LUISS

Department of *Economics and Finance*
Master's degree in *Finance*
Chair of *Financial Market Law and Regulation*

Central Bank Digital Currencies: risks, opportunities and challenges.

Prof. Paola Lucantoni
SUPERVISOR

Prof. Mirella Pellegrini
CO-SUPERVISOR

Marco Peluso 707621
CANDIDATE

Academic Year 2019/2020

I pioppi sono pioppi.

Le querce sono querce.

Contents

Introduction **1**

1 The evolution of the money **3**

1.1 From barter to bills 3

1.1.1 Barter 4

1.1.2 Coins 6

1.1.3 Bills 7

1.2 The role of gold in the monetary system 9

1.2.1 Gold Standard 9

1.2.2 Bretton Woods 11

1.2.3 The birth of Bitcoin 13

1.3 Kind of money in the current system 13

1.3.1 Cash 13

1.3.2 Bank deposit 14

1.3.3 Central Bank Reserve 14

1.3.4 Electronic money 15

1.3.5 Digital currency 17

2 The era of cryptocurrencies **19**

2.1 Origin of cryptocurrencies 19

2.2 Why use cryptocurrencies? 22

2.3 Coin and Token 23

2.4 Stablecoins 24
2.4.1 How the stablecoins work? 26
2.5 Tecnology 29
2.5.1 Distributed Ledger Technology 29
2.5.2 Blockchain 30
2.5.3 How the Bitcoin Blockchain works? 34

3 Regulation **41**
3.1 An uncertain regulatory framework 41
3.1.1 Looking for a legal nature 41
3.1.2 Risks related to the absence of legislative protections . . . 44
3.1.3 Exchange 45
3.1.4 Initial Coin Offering (ICO) 47
3.2 Kind of approaches 51
3.2.1 Inaction 51
3.2.2 Prohibition 52
3.2.3 Regulation 54
3.3 The European situation 60
3.3.1 European Union 60
3.3.2 European Banking Authority 62
3.3.3 European Securities and Markets Authority 67
3.3.4 European Blockchain Association 67
3.3.5 Association for Trusted Blockchain Applications 69
3.4 Markets in Crypto Asset Regulation (MiCA) 71
3.4.1 Scope and definitions 72
3.4.2 Supervisory Authority 74
3.4.3 Regulations for Cryptocurrency Service Providers 76
3.4.4 European States want to protect consumers 77
3.5 US Banks and stablecoins 78

4 Central Bank Digital Currency **81**

4.1 A new financial system 81

4.2 Definition of CBDC 83

4.3 Central Banks and financial intermediation 84

4.4 Possible scenarios 87

4.5 Diem 88

4.5.1 Diem association 90

4.5.2 Risks 91

4.6 Digital Euro 92

4.6.1 The Digital Euro must meet the needs of change 92

4.6.2 How the Digital Euro will work 94

4.6.3 Benefits 94

4.6.4 Areas of uncertainty 95

4.7 Digital Yuan 97

4.7.1 Cross-border payments 98

4.7.2 The first tests 99

4.7.3 China wants to be a pioneer 100

Conclusions **103**

Glossary **107**

Bibliography **111**

Abstract **123**

Introduction

Money is indispensable for the functioning of an economic system. First metallic, then paper, electronic and now also digital. The choice of digital currency as a research topic is based on several factors involving this type of money.

The financial innovations that society has experienced in recent centuries are strongly linked to the degree of technological progress. This data can be seen by analyzing the development of telecommunications and the opportunity it represents for entities that provide financial services, which constantly introduce new products and services on the market aimed at improving the efficiency with which their users carry out transactions.

In addition to the innovations promoted by the financial system itself, there is a trend whose goal is to allow economic agents to transact independently of financial institutions, which has been combined with advances in cryptography research, more generalized internet access and increasing the processing capacity of computers. Together, these elements have facilitated the development and worldwide expansion of assets known as cryptocurrencies.

A cryptocurrency needs an infrastructure to function, this infrastructure is called Blockchain and can be defined as an electronic accounting system that keeps records of transactions between people. This accounting system is decentralized, i.e. it does not require a third party to validate the accounting entries.

In this system, encryption is used as a technique that allows you to verify the secure transfer of resources between economic agents and, in addition, to control the creation of additional drives in the system.

The transaction log is transmitted in real time to the entire network, generating a large number of copies. The owner of these units has the option of storing them in a digital wallet, which can be accessed via an electronic device.

Some characteristics of cryptocurrencies allow them to be used mainly as a mechanism for storing value, but also as a medium of exchange, uses traditionally assigned to the currency issued by Central Banks.

This could lead to confusion among some economic agents about its potential use and the risks it poses to personal finances, the financial system and the economy as a whole.

As a result, Central Banks face a difficult choice between two options: block cryptocurrencies or issue a Central Bank Digital Currency (CBDC).

In seeking a comprehensive view of this phenomenon, this research incorporates considerations from not only the European Central Bank, but also from the different supervisory entities of the global financial system.

The document is structured as follows: after this introduction, chapter 1 deals with the history of money we know today, starting from bartering to modern means of payment. The origin of the Blockchain technology that allowed the emergence of cryptocurrencies is summarized in chapter 2, while chapter 3 analyzes the legal aspects of these assets. The possible implications from the point of view of the global financial system due to the so-called CBDCs are described in chapter 4.

Chapter 1

The evolution of the money

> *"For there was once a time when no such thing as money existed... a material was selected which, being given a stable value by the state, avoided the problems of barter by providing a constant medium of exchange. That material, struck in due form by the mint, demonstrates its utility and title not by its substance as such but by its quantity, so that no longer are the things exchanged both called wares but one of them is termed the price. And today it is a matter for doubt whether one can talk of sale when no money passes."*
>
> – Julius Paulus Prudentissimus[1]

1.1 From barter to bills

The different means of payment, and in particular money, in the course of their evolutionary history, have had the characteristic of influencing all the dimensions of collective and individual work, thus obtaining a profound impact on the human societies that use them. However, it would be difficult to appreciate the true impact of the changes that are taking place today, with regard to electronic

[1]Paulus served as chief legal advisor to the Roman emperor Severus Alexander (222-235 AD)

means of payment, if one does not first make a brief historical overview of money and its different meanings.

1.1.1 Barter

The currency was not born in a day but is the result of a long process of evolution of the means of payment, determined by the search for more effective methods to facilitate trade. Once the currency did not exist, people in that period lived in small settlements, grew vegetables and raised livestock. Clothes, food and drink were produced exclusively for the family. But what if a family from that period needed a little more milk? This family should have gone to another family and started doing business. For example, they might trade chickens for a new cow.

The human needs for the exchange of goods have led to the search for quantifiable and lasting means to carry out this exchange, or as it is better known: barter.

This bartering trade became increasingly clumsy and cumbersome in the more developed societies[2]. How many chickens do you need for a sheep? Three, four or maybe five? Or what if a person needs something but has nothing that the other party wants to get in return? That is why there was a growing need for an item that was generally accepted in exchange for goods and that was easy to handle.

This is how money was born. Over the centuries, many different objects have been used as money. Livestock, salt, as well as pearls and shells were once used in a similar way to our coins and bills. As a means of exchange or payment, "money" must meet a number of conditions.

[2]See Davies Glyn 2002, p. 9

Traditionally, money has been defined as an asset that acts as a unit of account, a store of value and a medium of exchange[3]:

- **Unit of account**: money allows you to realize the relative value of goods and make choices accordingly, comparisons are much more complicated in a barter system. It thus makes economic calculation possible, i.e. the allocation of resources where they are useful, based on their optimal use;
- **Store of value**: money allows savings, i.e. the accumulation of capital. Saving therefore allows for long-term development and growth. But for this to happen, the currency must be stable, meaning that you can save without fear that the physical money or the amount deposited in the bank will lose in value;
- **Medium of exchange**: Money should be able to facilitate the sale of goods and service. The seller in a transaction must accept the instrument as a means of payment with the belief that the seller can give the instrument as a method of payment for other transactions. Moreover, money should be divisible in order to conduct transactions of any size making possible exchanges that would be too complex, and therefore impossible, with a simple barter.

These functions are closely related to each other. For example, an asset is less useful as a medium of exchange if it is not so valuable tomorrow, i.e. if it is not a good store of value. Indeed, in some countries where prices have risen due to very high inflation rates, other foreign currencies have been used as an alternative medium of exchange. For example, in the five years after the end of the First World War, the prices of goods in German marks have doubled 38 times. For this reason, at that time in Germany some people started using other coins instead of marks to buy and sell things.

[3]See Brunnermeier Markus K., James Harold 2019, p. 7

Another important aspect is that a person should not be able to mint money himself, otherwise it would lose its value. Cowries, which are small shells, have been used as currency in Asia and Africa for thousands of years, so shells have become a kind of money. An advantage of cowries is that they are all the same size, but this "money" also had disadvantages: those who lived near the beach always had many shells. So in places near the beaches the shells were worth less than in places far from the beach. If money is to be used as a medium of exchange, it must have the same value everywhere.

In addition to shells, in ancient times salt was also used as a currency. For a long time, salt was very important and valuable to people as they used it for meat and to preserve fish and vegetables. Salt was very rare at the time and has been used as a means of payment for a long time[4].

1.1.2 Coins

With the passage of time, the usefulness of the old means of exchange diminished when the metal was discovered, as it was a scarce and difficult to find commodity, its shelf life was much greater, it did not disappear when consumed and could be segregated into small pieces. It should be noted that the metals whose importance and use transcended others were gold and silver, which would form the basis for forging the new means of payment: money.

The first coin was made in western Turkey around 700 BC[5]. They were not yet real coins, but worked nuggets made of gold or silver. These nuggets thus became the first official means of payment.

More complex coins arrived in Roman times. Roman coins were first minted around 200 BC. The most precious Roman coins were made of gold and silver, then there were copper ones. Throughout the Roman Empire it was possible

[4]See Davies Glyn 2002, p. 27

[5]See Ibidem, p. 64

to pay with these coins, just as it is now possible to pay with the euro almost everywhere in Europe. As now, even in Roman times there were people who began to forge money. Sometimes secretly putting iron or copper in gold and silver coins. This began to become a problem, especially in the 3rd and 4th centuries, as the content and weight of a coin deteriorated more and more. At one point only small copper coins began to circulate and the entire monetary system collapsed causing barter to return.

Between the 11th and 13th centuries, many cities in Europe began to flourish thanks to trade and industry. These cities were located at important hubs along major sea routes: around the Baltic Sea, on the North Sea, on the edge of the Mediterranean and on major rivers such as the Rhine and Meuse.

The burgeoning trade increased the need for money that was universally accepted. Then the barter economy returned to a monetary economy.

Thanks to this economic boom, gold coins reappeared for the first time in the 13th century. A very famous coin was the gold florin issued by the city-state of Florence. This Italian city-state was at the time one of the richest areas in Europe. The first gold florin was minted in 1252[6].

Due to trade, more and more different coins came into circulation. Specialized knowledge was needed to distinguish them and know what they were worth. It is therefore understandable that goldsmiths were the first to engage in the money trade. In medieval Italy, goldsmiths inspected, weighed and exchanged coins for a small fee in return.

1.1.3 Bills

Of course, people who had money wanted to keep it safe. Goldsmiths and money changers have always had a safe home for fear of theft, this is why they often acted as cashiers and for a fee they took coins and other valuables for safekeeping

[6]See Davies Glyn 2002, p. 145

for others. The money changer had a book in which he wrote how much money he kept and for whom. Customers of course received a receipt and could later exchange that receipt for their own money. Soon people, thanks to the ease of use, started paying each other with these receipts just like we do today with bills. Furthermore, it was simply impractical to carry large quantities of gold and silver coins.

The money stayed in the same place, but the owner of the money kept changing. Instead of coins, you could also pay for purchases with a piece of paper. This gave the recipient of the document the right to withdraw money from the "bank" where the buyer had placed it in custody.

Because the account holders never withdraw their credit at the same time, the "bank" has been able to lend some of those funds to others. Thus began to grant loans, grant credits and so in the late Middle Ages the first banks in Italy arose. The oldest bank in the world, Banca Monte dei Paschi in the Italian city of Siena, was founded in 1472.

