://eba.europa.eu/eba-reports-on-crypto-assets>
23. https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png last accessed August 2020
24. https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png last accessed August 2020
25. <https://github.com/aave/aaveprotocol/>
26. <https://makerdao.com/it/whitepaper#abstract> Last accessed September 2020
27. <https://medium.com/marbleorg/introducing-marble-a-smart-contract-bankc9c438a12890>
28. <https://medium.com/reserve-currency/the-end-of-a-stablecoin-the-case-of-nubits-dd1f0fb427a9> Last Accessed September 2020
29. <https://news.bitcoin.com/80-of-the-21-million-bitcoins-have-been-mined-in-to-existence>
30. https://pbs.twimg.com/media/DuGgqN_WoAAGbnZ.jpg
31. <https://tether.to/> Last accessed September 2020.
32. <https://uniswap.org/>
33. <https://www.bis.org/cpmi/publ/d137.pdf>
34. <https://www.buybitcoinworldwide.com/it> last accessed August 2020
35. <https://www.buybitcoinworldwide.com/it> last accessed August 2020
36. <https://www.coindesk.com/learn>
37. <https://www.coinhouse.com/bitcoin-studied-through-monetarism-prism/#:~:text=We%20will%20look%20at%20%E2%80%9Cthe,or%20MV%20%3D%20>

- PT)%20where%3A&text=M%20is%20the%20money%20supply,millions%20of%20bitcoins%20(BTC). Last accessed August 2020
38. [https://www.coinhouse.com/bitcoin-studied-through-monetarism-prism/#:~:text=We%20will%20look%20at%20%E2%80%9Cthe,or%20MV%20%3D%20PT\)%20where%3A&text=M%20is%20the%20money%20supply,millions%20of%20bitcoins%20\(BTC\).](https://www.coinhouse.com/bitcoin-studied-through-monetarism-prism/#:~:text=We%20will%20look%20at%20%E2%80%9Cthe,or%20MV%20%3D%20PT)%20where%3A&text=M%20is%20the%20money%20supply,millions%20of%20bitcoins%20(BTC).) Last accessed August 2020
39. <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191202~f8d16c9361.en.html>
Last accessed August 2020
40. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
41. <https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications/>
42. <https://www.ilsole24ore.com/art/ue-nuove-regole-criptovalute-misure-salvaguardia-patrimonio-e-diritti-investitori-ADYtrPr>
43. The End of a Stablecoin - the case of NuBits, Reserve research team, Medium.com, July 2018
44. www.bitkom.org