Paper money, initially convertible into metallic currency, are finally transformed into "fiduciary" or "fiat currency"[7], that is, not convertible except in itself, the value of which is based exclusively on the trust placed in it by citizens. Today, with the transition from analogue to digital society, we are faced with a progressive dematerialization of money, the phenomenon of which is indicated with the term cashless society.

[7]The term "fiat" refers to the phrase from the Bible "Deus fiat lux et lux facta est" translated "God said light is made and light was made", precisely to describe the nature of these coins and the fact that they are created out of nothing.

1.2 The role of gold in the monetary system

1.2.1 Gold Standard

The gold standard had its heyday during the 18th and early 19th centuries, in which many countries that adopted different metal standards adopted gold as their only monetary base. In 1871, the German Empire made gold its standard and in 1873 a parallel decision followed in the United States. By 1878, silver had been demonetized in France and virtually every other European country[8]. By the end of the 19th century, most of the leading countries had established a fixed exchange system of their currencies in relation to gold, with Central Banks pledging to buy and sell gold indefinitely at the fixed exchange rate. Gold thus became the main element of the international monetary system.

In addition to the redemption of gold, the system contained a number of rules that Central Banks would have to abide by. For example, in the event of an outflow of gold due to an external imbalance, the Central Bank would have to raise interest rates to reduce the supply and demand for domestic money. Similarly, the Central Bank would have to lower interest rates in the event of an influx of gold. By adjusting the interest rate in the event of imbalances, it was thus possible to obtain a stabilizing effect on the system.

The classical gold standard, with its clearly defined rules, contained a binding mechanism that gave the system a high degree of credibility. The classical gold standard coincided with the time when Britain had its heyday and when London served as a world financial center. Britain's long link with the gold standard underpinned the system's importance, and many countries using the gold standard had the pound as a reserve of foreign exchange. Holding pounds was seen as another way to hold gold, while pounds was just a more appropriate means of trading. The classical gold standard lasted until 1914 when due to First

[8]See Scammell William M. 1965, p. 32

World War countries began to make autonomous decisions and the conversion was stopped. Thus system passed from a system of fixed exchange rates to a system of floating exchange rates.

At the end of the First World War, to decide how to reorganize the post-war monetary system, representatives of thirty-four nations, including all the great powers except the United States, met in Genoa. During the Genoa conference, which lasted from April until May 1922, it was decided that it was necessary to reintroduce a system similar to the gold standard. Britain dominated the conference and together with many other countries decided that a return to the gold standard was necessary and, above all, that it was necessary to return to the exchange rates of the pre-war period. This scenario was unimaginable for most continental European countries because inflation, caused by the war, greatly diminished the value of their currencies relative to pre-war values. To return to those values, the countries that had experienced high inflation would have needed severe deflation otherwise their currency would have been widely undervalued.

This decision to return to pre-war parity served primarily to restore confidence in the monetary system.

United State aid was essential and made it possible for the British to return to the old rate. "For America, the stabilization of the pound was considered very important precisely because it was an important step towards the stabilization of the European currency, a fundamental prerequisite for achieving American financial and commercial ambitions"[9].

The British, with this American assistance, were able to re-establish pre-war parity in May 1925. This result was widely criticized by John Keynes who argued that the pre-war parity was too high and the result would be unnecessary and painful deflation for the British economy[10]. After Britain re-established the gold standard, nearly forty other countries followed.

[9]See Clrarke Stephen V. O. 1967, p. 72

[10]See Keynes John M. 1925, p. 207

In the interwar years, therefore, the gold standard system was reintroduced but differed from the classical gold standard in a number of respects. One significant difference was that gold was withdrawn from circulation and placed as a reserve in Central Banks.

In addition, in order not to put pressure on gold reserves, the United Kingdom through the British Gold Standard Act of 1925 introduced a Gold Standard in gold bars and at the same time put an end to the circulation of gold coins. Under the classical gold standard, the Central Bank was obliged to redeem every single note on demand, whereas now the Central Bank was only obliged to distribute whole gold bars, i.e. to exchange amounts corresponding to the value of a whole gold bar. This saved money on gold and there was no need for such extensive gold coverage. At the same time, it reduced gold's role as a medium of transaction and removed gold from citizens.

Another important difference from the past was that Britain had lost its role as an economic and political leader. This meant that the pound lost its former importance in the international monetary system and that the dollar was increasingly used as a reserve currency.

The gold standard of the interwar period collapsed in connection with the depression of the 1930s. Britain left gold in 1931 and the United States in 1933.

1.2.2 Bretton Woods

The difficulties of reconstruction after First World War prompted Western powers to meet in Bretton Woods, in the United States, in 1944 to develop a new international currency system. Understanding the importance of formulating rules to guide national policies after the war to facilitate common objectives, two pillars of the new international financial system were founded: the International Monetary Fund and the World Bank.

Countries with payment problems could turn to the IMF for credits and foreign currency. The bank focused on rebuilding. The two dominant countries, the

United States and the United Kingdom, disagreed on how the system should be designed, and also on the future role of gold.

Britain had used up all of its gold and foreign exchange reserves during the war and therefore wanted a system in which gold played only a minor role. The United States, on the other hand, had large gold reserves and wanted a firm link to gold. In the end, it was the American proposal based on a close relationship with gold that won.

Countries in the system could choose a direct link to gold, or an indirect one by bonding to the dollar, which was defined in relation to gold at 35 dollar per ounce[11].

Foreign exchange reserves could then be held in both dollars and gold in what might be called the gold-dollar standard. Most countries have chosen to tie their currencies to the dollar. The United States was obliged to buy and sell gold to maintain the gold price, while the other countries in the system were obliged to maintain their exchange rate in relation to the agreed parities within a margin of +/- 1 percent by buying and selling dollars.

The redemption of gold, which had been a fundamental component of the classical gold standard, was limited in the Bretton Woods system to apply only to Central Banks. Therefore, there was no longer general access for citizens to gold reserves.

The Bretton Woods result marked the new status of the United States as an economic powerhouse. All other countries now had the value of their currency pegged to the dollar, which was the only currency pegged to gold. However, the more dollars that came into circulation, the more difficult it was for the United States to fulfill this obligation. It would deplete the gold reserves. This scenario became a reality in the 1960s.

The United States has seen its share in the world economy shrink due to, among others, the rise of Germany and Japan. The country printed dollars to

[11]See Davies Glyn 2002, p. 447

finance the costs of the Vietnam War. The US also suffered from solid inflation. Confidence in the dollar has declined. More and more countries have exchanged their dollars for gold and let go of the bond with the American currency. Despite numerous attempts to stem the crisis, the Bretton Woods system collapsed in August 1971, when President Nixon announced that the dollar was no longer redeemable against gold. This put an end to the Bretton Woods system. The IMF and the World Bank remained and continued to grow into important economic institutions.

1.2.3 The birth of Bitcoin

Fast forward to the 21st century, many things have happened since the end of the gold standard. In 2008, a financial crisis erupted that threatened to destroy the global banking system. To prevent a collapse of the system, Central Banks around the world bailed out financial institutions, printed huge amounts of money, and engaged in massive asset purchases (a practice known as quantitative easing).

It is precisely in this context of mistrust towards the monetary system that an anonymous programmer, who calls himself Satoshi Nakamoto, launches the first cryptocurrency in the world: Bitcoin. Contrary to the modern monetary mechanism, he included in the first block of the blockchain the title printed on the cover of a British newspaper: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

1.3 Kind of money in the current system

1.3.1 Cash

Cash in circulation, i.e. bills and coins, represents only a small amount of money held by individuals and companies in the economy. Cash is typically printed, minted and provided by the Central Bank to be used by all economic actors

(private money users, commercial banks, Central Banks and governments).

The use of cash has advantages such as the immediacy of the transaction and the absence of transaction costs. However, to simplify large transactions and for security reasons, consumers generally don't want to keep all their money in cash. Additionally, outstanding cash pays no interest and is therefore less attractive to hold than other assets, such as bank deposits. For these reasons, most consumers prefer to keep an alternative medium of exchange: bank deposits.

1.3.2 Bank deposit

When a consumer deposits his bills in a bank, the commercial bank receives additional bills but in return credits the amount deposited into the consumer's account. Consumers exchange their money for bank deposits because they believe they can always be repaid. Banks must therefore ensure that they can always obtain sufficient amounts of money to meet the expected demand of depositors and redeem their bills. These deposits are guaranteed up to a certain value[12], to ensure that customers continue to trust them. This ensures that bank deposits are considered to be easily convertible into cash and can serve as a medium of exchange.

The use of bank money is so widespread that even many people now receive salary payments in bank deposits and not in cash, in fact most people no longer use cash to make purchases but use credit cards linked to bank deposits.

1.3.3 Central Bank Reserve

Commercial banks must hold cash to meet bank customer withdrawals and any cash flows. To avoid the use of cash, which would be very inconvenient for the

[12]In Europe, the Interbank Deposit Protection Fund is a special fund whose function is to provide compensation, in the cases provided for by law and up to a maximum of 100,000 euros, in the event of a bank failure.

numerous and large transactions that banks carry out between themselves, banks can hold a different type of money: Central Bank reserves.

The reserves of a Central Bank are simply an electronic record of an amount owed by the Central Bank to each individual bank. Central Bank reserves function exactly like traditional deposits, the difference is that companies and non-bank individuals cannot have access to Central Bank reserves for payments or deposits. The operation is very simple, when a bank has to transfer funds to another bank it will tell the Central Bank to adjust its reserve balances accordingly. An example would be paying by credit card in a store, if the merchant's bank is different there will be a request from the bank to transfer those funds[13].

In any case, the Central Bank, as the issuer of outstanding liquidity, always guarantees the conversion of these reserves into cash in the event that a bank has a request for payment to private consumers.

1.3.4 Electronic money

The history of credit card

The modern technology of payments really began to evolve with the invention of the credit card. The first cards appeared in the United States, but not as they are currently issued: at banks, but at gas stations. This new idea was immediately adopted by chain stores and then, finally, in 1950, Diner's Club created the first credit card, made of cardboard and intended for general consumer use in restaurants.

Subsequently, in some states of the North American country, a credit card was also used that authorized a person to stay in any of the hotels that made up

[13]The clearing phases are managed by private operators at periodic time, who operate in competition with each other, while the settlement phase is typically carried out by Central Banks. This last phase consists in determining the multilateral balances for each participant (debit/credit position towards all other participants in the system) and in settling the balances on the accounts held with the Central Bank.

the hotel chain. Also, in 1920, the gasoline company Texaco and Esso took on the task of distributing credit cards for the purchase of products whose use was disappearing due to war rationing. However, later, some railway companies begin to deliver them, the custom is extended to airlines. The idea seemed so feasible to merchants that companies in charge of credit card management quickly emerged, changing their base and issuing new plastic cards, which has allowed, since the 1960s, an even greater and faster spread of this new financial invention.

However, when banks realized that there was a new financial product that threatened to take their credit control away for relatively small amounts, they decided to create their own laminated credit cards[14]. The American bank to which the first creation of a card of this type is attributed is the Bank of America, which in 1958 was entrusted with the task of introducing the card called BankAmericard to the market. Therefore, all the other banks, observing the success of the aforementioned raid bank, also aspired to have their own credit card, however, due to its poor development, many of them failed in the attempt, hence the only option to get their own card, had to become part of the existing credit network, provided by the most powerful banks, economically speaking.

In 1977 BankAmericard changed its name to "Visa" and this bank achieved a significant spread of credit cards in its country of origin, putting into circulation about 400 million cards.

Later, in 1967, the New York City Bank also managed to introduce its own credit card called the Everything Card, which later became the famous "MasterCard" card.

The development of payments technology

The recent past has seen a wave of innovations in payment technologies. A number of innovations allow families and businesses to convert bank deposits into other purely electronic forms of money (sometimes referred to as "electronic money")

[14]See Ryan Andrea, Trumbull Gunnar, Tufano Peter 2011, p. 474

that can be used to transact. These technologies seek to improve the payment process (e.g. PayPal) and for some transactions it may even be more convenient to use money from an electronic account instead of bills or bank deposit. These forms of money have some characteristics similar to bank deposits. For example, money in an e-money account represents a store of value provided the supplying companies are trusted. Electronic money can also be used as a medium of exchange with companies or people who accept it.

1.3.5 Digital currency

Another class of innovations are digital currencies, such as Bitcoin. The key difference between these and local currencies is that the exchange rate between digital currencies and other currencies is not fixed. Today, digital currencies are not widely used as a medium of exchange. But its popularity comes mainly from its ability to serve as an asset class. As such, they may have more conceptual similarities with commodities like gold than with money. They also differ from the other technologies discussed so far in this box because they can be created from scratch, albeit at predetermined speeds. Although the amount of money held in electronic accounts or in local currencies depends entirely on demand, the supply of digital currencies is generally limited.

Chapter 2

The era of cryptocurrencies

"There are three eras of currency: Commodity based, politically based, and now, math based."

– Chris Dixon[1]

2.1 Origin of cryptocurrencies

The genesis of cryptocurrencies stems from the cypherpunk movement of the early 1990s. In the words of Julian Assange, one of the leading figures in this movement, a cypherpunk is "an activist who uses cryptography as a form of non-violent direct action to achieve political and social change"[2].

The cypherpunks were initially a group of activists with high knowledge of cryptography, computing and programming who were very concerned about the possibility that the government was using the internet as a mechanism for repressing people and violating their privacy and personal freedom. A small group

[1]Chris Dixon (born 1972) is an American internet entrepreneur and investor. Co-founder of Hunch now owned by eBay and Co-founder of SiteAdvisor now owned by McAfee.

[2]See Assange Julian, Appelbaum Jacob, Muller-Maguhn Andy, Zimmermann Jeremie 2016, p. 15

of this conglomerate of activists, has consistently talked about the need and possibility for a digital currency to be anonymous or could be anonymized using cryptography[3]. And this is precisely the ideological basis of cryptocurrencies.

The goal of the cryptographic mailing list[4] group was to create a decentralized electronic currency that would be used as an alternative to government-issued fiat money.

The characteristics that this currency should have should be the following: that it was anonymous, decentralized and that the exchange between users of this digital currency had to be direct and not depend on banking or financial institutions as intermediaries[5].

Prior to the creation of cryptocurrencies, cypherpunks developed various electronic currency prototypes such as BitGold, B Money and DigiCash. These early prototypes did not work due to the following factors: there was no adequate technological development to implement them in a functional way, the internet was not yet fully integrated into international trade and there was no market for people willing to acquire these products because they did not see a real need to depart from the legal tender with which they were already familiar[6].

---

[3]See Kaplanov Nikolei M. 2012, p. 112

[4]The cryptographic mailing list was a mailing list created by Tim C. May and John Gilmore with the purpose of establishing communication with other members of the cypherpunk movement with the aim of exchanging ideas for the creation of protocols or systems that make possible the processing a decentralized virtual currency, among the top crypto mailing list members were David Chaum (creator of Digicash), Hal Finney (RPoW developer), Phil Zimmermann (PoP crypto developer), members of the cryptography mailing list, Wei Dai (creator from B money) , Nick Szabo (creator of Bit Gold), Adam Back (creator of Hash Cash) and Satoshi Nakamoto (creator of Bitcoin)

[5]See Assange Julian, Appelbaum Jacob, Muller-Maguhn Andy, Zimmermann Jeremie 2016, p. 23

[6]See Pitta Julie 1999

The cypherpunk dream of an electronic currency foreign to any government or institution seemed like a utopia. However, an event set the stage for that dream to come true. That event was the 2008 financial crisis.

A global economic crisis erupted in 2008 following the collapse of the financial market in the United States. The origin of this crisis is mainly due to the fact that in the early 2000s, banks and financial institutions created subprime mortgages as a type of structured financial product to obtain large economic benefits from what was initially believed, very low risk. These were variable rate mortgages aimed at users with bad credit histories and precarious financial resources, for that these users were at high risk of default in the payments of these mortgages[7].

Banks and financial institutions made large profits through these mortgages, but created a financial bubble that burst as millions of debtors went insolvent at the same time in late 2007, unable to pay mortgage interest[8]. Many banks, corporations and other financial institutions began to fail such as Circuit City, Washington Mutual, and the famous Lehman Brothers[9]. In the face of the crisis, the US Federal Reserve intervened and began providing emergency loans to banks through the TARP Program[10], known as Bank Rescue.

The bank bailout was harshly criticized by the US population as many families went bankrupt and lost their homes as they watched the government bail out the banks and corporations that were the main causes of the crisis[11].

Outrage in the North American country increased when they observed that no legal measures were taken to condemn those responsible for the economic ruin. All these factors have led many people to feel mistrust and repudiation of financial

[7]See Rimkus Ron 2016

[8]Ibid

[9]Ibid

[10]TARP: Troubled Assets Relief Program. $700 billion to bail out banks and support other sectors of the economy

[11]See Murphy Austin 2008, p. 15

and banking institutions.

Suddenly, the ideas that cypherpunks had seemed aligned with the sentiment of the population, cryptocurrencies now seemed achievable in the market. Two weeks after the Lehman Brothers bankruptcy, a cryptographic mailing list user whose true identity still remains a mystery, Satoshi Nakamoto, published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"[12] proposing a computer protocol to create the first cryptocurrency.

2.2 Why use cryptocurrencies?

Cryptocurrencies have a number of advantages over the current financial system. First of all, the Blockchain system makes the transaction costs practically free and the transfer of value is instantaneous, while transactions in the financial system are subject to high percentage fees and charges, and due to centralization, validating a transaction or transfer takes much longer.

Cryptocurrencies have the ability to make transfers regardless of the size of the transfer, for example, it is possible to send five or ten dollars from one account to another in different continents while, in the current financial system, the same transfer would not be possible for the high percentage of commission charged by the intermediary financial institution of the transaction.

The second benefit provided by cryptocurrencies is that it would allow millions of people who don't have a bank to participate in the financial market. By not asking for any kind of requirements, this would make it easier for millions of people to be able to make money transfers.

The third advantage that cryptocurrencies offer is the privacy to its users in their purchases, as they act in a similar way to cash. The fourth advantage that cryptocurrencies provide through its Blockchain system is transparency and security in transactions since all these are stored in a public ledger that is replicated

[12]See Nakamoto Satoshi 2008

in all nodes of the network.

Finally, many cryptocurrencies are resistant to inflation since, like gold or silver, there are a finite number of them, unlike fiat money which can be printed indefinitely by a central bank.

All of the above features make this technology ideal for money transfer, but this is only the first application that has been used for this new technology. Future uses of cryptocurrencies and Blockchain systems are expected to grow exponentially.

2.3 Coin and Token

The terms cryptocurrency and token are often used interchangeably but they are not exactly the same: while all tokens are cryptocurrencies not all cryptocurrencies are tokens. Cryptocurrencies can be divided into two categories:

- **Coin**: they use their own Blockchain;
- **Token**: they rely on another Blockchain.

It is important to note that the commissions for sending a token are paid precisely in the coin of the Blockchain it relies on. A token can always be converted into a coin: Tron (TRX) born in 2017 as a token on the Ethereum Blockchain became a coin when in 2018 it switched to its own Blockchain.

Tokens are usually issued via Initial Coin Offering (ICO). The Startup issues digital tokens and then sells them to finance the project.

There are many types of tokens, the main ones are:

- **Utility tokens**: give the owner the rights to use certain products or services and used outside the context in which they are exchanged, they have no value. Some examples can be the points of the supermarket, of an airline, etc. . . ;

- **Asset tokens**: represent the right of ownership of a certain asset that is held by the company that issues them, some very famous examples are Tether (USDT) for the dollar and Paxos Gold (PAXG) for gold;
- **Equity tokens**: These work just like regular stocks and represent ownership of an underlying company.

Tokens can be traded Peer-to-Peer without any intermediary, enabling a new type of decentralized digital market. In addition, there are tools that allow the issuer of a token to send cryptocurrencies to all token holders, just like the dividends that are paid by companies to shareholders.

2.4 Stablecoins

Cryptocurrencies are currently going through a period of accelerated growth, as, together with the Blockchain, they have demonstrated their high potential. However, they have proved impractical in common use for several reasons, mainly due to the volatility of their price.

Bitcoin price - Source: CoinMarketCap[13]

[13]https://coinmarketcap.com/currencies/bitcoin/

The stablecoins have been introduced to contain price movements and bring some stability to a market that has, up to now, been quite difficult to control.

A stablecoin is a cryptocurrency with a fixed price, i.e. it maintains a constant value with respect to a target price. The price of most cryptocurrencies is determined by the market, on the contrary, stablecoins aim to maintain a fixed price which must be maintained through different mechanisms.

The stablecoins are therefore a very interesting proposal because, maintaining all the advantages of the Blockchain, they provide the necessary stability that makes them usable in real life.

At the moment, cryptocurrencies are mainly held by investors and speculators who seek to maximize their profits in relation to the price of the various cryptocurrencies in the market. Few people will keep their cryptocurrencies and use them for the daily purchases they make with fiat currencies. Therefore, it is hard to imagine anyone accepting their salary to be paid in Bitcoin given the significant fluctuations cryptocurrencies undergo during the same day. By guaranteeing a fixed price, stablecoins would make the following use cases possible.

Greater global access to a stable currency

The relative stability of the US dollar or Euro is often taken for granted. While inflation is slowly eroding the value of the US dollar, this gradual erosion remains low compared to the hyperinflation experienced by countries like Argentina, Egypt, or Nigeria. In these countries, annual inflation rates often exceed 15%[14].

Citizens of these countries will therefore want to have a certain amount of stable currency, such as the US dollar, to preserve a certain level of wealth.

A stablecoin could make this possible even as the capital regulators of these countries try to prevent citizens from using non-native currencies to transact.

A widely accessible digital and decentralized currency whose price would be stable would offer a welcome alternative to citizens of countries where the system's

[14]https://data.worldbank.org/indicator/FP.CPI.TOTL.ZG?

monetary instability leads to restrictions on the control of their capital.

A currency dedicated to a cryptocurrency loan market

A promising use case for cryptocurrencies and the Blockchain is to serve as the infrastructure for a modern financial ecosystem by reducing intermediaries, fees and inaccuracies. However, for cryptocurrency-backed capital markets to emerge, price levels must remain relatively stable.

The issuance of Ether token-based loans on the Ethereum Blockchain is currently prohibitive on a large scale. This is because both the lender and the borrower take on significant currency risk by exposing themselves to fluctuations in the currency price with an Ether-based loan.

Having a stable currency is one of the primary goals of Central Banks. Being able to rely on a price and value for a given currency is the key to building reliable and sustainable businesses.

Price stability means that inflation is low enough and stable enough to not influence the economic decisions of households and businesses. With low and reasonably stable inflation, public opinion is not wasting time and resources trying to protect itself from this inflation. They can indeed invest with confidence that promotes growth in economic activity.

2.4.1 How the stablecoins work?

Currently, there are three approaches to developing a cryptocurrency with a stable price: secured through the support of a fiat currency, secured through the support of a cryptocurrency and through seigniorage actions.

Fiat-backed

This stablecoin implementation is clearly the simplest solution. Each unit of stablecoin is therefore backed by a corresponding unit of fiat currency, such as the US dollar.

The implementation mechanisms remain fairly simple. A trusted third party accepts deposits in US dollars (or any other fiat currency) and then issues one unit of stablecoin for every dollar deposited. To cash in a stablecoin unit, the third party sends a US dollar to the bearer and then destroys the stablecoin unit in question.

In this system, transparency on the part of the third party responsible for the safekeeping of deposits is essential as is trust in the third party responsible for the verification. If these two essential conditions are met, the system can be successful.

Crypto-backed

This approach will consist of supporting the stablecoin on a cryptocurrency rather than a fiat currency. Instead of having a 1 to 1 parity in fiat currency, we can have a greater than 1 to 1 ratio between the collateral cryptocurrency and the issuing units of a stablecoin backed by this cryptocurrency.

This method is implemented by relying on a Blockchain, such as Ethereum, which will act as a guarantee, this avoids the problem of the trusted third party present in supporting a fiat currency. The main problem with this implementation, however, is that the collateral cryptocurrency can be very volatile. To avoid potential significant price reductions, you need to hold a larger amount of collateral with a ratio that can be 2 to 1 or even more.

Seignorage

This third approach does not rely on a fiat currency or cryptocurrency support. This is the most complex approach, but potentially the most powerful for the ecosystem. To maintain a certain price level, a “Central Bank” will be created in charge of maintaining, through an algorithm, the money supply, increasing it when the price increases and decreasing it when the price falls.

As a general rule, seigniorage is based on the following system of rules. In the

event that the trading price exceeds $1 per unit, the "Central Bank", represented by a smart contract, will issue additional units in order to increase the supply until the price reaches $1. During this process, there is a collection of a certain amount of units representing the profits which here corresponds to seigniorage.

If the price falls below $1 per unit, the "Central Bank" will use its seigniorage profits to buy back the units. This will then reduce the supply and raise the price again. If the price remains below $1 per unit after the "Central Bank" has spent all the acquired amount on seigniorage, the "Central Bank" issues "seigniorage shares" promising future seigniorage to buyers in order to raise funds.

This system is clearly based on the future growth of stablecoin demand. When the "Central Bank" reaches a point where the price of the currency fluctuates below $1 per unit, that it no longer has seigniorage reserves, and that it is unable to sell "seigniorage shares" to raise funds, then traders will lose confidence in the prospects of stablecoin which risks bringing its price down irreparably.

It is therefore clear that the seigniorage quota system can only cope with a moderate level of pressure as its resilience capabilities are in the hands of seigniorage holders.

Conclusion

At the moment, stablecoins are a highly experimental field. However, a successful implementation of a stablecoin would have significant impacts for the crypto world and perhaps also for the ecosystem of the traditional financial world.

As interest in stablecoins continues to grow and as they begin to gain value, it will become important to fully understand and evaluate the systemic risks their mechanisms will induce without stopping just at their obvious benefits.

2.5 Tecnology

2.5.1 Distributed Ledger Technology

The term Blockchain is often confused with that of Distributed Ledger Technology (DLT) but they are not quite the same thing.

A DLT works like this: the ledger is stored on many servers (the so-called nodes) which communicate with each other to ensure that the registry is kept up to date. The process is really very simple, a node proposes a modification of a certain file and through a voting mechanism it will be decided whether to validate the modification or not. However, the right to vote will depend on the rules of that registry, sometimes all nodes can participate, other times only selected nodes will participate. Once the permission is given, the updated file overwrites the existing one and all nodes will receive the updated file.

The Blockchain has a very similar functioning but unlike a DLT it only allows you to add new data. This is an aspect that distinguishes it from traditional databases since it is not possible to remove existing data, any changes that are made remain in the history.

Another important difference is that in the Blockchain there is no hierarchy between nodes, each node has the same importance and, consequently, can add new data. Precisely for this reason it is said that the Blockchain is based on a Peer-to-Peer (P2P) technology, as there are not one or more central authorities that must authorize the addition of this data, each node can do it without asking anyone's consent. Even though each node has the permission to add new data it cannot do what it wants, every time a node wants to add new data, it is checked by the other nodes and, if the data does not meet certain requirements, it is discarded before being imprinted in the Blockchain.

So, the way it was built, the Blockchain is very difficult to block since all the nodes in the network should be turned off, as long as at least two nodes exist, the Blockchain will continue to function. This also ensures a lot of stability to

the network, as, should a node be hit by a natural disaster (earthquake, tsunami, etc ...), there will always be other nodes in other parts of the world that will be able to add data and keep an updated copy of the ledger.

In simple terms, the Blockchain is a type of Distributed Ledger Technology and its characteristics make it safe, immutable, incensurable and above all not hackable.

2.5.2 Blockchain

Distributed Ledger Technologies and, in particular, Blockchain technology, which rely on public key cryptography, enable the creation of a record unalterable and managed in an absolutely decentralized way, which allows new applications that were previously unthinkable, with undoubted potential.

Blockchain technology is described as a software protocol and distributed ledger for recording transactions, which can serve as a global computing substrate for processing any type of digitized business.

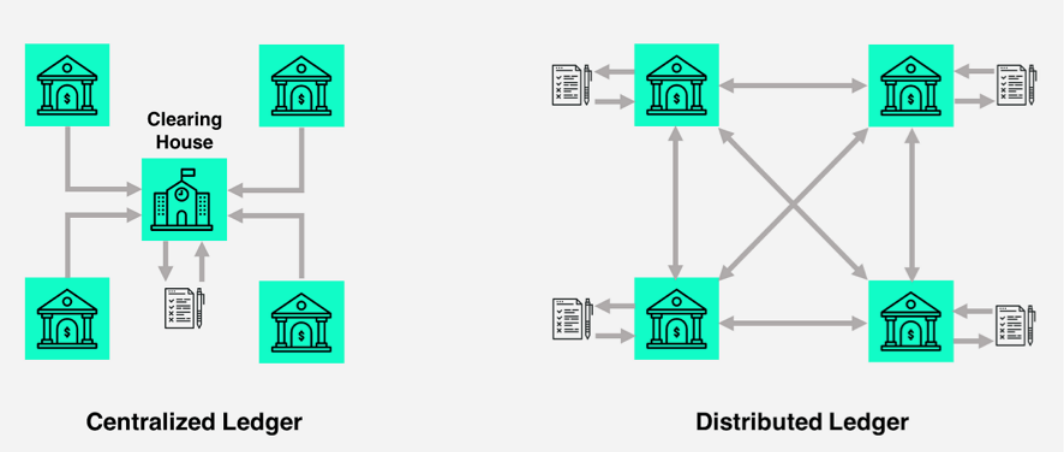
To understand better how a Blockchain works it can be imagined as a big interactive cloud shared document that anyone can view and in which independent administrators constantly check and update the book to confirm that each transaction is valid, resulting in the creation of a secure network in which each transaction can be independently confirmed as unique and valid without the intervention of a centralized intermediary, such as a bank, government or other institution.

From this point of view it is a system that is no longer based on trust between the parties, but on the functioning of the Blockchain system itself, which is based on mathematical techniques of consensus.

It should be noted that these systems use digital signature technologies very similar to those used for the electronic signature of documents, therefore it can be considered as an advanced electronic signature system.

From a more abstract point of view, Blockchain technology allows the updating

of all nodes of a network in a distributed IT environment which allows to confer a shared state of trust in a distributed system, i.e. when an action is recorded using these technologies, what actually happens is that this recording is done in a large number of different locations, rather than in one centralized location, so we can consider that recording to be true.



Source: Bit2me[15]

In short, this is a system in which we can write any information we want, using a specific node in the network. From that moment on, this information will be copied to all the remaining nodes of the network, so none of them will be able to delete this information unilaterally. Only with the competition of a large number of nodes could an insertion in the network in question be eliminated, in this way an insertion of information that has spread within the network is considered "true".

This does not mean, of course, that the information itself is true, but it is true that this information was written and not other different information. The same is true when using the advanced electronic signature based on an electronic certificate to authenticate a private document: the content of the document is attributable to the signer, regardless of whether the content is true or not. For example, when a false declaration is issued and signed, the document is authentic

[15]https://academy.bit2me.com/en/which-is-ledger-distributed-ledger/

because it is attributable to the signer, but its content is false. The same is essentially true with distributed recording technologies.

What really differentiates the two cases has to do with one of the most peculiar characteristics of the electronic document, and it is the possibility of making infinite identical copies, all with the conditions of the original and at the same time.

An example would be to write a contract in a PDF file and sign it electronically. The physical copy containing the signature would be original on paper and, given the impossibility of reproducing it, we will need at least two copies, each signed by both parties, to formalize the contract (which, for this reason, is signed "in duplicate"). Otherwise, in this type of electronic medium and PDF format, it is sufficient to sign a copy, which can be reproduced infinite times through a simple copy of the corresponding computer file.

The example just cited shows one of the benefits of electronically signing a document, but it also shows a good example of one of its limitations, which can be quickly realized, in fact it is not a useful mechanism for those cases in which the transfer of a value occurs through the delivery of a document.

Indeed, Distributed Ledger Technologies allow, for the first time in history, applications such as the creation of endorsements, thus facilitating the implementation of electronic titles of all kinds, or the effective and unalterable execution of unalterable legal and administrative acts, in particularly those in which transfers of assets or assignments of powers.

Until the advent of these technologies, the approach to the digitization of securities of all kinds consisted in the use of registering in a centralized register of holdings and their subsequent amendments. This has occurred in secondary markets, in money transfers and other payment transactions.

But it is not only in this area that applications of Distributed Ledger Technologies have been proposed, in fact this technology would allow the implementation of authenticity guarantees in central databases, preventing undetectable modifi-

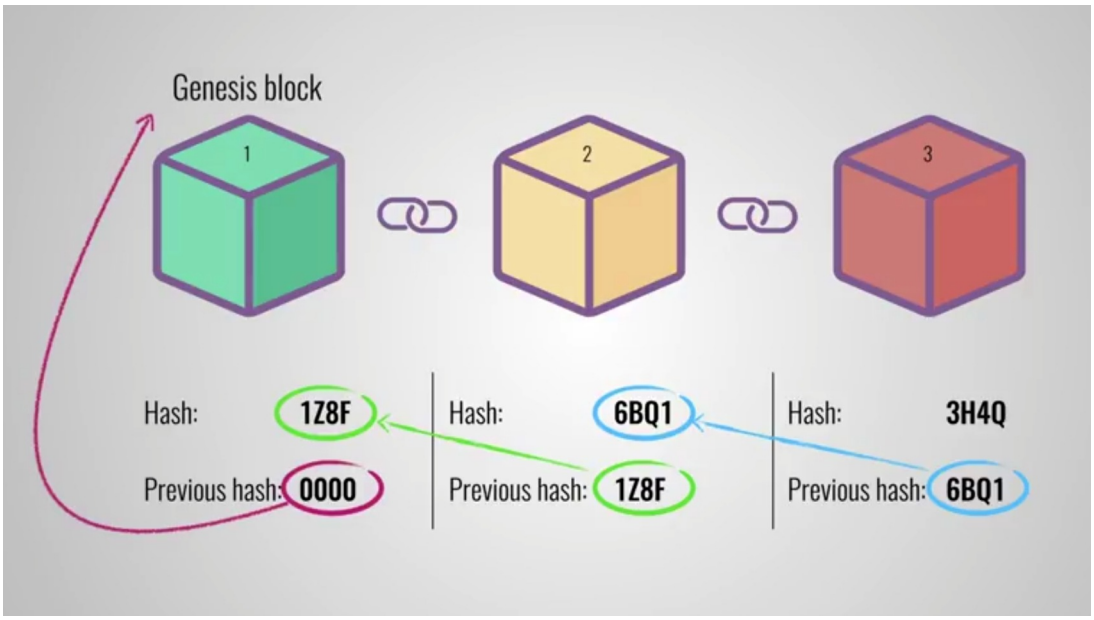
cation of the records that contain them.

Finally, it is absolutely essential to refer to the possibility of implementing, through Distributed Ledger Technologies, traceability systems for all kinds of objects, both in the electronic and physical world, using the tokenization technique, especially when tokens represent properties.

It should be noted, therefore, that due to the application requirements of data protection regulations, usually all uses of Blockchain systems imply that the documents or writings, or data to be transmitted or protected with this technology are outside the Blockchain. That is, what is recorded in the Blockchain is not the data itself (which is outside the system), but only its cryptographic summary. In this way, it can be ensured that the document or data have not been modified, but without advertising its content and with the possibility of complying with data protection regulations, in particular the right to erasure.

2.5.3 How the Bitcoin Blockchain works?

To better understand the functioning of the Blockchain and why it is so secure, we can start from the name which is formed by two words Block and Chain. The Blockchain is just that, a set of blocks held together by a chain that ensures their chronological order.



Source: What is Blockchain Technology?[16]

These blocks are nothing more than files containing all the transactions that are made by users. When a person sends a Bitcoin to another person, many mistakenly think that the Bitcoin is physically inserted into the block and sent, but this is not the case. Only the request, by the person who is sending, to transfer the ownership of that Bitcoin to the receiving person is inserted in the block.

Example: Alice has to sell a property to Bob. Alice will not put the wheels under the property to take it to Bob, but they will certainly go to a notary who will certify, through a signature, the transfer of ownership.

When a person sends Bitcoin the same thing happens, the name of the owner of those Bitcoin is changed. Therefore, there is a need for someone to sign and

[16]https://www.umeandit.co/2020/09/what-is-Blockchain-technology.html

certify the transfer of ownership of the Bitcoin. In the Bitcoin Blockchain, the confirmation of transactions is carried out by the miners who, approximately every 10 minutes, sign the block and add it to the chain of previous blocks, making the transactions irrevocable.

There are various ways in which these blocks can be added, in the Bitcoin Blockchain this is done through the Proof-of-Work. This means that miners to sign a block and add it to the Blockchain have to solve a math puzzle to prove they have done the job so they can be rewarded.

The puzzle consists in finding a number called nonce which, when inserted into a mathematical expression, gives us a precise result. The term nonce is a combination of two words, "n" meaning number and "once". Therefore, nonce means using a number only once. The nonce is an arbitrary 32-bit random number that can be between 0 and 2^{32} (i.e. 4,294,967.29).

To understand where to insert the nonce within the mathematical expression, it is good to first understand what a hash is. A hash is simply a large base number 16. In everyday life, a base 10 number system is used, i.e. a number system consisting of 10 digits ranging from 0 to 9. There are bases other than base 10, for example a system base 2 numeric includes only two digits: 0 and 1. A hash is a base 16 number that is simply stretched using the first 6 letters of the alphabet to reach 16 digits.

Base	Numerary system	Digits
2	Binary	0, 1
3	Ternary	0, 1, 2
4	Quaternary	0, 1, 2, 3
10	Decimal	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
16	Hexadecimal	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f

Source: personal

To calculate a hash you need to use a hash function. There are many different hash functions, the one used by Bitcoin is called SHA-256 and produces an output

of the size of 256 bits that is 64 digits. A hash can be obtained by inserting any data (text, photos, files, etc ...) within a hash function, the output that will be generated will always be of fixed length.

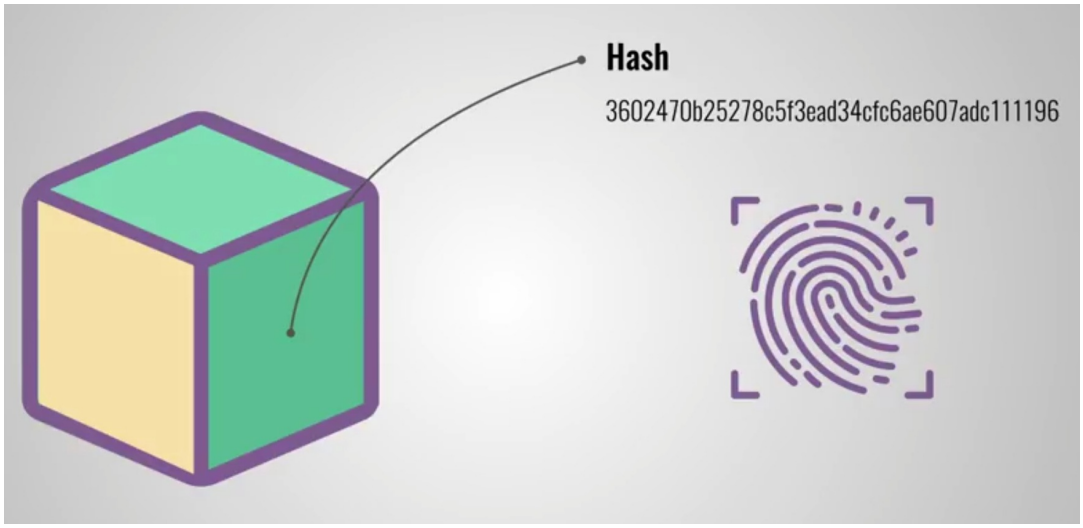
Example: Using an online hash function[17] can help clarify the concept. By inserting a text such as "Luiss Guido Carli" within the function, the following string will come out:

7e44c57f8df39ce8c2485fb5adbe2be72d625cd45f2994f33b9e7873e4658aef

If a letter in the input text is changed, even if it is only uppercase or lowercase, or a space, the string changes completely. Example:

- luiss guido carli:
  a4b8db1d19596f5997c2cb571b8fa55f31b2ddebae1d5b3ea9e5e3dbff86317e
- luissguidocarli:
  49e401a9c47dcf610822c57eb4ea11831f8123c89d5dea83e4213e8cb1a1b814

This ensures that each hash has a unique input associated with it.



Source: What is Blockchain Technology?[18]

[17]For example https://emn178.github.io/online-tools/sha256.html

[18]https://www.umeandit.co/2020/09/what-is-Blockchain-technology.html

It is important to understand a difference: the SHA-256 function is not a cryptographic function but a hash function. The key difference is that while the cryptographic function is a two-way function (we can decrypt the data) the hash function is a one-way function: through a hash function we can calculate the hash, but having the hash is difficult (and mathematically impossible) to obtain the starting input.

The hash plays a fundamental role within the Blockchain and, precisely because a single output is associated with an input, the hash is used to identify transactions or blocks. It is also used in conjunction with the nonce to bind the blocks in chronological order via the math puzzle set out above. Each block consists of:

1. hash of the previous block;
2. the timestamp;
3. the root of the Merkle tree of all transactions included in the block;
4. the nonce;
5. the difficulty of the block.

The mathematical puzzle consists in finding the only unknown, that is the nonce (4), which gives us as a result the hash of the block that we want to confirm with that difficulty (5).

Example: in the classroom the teacher writes a problem on the blackboard that students have to solve. The first student who solves it wins a prize. The problem is the following:

$$10 + ? \; = \; 17$$

The first student who finds the missing number (i.e. the nonce) will win the prize. Before receiving the award, however, he will have to show the solution to the rest of the class who will verify its accuracy. If he has found the number 7 and his classmates agree, he will be able to collect the prize.

The nonce is therefore the number that inserted in a hash function together with the inputs of points 1, 2 and 3 gives us the hash that we need to find (point 5). It is important to note that the timestamp changes every second, so miners will have to find the correct nonce within that time frame otherwise the nonce will change and they will have to start over.

The hash of a block will be different for each miner because it is extremely unlikely that two miners have the same Merkle root. Therefore, it is not a race to solve the puzzle, rather, it is a lottery system. But, of course, a miner is likely to get luckier depending on his hashpower.

So actually miners don't have to find a specific hash, they are only asked to find a hash with certain requirements. The hash of a block always starts with 0, and when a miner finds the nonce that, together with the other inputs, returns a hash that starts with a 0, it will show the result to the other miners and, if correct, will win the prize.

Example: Let's go back to the example above, the teacher proposes the same problem but this time he wants the result to be greater than 17

$$10 + ? > 17$$

The first to try, therefore, to enter any number greater than 7 will win the prize as it will be correct. This is to say that the nonce is not unique but there are several, the first student who finds one will win the prize.

This reward is called "coinbase" and is always the first transaction in the block that transfers completely new Bitcoin, plus the transaction fees that users pay, to the wallet of the miner who signs it.

Satoshi Nakamoto in the Bitcoin protocol established that the Bitcoin that are created for the miners must halve every 210,000 blocks (about 4 years) and this event is called "halving". The process of halving the created Bitcoin ensures that no more than 21 million Bitcoin can ever exist.

To ensure that the average between one block and another is 10 minutes,

the difficulty in finding the nonce is periodically increased or decreased. The difficulty lies in the quantity of initial 0 of the block hash. Each time a 0 is added or subtracted, the calculation difficulty required to find the hash increases or decreases.

Increasing the initial 0 decreases the correct nonce to find and therefore the difficulty increases, vice versa decreasing the 0 decreases the difficulty because the correct nonce increases and it is easier to find them.

Chapter 3

Regulation

"Nothing in life is to be feared, it is only to be understood. Now is the time to understand more so we can fear less."

– Marie Curie[1]

3.1 An uncertain regulatory framework

3.1.1 Looking for a legal nature

Due to the spread of cryptocurrencies in recent years, many questions have emerged related to their use and, above all, their legal nature. In an attempt to outline a legal framework in which to insert cryptocurrencies, it is necessary to start from the concept of currency. It is not at all as simple as one might think since, even if it can be sent and received like a real coin, part of the doctrine argues that cryptocurrencies cannot be included in the concept of money, this for two reasons[2]:

[1]Marie Curie (Warsaw, 7 November 1867 - Passy, 4 July 1934), was a French naturalized Polish physicist and chemist. She took the Nobel Prize in Physics in 1903 and the Nobel Prize in Chemistry in 1911.

[2]See Bocchini Roberto 2017

- Cryptocurrencies are not recognized by any state and a merchant, therefore, could refuse to accept this method of payment, without contravening the precept set by art. 693 of the Italian Criminal Code, which, with reference to the Criminal Law, provides for and punishes the refusal of coins having legal tender;

- It does not fulfill the fundamental roles associated with a currency: it cannot be used as a store of value as the price is susceptible to great volatility over time, it is not always accepted as a medium of exchange and cannot be used as a unit of account due to the uncertainty of the foreign exchange market.

A different school of thought argues that even if cryptocurrencies cannot always perform the function of a store of value, they could, instead, fulfill the other two functions of monetary theory, i.e. medium of exchange and unit of account.

Continuing to deepen the legal nature of Bitcoin, one might be tempted to assimilate it to a type of electronic money, a case defined by art. 2 of Directive no. 2009/110/EC on electronic money institutions (EMD2), implemented in Italy with the legislative decree 16 April 2012, n. 45, such as "the monetary value stored electronically, including magnetic storage, represented by a credit towards the issuer that is issued to carry out payment transactions (...) and that is accepted by natural and legal persons other than issuer". Bitcoin, in fact, takes the form of a dematerialized currency, the value of which, stored electronically, is accepted by natural or legal persons other than the issuer.

Although a conclusion has not yet been reached, due to the growing spread of cryptocurrencies, the importance of this answer becomes increasingly important for their legal qualification. Furthermore, it is very important to find a legal framework for them, as many jurists and economists have highlighted the systemic problems that unregulated means of payment could bring to the entire financial system.

There are several ways to find a legal nature[3]:

- **Legal asset ex art. 810 of the Italian civil code**: cryptocurrencies could be qualified as a legal asset that can be subject to rights and therefore be worthy of protection. It is not, however, that simple. The sorting as it is structured is still very much linked to the notion of material asset and this cannot be applied to cryptocurrencies due to their intrinsic nature;
- **IT document**: the thesis has been proposed for which cryptocurrencies can be traced back to an IT document, that is the computerized representation of legally relevant deeds, facts or data, as defined in Italian system by the legislative decree 7 March 2005, n. 82, of the Digital Administration Code. As an IT document, it would give the holder legitimacy to use them for economic purposes;
- **Financial instrument**: as some cryptocurrencies, such as Bitcoin, have shown a considerable increase in value over time. It is therefore legitimate to ask whether Bitcoin can be included in the category of "financial products", which in the Italian legal system are identified by art. 1, co. 1, lett. u), TUF, such as "financial instruments and any other form of investment of a financial nature". But even here there is no clear answer as the definition of a financial instrument contained in Legislative Decree no. 58/1998 (Testo Unico della Finanza) in art. 1-bis, 2nd paragraph does not include the means of payment. The so-called virtual currencies therefore remain outside the scope of application not only of the TUF, but are also excluded from the application of the MiFI system, envisaged by Directive 2004/39/EC relating to markets in financial instruments. If it is considered as a financial product, however, prudential and supervisory regulations for individuals who do not use cryptocurrencies for private purposes can be found. The Communication from the Bank of Italy, in fact, reminds that "In Italy, the purchase, use and

[3]See Bocchini Roberto 2017

acceptance of virtual currencies in payment must be considered legitimate activities by the state; the parties are free to undertake to pay sums even if not expressed in legal tender currencies. However, attention is drawn to the fact that the activities of issuing virtual currency, converting legal money into virtual currencies and vice versa and managing the related operating schemes could instead result in the violation of regulatory provisions in the national law, criminally sanctioned, which reserve the exercise of the related activity only to legitimate subjects (articles 130, 131 TUB for banking and savings collection activities; article 131-ter TUB for the provision of payment services; art. 166 TUF, for the provision of investment services)"[4];

- **Payment method**: thanks to their ease of transfer, cryptocurrencies could fall within the scope of application of Directive 2007/64/EC, relating to payment services and implemented in Italy with Legislative Decree no. 27 January 2010. 11 as "any customized device and/or set of procedures agreed between the user and the payment service provider and which the payment service user uses to issue a payment order". As mentioned above, the only objection that can be made to this thesis is not to be recognized as legal tender by the state.

3.1.2 Risks related to the absence of legislative protections

Obviously, as there is no regulation, there are some risks involved:

- **Lack of information**: without a law that obliges transparency within the sector, it could be difficult for an economic agent to find reliable information and, therefore, fully understand the risks;
- **Absence of legal protections**: unlike the purchase, exchange and use

[4]See Banca d'Italia 2015, p. 2

of fiat currencies, similar transactions in cryptocurrencies are not legally protected. Due to this deficiency, the buying and selling of cryptocurrencies could lead to unclear costs and commissions that would be difficult to prove, precisely, due to the lack of disclosure obligations;

- **Acceptance**: not being a legal currency, cryptocurrencies are not universally accepted but are exchanged through agreements, this means that there is no certainty of being able to use them;
- **Absence of forms of control and supervision**: for now, the issuance and management of virtual currencies is not subject to any regulation by any Italian or European authority. This situation should change with the MiCA proposal that the European Union released at the end of 2020;
- **Absence of forms of deposit protection or guarantee**: Italian banks are required to join the Interbank Deposit Protection Fund, which guarantees depositors a refund of up to 100,000 euros. This is an important guarantee for customers, as it allows them to protect their savings in the event of insolvency situations with banks. In the case of cryptocurrencies, this legislation does not exist, so platforms offering deposit and withdrawal services are not required to cover losses incurred in the event of fraudulent conduct, bankruptcy or cessation of business.

3.1.3 Exchange

Cryptocurrencies have become popular in another layer of the web world, the "Deep web", to trade on sites not regulated by conventional internet policies. Although they became popular thanks to the anonymity they guaranteed, gradually these currencies have migrated to other spheres of the conventional web where their acquisition and exchange is possible.

Millions of investors pay their attention to the movement of cryptocurrencies and invest in them through exchanges. Exchanges are online platforms and rep-

resent a key operator in this new market where it is possible to buy and sell cryptocurrencies.

Once the cryptocurrencies are placed on the market, the exchanges perform the important task of bringing together the supply and demand of the secondary market. The exchanges in addition to offering the cryptocurrency trading service also offer the custody service, thus acting like a real bank.

Exchanges, however, are not all the same as there are two types: centralized and decentralized. Centralized exchanges are by far the majority where trading takes place by giving orders to the platform, consequently, in these platforms the cryptocurrency custody service is necessarily entrusted to exchanges. In decentralized exchenges, on the other hand, the platform is only the place where users carry out transactions with each other without the need for intermediation.

The market is growing really fast, it is estimated that there are more than 200 platforms in the world, with a daily trading volume roughly quantified at 10-15 billion dollars[5].

Like many other things in this industry, deposits are also not regulated. Pending future regulation, it is possible to analyze the relationship between user and exchange to identify an applicable discipline with the current regulatory framework.

A recent sentence of the Court of Florence, bankruptcy section, has had the opportunity to analyze the issue[6]. The Court found itself to ascertain the existence of the conditions for the declaration of bankruptcy by an exchange which, due to a cyber attack, cryptocurrencies deposited by users were stolen. After analyzing the case, the Court of Florence came to the conclusion that the relationship between the user and the exchange was, pursuant to art. 1782 of the Italian Civil Code, of an irregular deposit according to which "If the deposit concerns a quantity of money or other fungible things, with the right for the depositary to use

[5]See Caloni Andrea 2020

[6]Ibidem

it, the latter acquires the property and is required to return as many of the same species and quality".

It is interesting to note that the user does not physically deliver the cryptocurrency to the exchange but only delivers the private keys that will allow the platform to use those funds. Well, the jurisprudence has had the opportunity to establish that the delivery of the car keys to the hotel driver integrate the custody not only of the keys themselves, but of the goods to which they allow access.

It seems clear that the differences between exchanges and banks are not so many. A brief study is noteworthy after the Court of Florence has qualified the deposit of cryptocurrencies as an irregular deposit.

Banking is defined by Article 10 of the Testo Unico Bancario (TUB) on two related activities carried out in the form of a business: the collection of savings and the exercise of credit. The collection of savings, on the other hand, is defined by Article 11 of the TUB as "the acquisition of funds with a repayment obligation, both in the form of deposits and in another form".

With regard to the collection of savings, the law reports the term "funds" which in the legal context is interpreted as "money", but since, as seen above, cryptocurrencies are not considered money, exchanges cannot be considered banks, also because they do not exercise credit.

3.1.4 Initial Coin Offering (ICO)

The Blockchain is a technology that is based on the so-called Distributed Ledger Technologies (DLT), over time the Blockchain has evolved, first focused on the exchange of cryptocurrencies, now it is considered a suitable infrastructure to pursue further and specific negotiation purposes through distributed software, also known as smart contracts. Smart contracts are protocols that automate certain processes without the need for a third party to intervene.

Thanks to this evolution it was possible to create the first crowfunding through tokens. The doctrine therefore defines crowdfunding as "a collective effort by

people who network and pool their money together, usually via the Internet, in order to invest in and support efforts initiated by other people or organizations"[7].

An initial coin offering or ICO is a funding mechanism that allows a project or company to raise capital in highly liquid cryptocurrencies, such as Bitcoin or Ethereum, and fiat coins, such as the dollar or euro, through the sale of a new cryptocurrency in a completely decentralized model based on Peer-to-Peer mechanisms. It is a use case of crowdfunding, which is a method of financing a project or company by raising small amounts of money from a large number of people, typically on the internet.

In an ICO, the money-seeking project issues a certain amount of cryptocurrencies or tokens on an existing blockchain platform, such as Ethereum or Avalanche, and delivers them to investors in exchange for cryptocurrencies or, in rare cases, fiat money such as the dollar. or the euro. The entire operation is carried out using smart contracts that automate the token distribution process based on the requirements established by the ICO holder. Therefore, when the payment condition is met, the contract automatically assigns and sends the amount of the corresponding tokens to the investor's wallet.

The company receives cryptocurrencies, highly liquid, and in return the investor receives cryptographic assets that can be used on the platform and can be exchanged with others.

Early ICOs, like that of Ethereum, consisted of a single phase or period of execution and offered a bonus to investors for their early participation, accessible to anyone. Newer ICOs are usually executed in two stages, a first pre-ICO call, pre-sale or private placement, the goal of which is to raise as much money as possible from private investors during this non-public period, by offering them a discount or bonus, greater of those who participate in the second phase or ICO, for being willing to take the risk of giving a large sum of money to an immature project.

[7]See Gregori Gitti 2020

The platform most used to carry out ICOs is the Ethereum blockchain, for two fundamental reasons: the ease of creating compatible ERC20 tokens and the automation of the token distribution process through smart contracts supported by this blockchain.

The ERC20 protocol is a standard method that ensures interoperability between tokens. If all tokens created on the Ethereum network use the same standard, those crypto assets will be easily interchangeable and can work immediately with decentralized applications (dApps) that use the ERC20 standard. What makes a token "standardized" is that it uses a certain set of functions, which make it easier to integrate it into projects with less fear of errors. If different tokens behave similarly, calling the same functions the same way.

Differences between an IPO and an ICO

The Initial Coin Offering has elements of analogy with the Initial Public Offering (IPO), however ICOs are characterized by some specificities with respect to IPOs. An initial public offering or IPO is the process of selling a portion of a company's shares to the public for the first time in the capital market, its buyers becoming shareholders of the company. Conversely, the ICO sells a cryptoasset or utility token that does not represent the equity of the company or project, but allows its owner to interact on the platform to be launched in the way that creators dispose (for example, by activating an asset digital in a game) and exchange it in the market for other crypto assets or fiat money. Additionally, the token can represent an ownership or royalty right on the benefits of a project or company, as agreed by the issuer.

The main features of ICOs as a source of financing for projects and startups are, among others[8]:

- **Global**: Using the Internet as a means of access to mass sales, anyone anywhere in the world can invest without limitations beyond those set out in the ICO;
- **Ease**: Investors can trade directly on the platform without the need for brokers or brokers as intermediaries, at any time during the ICO;
- **Unlimited investment**: Investors can make large or small purchases of the offered tokens, limited only by the conditions that the owners of the ICO impose. Large investors can even buy pre-ICO, thus guaranteeing better discounts or promotions;
- **Little regulation**: Another big difference between ICO and IPO is that there is little regulation in the world, so the protection of the investing public is minimal or nonexistent. The IPO regulation obliges the promoters of the IPO to disclose, initially and periodically, a series of relevant information on the business, its commercial operations, financial situation, operating results, risk factors and management.

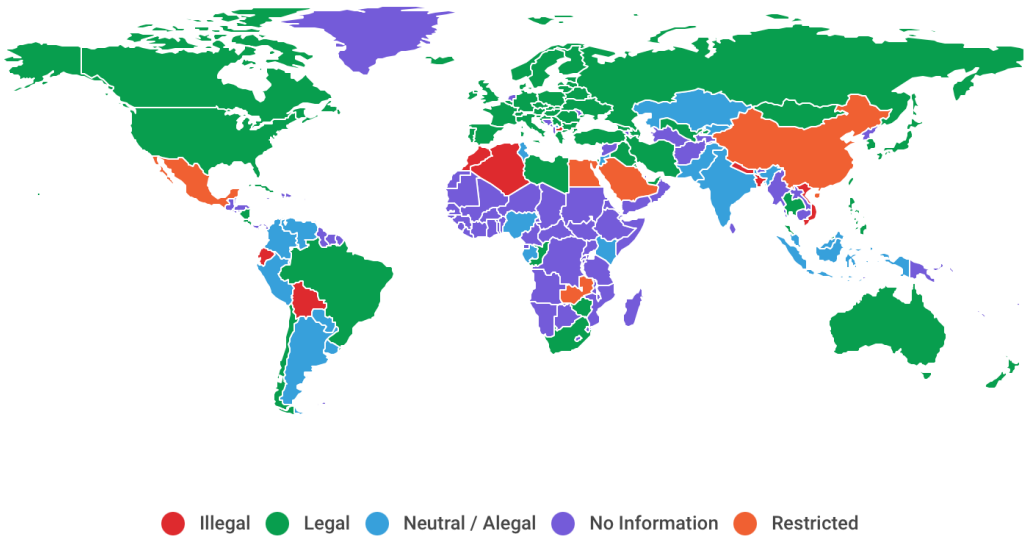
The current legal vagueness reinforces the crypto-skeptical climate of the general public, with investors not knowing what legal status to give to crypto-assets that are not considered "currencies" in the eyes of the law. It is for this reason that with the new MiCA regulatory proposal, the European Union now proposes to provide a framework for ICOs.

[8]See Gregori Gitti 2020

3.2 Kind of approaches

Unfortunately, cryptocurrencies are not always used for legal purposes, in fact, today they are the most efficient tool for illegal transactions. Cryptocurrencies are more efficient for recycling even than cash due to the great ease and speed of movement that cash cannot possibly have in the face of an almost comparable level of anonymity.

Now, as cryptocurrencies can be used for the commission of crimes, countries to solve this new problem have taken different positions that can be grouped in three different ways of dealing with: inaction, prohibition and regulation.



Source: Coin Dance[9]

3.2.1 Inaction

There is currently no international consensus on how cryptocurrencies should be regulated. Most nations have not developed regulations governing the uses of cryptocurrencies as it is still a challenge to understand all the edges this new technology encompasses.

[9]https://coin.dance/poli

A large number of countries allow the use of cryptocurrencies, but do not have a regulatory body or supervisory bodies that oversee the industries that provide services related to them. Some countries even stated that they did not feel it necessary to regulate cryptocurrencies, as in the case of Finland, which at the time stated, through its Central Bank, the following[10]:

> *"Bitcoin is a monopoly managed by a protocol, which prevents the negative aspects of traditional monopolies, such as the abuse of power and the manipulation of prices for the individual advantage [...] There is no need to regulate it because as a system it is bound to the protocol as it is, and the transaction fees charged to the user are determined by the users regardless of the effort of the miner."*

As time goes by, nations are beginning to understand the impact, both positive and negative, of cryptocurrencies. For this reason, more and more countries abandoning their position of inaction and are now focused on finding solutions to the challenges of this new technology.

The position of inertia is not adequate to solve the problematic effects of cryptocurrencies as the lack of regulation makes harmful cryptocurrency practices thrive and does not provide the legal certainty necessary for the growth of the industry.

The current market seeks clear and precise regulation on permitted uses of cryptocurrencies and how users' rights will be protected against this new technology. At the same time, the market seeks that these regulations are flexible enough not to limit technological progress and innovation.

3.2.2 Prohibition

The Coin Dance website has published a list of the legal status of Bitcoin in all countries of the world. This report details the countries where Bitcoin and

[10]See Huberman Gur, Leshno Jacob D., Moallemi Ciamac 2017, p. 36

other cryptocurrencies are considered illegal, these are: Bolivia, Algeria, Nepal, Bangladesh, Vietnam, Macedonia, Afghanistan, Kyrgyzstan, Qatar and Vanuatu[11].

Of all these countries, only Bangladesh has established sanctions for people carrying out cryptocurrency transactions with penalties of up to 12 years in prison[12].

The normal reaction when disruptive technology emerges, especially one that has potentially harmful uses, is to view it with skepticism and even fear. Nations are understandably cautious when it comes to cryptocurrencies or other virtual currencies.

However, the prohibitive measures that the aforementioned countries have taken are questionable at best. Punishing the use of cryptocurrencies with prison terms is a violation of the fundamental principles of criminal law.

It should be remembered that criminal law is a minimum intervention, meaning that the application of a criminal law must be an ultimatum, applied only in cases of extreme gravity in order to safeguard protected legal assets. Not all uses of cryptocurrencies violate legal rights, therefore, sanctioning these uses indiscriminately violates people's rights.

It should also be emphasized that despite its possible criminal uses, cryptocurrency technology offers a number of advantages and benefits that cannot be ignored. This technology is not only having an impact in the financial sector but in sectors such as health services, data storage and distribution, electoral process improvement, land registry and many others[13].

These nations must realize that their banning policies directed at this technology are useless as it is impossible to permanently shut down the Bitcoin system in the same way that it is impossible to do the same with the internet.

Most of the nations that have banned Bitcoin are countries with precarious

[11]https://coin.dance/poli

[12]See The Law Library of Congress 2018, p. 98

[13]See Gazdecki Andrew 2018

economies that could very well use this technology to create a new source of employment for thousands of people.

If cryptocurrencies and Blockchain become the new technological revolution, similar to what happened with the internet, prohibiting their use and not developing legislation that favors their incorporation into the market will entail a great disadvantage for these countries, which will have a tough battle against the rest of the nations that were receptive to cryptocurrencies. On the contrary, many of the richest nations in the world (Switzerland, Japan, Singapore) are competing to become the center of the crypto world[14].

Some countries changed their initial stance on Bitcoin as they realized that the ban was not a viable option. Germany, Estonia and Colombia were countries that a few years ago spoke out against cryptocurrencies and are now looking for ways to implement them in their financial systems and regulate them in regulatory bodies.

The Bank of the Republic of Colombia declared in 2014, through the Financial Superintendency, to reject Bitcoin since the Colombian peso is the only legal tender currency authorized by the government. In September 2018, the same entity convened a group of experts to begin drafting a bill to regulate crypto assets[15].

3.2.3 Regulation

To date, Malta and the United States stand out as the countries with the largest production of legislation aimed at regulating cryptocurrencies[16]. However, the approach these two countries take when regulating cryptocurrencies is very different.

On the one hand, Malta has created comprehensive and specialized legislation

[14]Muth Tomoko 2021

[15]See Lanz Jose Antonio 2019

[16]See Ciphertrace Cryptocurrency Intelligence 2018

for cryptocurrencies, on the other hand, the US has not created special laws for regulating cryptocurrencies, but has sought to integrate cryptocurrencies into their current laws.

Malta

Malta is known around the world as the Blockchain island among cryptocurrency enthusiasts as this nation has stood out for being very receptive to innovative technology initiatives and for providing many facilities for cryptocurrency businesses to thrive. Malta was the first country in the world to pass comprehensive legislation for cryptocurrencies and Blockchain technology.

In November 2018, the law on virtual financial assets [17], the law on agreements and services in innovative technologies[18] and the law of the Authority for digital innovation[19] came into force.

Its Virtual Financial Assets Act is designed for the purpose of regulating ICOs. This law governs ICOs much like IPOs. The common practice of how the laws have regulated IPOs is to require companies making the offer on the stock exchange to submit a prospectus. The prospectus is a paper whose main function is to provide detailed information about the company such as the name, the company name and the company name of the issuer, the domicile, the risk assessment, the subscribed capital, the amount and the type of securities to be issued, etc. In the case of ICOs, the equivalent of the prospectus is a white paper, which performs virtually the same functions.

What Malta has done by implementing these laws is to create a kind of stock market for crypto assets with one entity regulating all aspects of that market. This was done through the Digital Innovation Authority Act, which created the Malta Digital Innovation Authority (MDIA), an autonomous body that is the

[17]Initial Virtual Financial Asset Offerings and Virtual Financial Assets Act.

[18]Innovative Technology Arrangments and Services Act.

[19]Digital Innovation Authority Act.

top regulator for this new cryptocurrency market.

In this way, ICOs are registered in the virtual registry of the MDIA and this body analyzes the white papers of those ICOs and assigns them a risk rating [20]. This assessment helps investors get an idea of the compliance capability of ICOs and the risk of investing in these companies. This greatly reduces the risk of fraudulent ICOs. But the MDIA will not just regulate ICOs, it will also take care of issuing operating licenses for any type of business that wants to transact with cryptocurrencies, this includes exchanges, miners and other cryptocurrency service providers[21].

Malta, being part of the European Union, must comply with the directives that the Union issues on the fight against money laundering and the financing of terrorism AML/CFT[22]. The directive of the European Union to combat money laundering has established a series of guides for the implementation of an effective AML/CFT regime regarding cryptocurrencies.

Malta to comply with these regulations has created a virtual register of the MDIA which is linked to the Maltese Financial Intelligence Unit, in this way it is expected to have an effective register of companies that manage services related to cryptocurrencies and it will be possible to give better monitoring of cryptocurrency transactions.

The MDIA also requires all companies wishing to manage cryptocurrency-related services to implement AML/CFT controls, aka KYC[23] policies, to include cryptocurrency service companies as subjects required to report suspicious transactions to the Financial intelligence unit, and other additional measures

Maltese legislation in relation to cryptocurrencies is seen as the most comprehensive legislative body currently in existence regarding the regulation of this

[20]See Malta 2018, art. 4

[21]See Malta 2018, art. 6

[22]Anti-Money Laundering/Combating the Financing of Terrorism.

[23]Know Your Costumer.

new technology. These comprehensive regulatory bodies regulate cryptocurrency services from various areas of law such as intellectual property, competition, contractual, criminal, etc...[24].

However, Malta's reputation is in question as it has been the subject of money laundering investigations by the European Union Parliament in recent years[25].

Despite this, the Basel Anti-Money Laundering Index Report, which measures the risk of money laundering and terrorist financing, ranked Malta 132 out of 149 countries evaluated. This means that Malta is among the 11% of countries with the lowest risk of money laundering[26].

United States

The United States was the first country in the world to establish specific regulation for cryptocurrencies through BitLicense. In 2014, the US Department of Financial Services of the New York State issued regulations for companies that do business with cryptocurrencies or any virtual currency[27].

The BitLicense establishes that all the activities that fall into the category of Virtual Currency Business Activity (VCBA) are subject to the regulations established by the BitLicense and require an operating permit in order to carry out their economic functions. Davis Polk[28] explains that the requirements BitLicense sets for VCBA companies are as follows:

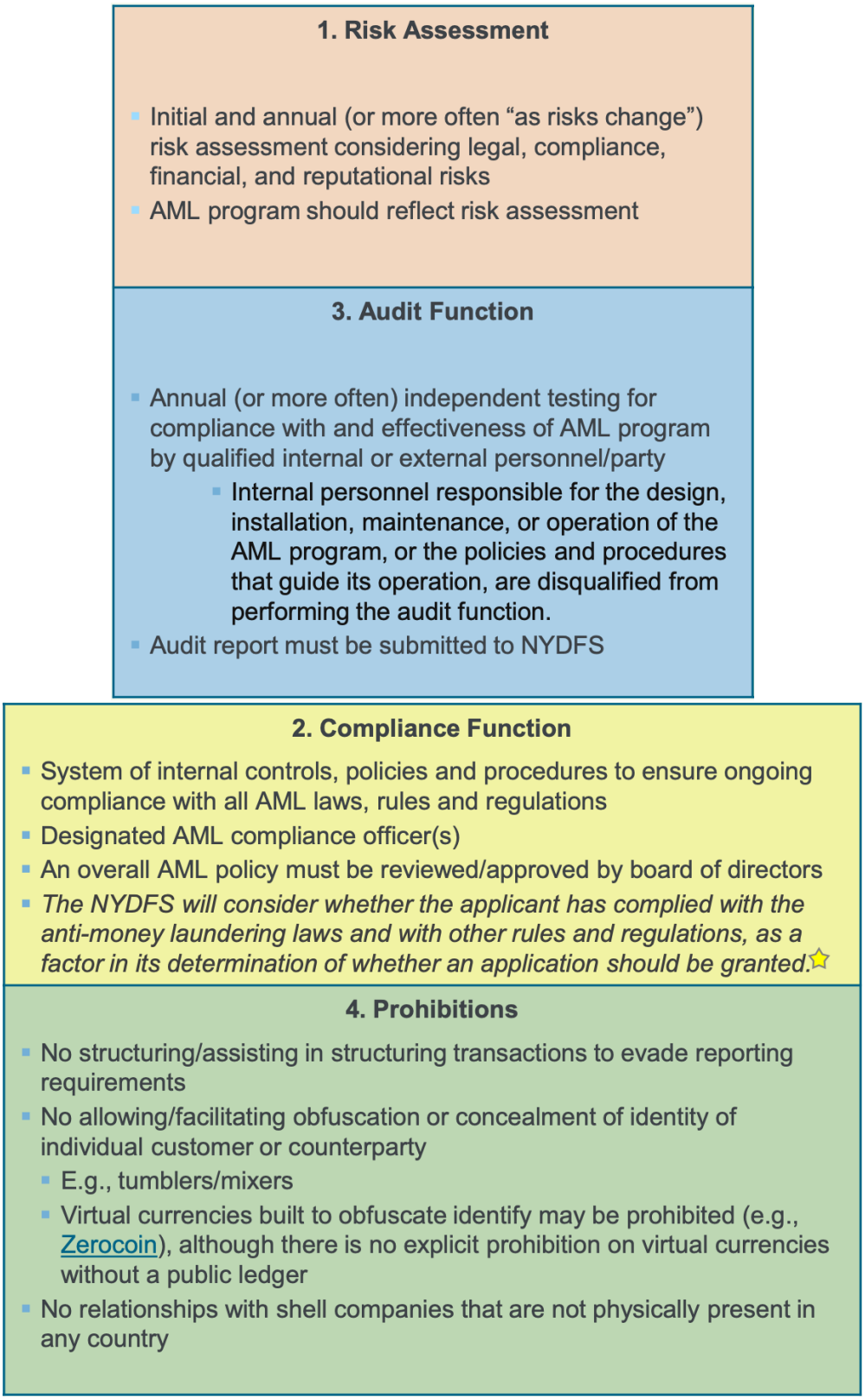
[24]See Wolfson Rachel 2018

[25]See Pronina Lyubov 2018

[26]See Basel Institute on Governance 2016, p. 3

[27]See Polk Davis 2015, p. 3

[28]Davis Polk & Wardwell, better known as Davis Polk, is an American international law firm, among the top thirty in the world by turnover.


1. Risk Assessment
Initial and annual (or more often "as risks change") risk assessment considering legal, compliance, financial, and reputational risks
AML program should reflect risk assessment
3. Audit Function
Annual (or more often) independent testing for compliance with and effectiveness of AML program by qualified internal or external personnel/party
Internal personnel responsible for the design, installation, maintenance, or operation of the AML program, or the policies and procedures that guide its operation, are disqualified from performing the audit function.
Audit report must be submitted to NYDFS
2. Compliance Function
System of internal controls, policies and procedures to ensure ongoing compliance with all AML laws, rules and regulations
Designated AML compliance officer(s)
An overall AML policy must be reviewed/approved by board of directors
The NYDFS will consider whether the applicant has complied with the anti-money laundering laws and with other rules and regulations, as a factor in its determination of whether an application should be granted.
4. Prohibitions
No structuring/assisting in structuring transactions to evade reporting requirements
No allowing/facilitating obfuscation or concealment of identity of individual customer or counterparty
E.g., tumblers/mixers
Virtual currencies built to obfuscate identify may be prohibited (e.g., Zerocoin), although there is no explicit prohibition on virtual currencies without a public ledger
No relationships with shell companies that are not physically present in any country

5. Records

- Must maintain detailed records for at least **7 years** including: the identity and physical addresses of **the licensee's customers/ account holders and, to the extent practicable, any other parties to the transaction**; the transaction amount or value (including denomination(s)); date(s) transaction was initiated/completed; description of the transaction; and method of payment*

7. OFAC Compliance

- Customers must be checked against the Specially Designated Nationals ("**SDN**") list maintained by OFAC
- Risk-based policies, procedures and practices to ensure compliance with OFAC regulations "to the maximum extent possible"

6. Reports

- Notify NYDFS within 24 hours of transactions/ series of virtual currency to virtual currency transactions by a person that exceed $10,000 in value in one day (a.k.a., Currency Transaction Reports or CTRs), unless the transactions are subject to federal CTR reporting requirements ☆
- SARs must be filed within 30 days if licensee is not subject to federal SAR filing requirements ☆

8. Customer Identification Program

- Reasonably identify/verify customer's identity, including name and physical address, when either customer opens an account or licensee establishes service relationship with customer
- Enhanced due diligence policies, procedures and controls for non-U.S. licensees and for accounts of non-U.S. persons
- Verify identity of accountholders initiating transactions with a value > $3,000

Source: See Davis Polk 2015 p. 41-42

Requirements set by BitLicense regarding compliance with AML/CFT policies are subject to the sanctions of the Bank Secrecy Act, which is the US money laundering law. The Financial Crime Control Network (FinCEN) is tasked with regulating money services activities and preventing and detecting money laun-

dering, fraud, scams and other illegal practices.

FinCEN published a guide on cryptocurrencies in 2015 where it bundles cryptocurrency services such as MSB[29], so all cryptocurrency service businesses must register with FinCEN as an obligated entity. The measures requested by FinCEN from the MSBs are the same as those established in the BitLicense.

3.3 The European situation

3.3.1 European Union

The first paper issued by the European Union in which reference is made to cryptocurrencies dates back to 2012 with the paper entitled "Virtual Currency Scheme"[30].

Virtual currency scheme

With this paper, the legislator warns European countries of the possible risks associated with this new type of digital currency, urging them to find adequate regulation.

The paper begins with a brief historical part in which the history of money is told and then reaches the present day, in which it is explained how the invention of the internet has revolutionized every sector over time.

In the second part, the term virtual currency scheme is explained as a type of digital currency, not regulated, which is controlled and issued by its developers, used and accepted among the members of a specific virtual community.

The paper continues by exposing three types of virtual currency:

- **Closed virtual currency schemes**: these coins have no connection with the outside world. An example may be virtual coins are earned and used by

[29]Money services and business.

[30]See European Central Bank 2012b

players to purchase in-game packages within games;

- **Virtual currency schemes with unidirectional flow**: are those coins that can be purchased with real money at a certain exchange rate and used within an ecosystem. These coins cannot be exchanged for real currency again.
- **Virtual currency schemes with bidirectional flow**: where virtual currency is easy to exchange with real currencies and vice versa: this makes them similar to any other real currency allowing the purchase of goods and services, including real ones.

Finally, the paper delves into the creation of Bitcoin by Satoshi Nakamoto, explaining how it works.

The text explains how people who use Bitcoin are often linked to the Austrian school. This school of thought criticizes fiat money subject to government decisions and, although it is based on the use of the gold standard, people who use Bitcoin see it as a first step in removing the monopoly from Central Banks regarding monetary policy decisions.

Through this paper, the ECB shows that it is afraid that cryptocurrencies could negatively interfere with the demand and use of legal tender, but explains that problems would arise only if Bitcoin began to be used on a large scale.

Furthermore, it is explained how Central Banks are not subject to the risk of bankruptcy and that they can stop, acting as a lender of last resort, possible systemic reactions in the economic system due to a crisis.

The paper ends by saying that these new systems cannot be considered safe as it is not ensured that the virtual unit of account will maintain its value, functionality or acceptability, based only on network acceptance.

Furthermore, it is explained how a system based on the absence of Central Banks is less secure, as banks are subjected to strict prudential and supervisory requirements, which ensure security and stability to the economic system thus

avoiding systemic risks.

While the ECB is clearly very concerned, it states that due to the decentralized nature of the system, cryptocurrencies are impossible to block.

3.3.2 European Banking Authority

Cryptocurrencies continue to gain popularity among people on the internet also due to the economic crisis that is shaking the whole world. This prompts the European Banking Authority[31] to publish two new papers in 2013 and 2014 entitled respectively "Warning to consumers on digital currencies" and "Opinion on virtual currencies"

Warning to consumers on digital currencies

In 2013, the EBA publishes the first paper entitled "Warning to consumers on digital currencies"[32].

The paper is not very long but draws attention to the risks associated with the purchase, possession and exchange rate of cryptocurrencies.

Above all, the risk that users run due to exchanges is emphasized. In fact, the exchange platforms, not being banks that store cryptocurrencies and, not being regulated, can cease their activity without notice. The reasons can be various,

[31] The European Banking Authority (EBA) is an independent authority of the European Union (EU), which works to ensure an effective and uniform level of regulation and prudential supervision in the European banking sector. The Authority's general objectives are to ensure financial stability in the EU and to ensure the integrity, efficiency and smooth functioning of the banking sector. EBA is part of the European System of Financial Supervision (SEVIF), which is made up of three supervisory authorities: the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions (EIOPA). The system also includes the European Systemic Risk Board (ESRB), the Joint Committee of European Supervisory Authorities and National Supervisors.

[32] See European Banking Authority 2013

from scams to cyber attacks, and all of this results in a loss on the part of users who held cryptocurrencies deposited on those exchanges.

Therefore, if an exchange fails, there is no specific legal protection, such as a deposit guarantee system, which ensures that it covers the losses arising from any funds held.

Another risk that the EBA points out is that, even if users held cryptocurrencies in a personal wallet (i.e. they had private keys), they would be exposed to cyber attacks by hackers who would try to steal our wallet.

Furthermore, since there is no central authority that records users and passwords, if the user were to lose their private keys, the cryptocurrencies would be lost forever.

It is also explained that, due to the high volatility, there is no certainty that the funds held in cryptocurrencies will remain stable and could quickly reach zero.

The paper also highlights the abuse that is made of cryptocurrencies to launder dirty money and finance criminal activities, being transactions that guarantee a high degree of anonymity. This abuse could have consequences for the consumer following the possible closure by the authorities of networks and funds based on the cryptocurrency in question.

Finally, despite the dangers exposed, the paper ends with recommendations for people who want to hold cryptocurrencies:

- act in full awareness by understanding the specific characteristics of virtual currencies, avoiding using and putting "real" money at risk of loss;
- pay the same attention to the electronic wallet as your traditional wallet or purse, avoiding storing large amounts of money in it for a long period of time and keeping it safe;
- acquire some familiarity with the ownership, business model, transparency and public perception of the exchange platforms to be used.

Opinion on virtual currencies

One year after the publication of the paper seen previously, the EBA publishes a paper entitled "Opinion on virtual currencies"[33].

Basically, compared to the previous paper, the EBA now focuses on the advantages that cryptocurrencies can bring to the modern economic system without neglecting some criticisms.

An example can be the cheapness and speed of transactions. The EBA, in fact, mentions the settlement in virtual currencies which takes place within 60 minutes, 24 hours a day, every day, against the 24-hour execution deadline and the general availability of 5 bank days out of 7 within SEPA.

While these benefits are praised, the EBA argues that the slowness and cost of traditional transactions are justified by the security that the banking system offers its customers. Moreover, the EBA explains that the cost-effectiveness of transactions is canceled out as, to return to a fiat currency, you have to pay commissions for the conversion of cryptocurrencies.

Another advantage that is identified is the certainty and irrevocability of transactions. In fact, once a transaction in cryptocurrency has been sent, it is impossible to cancel the operation. This irrevocability, although it does have some disadvantages, could help online merchants who many times, in the case of legal currencies, have complaints and refund requests delivered for a default that never happened.

The paper also acknowledges the advantage that cryptocurrencies could bring to people, especially outside the European Union, excluded from the financial system. In fact, many people cannot access traditional banking and financial services for various reasons, such as high administrative costs and burdens, especially due to problematic situations in certain embargoed or less developed countries.

Obviously, the EBA continues, this is not always an advantage as economic

[33]See European Banking Authority 2014

and commercial blockade measures could be circumvented towards countries with a terrorist or criminal inclination.

Finally, the paper concludes with the risks that require more attention:

Figure 1: Overview of risks

		ID	Risk description	Rank
A) Risks to users	General risks, irrespective of purpose	A01	User suffers loss when an exchange is fraudulent	High
		A02	User suffers loss when an ostensible exchange is not a genuine exchange	High
		A03	User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation	High
		A04	User holding VCs may unexpectedly become liable to tax requirements	Med
		A05	User who is a member of a VC mining pool does not get fair share of mined VC units from a mining consortium	Low
		A06	User suffers loss when buying VCs that do not have the VC features that the user expects	Med
		A07	User's computing capacity is abused for the mining benefit of others	Low
		A08	User suffers loss due to changes made to the VC protocol and other core components	High
		A09	User is not in a position to identify and assess the risks arising from VCs	Low
		A10	User is in violation of applicable laws and regulations	Med
		A11	User loses VC units through e-wallet theft or hacking	High
		A12	User loses VC units when exchange gets hacked	High
		A13	User's identity may be stolen when providing identification credentials to access VCs	High
		A14	Market participants suffer losses due to unexpected application of law that renders contracts illegal/unenforceable	Med
		A15	Market participants suffer losses due to delays in the recovery of VC units or the freezing of positions	High
		A16	Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations	High
		A17	Market participants suffer losses of VC units held in custody by others	Med
		A18	Market participants suffer losses through information inequality regarding other actors	Med
	When used as a means of payment	A21	User suffers loss when counterparty fails to meet contractual payment or settlement obligations	High
		A22	User experiences fraud or loss of FC when using VC cash machines	Med
		A23	User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis	High
		A24	User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet	High
		A25	User is not able to convert VCs into fiat currency, or not at a reasonable price	High
		A26	User is unable to access VCs after losing passwords/keys to their e-wallet	High
		A27	User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate)	High
		A28	User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate)	High
	When used as an investment	A41	User suffers loss as a result of VC prices being manipulated	High
		A42	User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss	Med
		A43	User is misled by unreliable exchange rate data	Med
		A44	User suffers loss when investing in fraudulent VC investment schemes	Med
		A45	User is exposed to significant price volatility within very short time frames	Med
		A46	User cannot execute the VC exchange at the expected price	Med
		A47	User is exploited by a VC Ponzi scheme	Med
B) Risks to non-user market participants	Specific to exchanges	B11	Exchange is operationally unable to fulfil payment obligations denominated in VCs or FCs	Med
		B12	Exchange is not in control of its operation	Med
		B13	E-wallet provider faces loss should their refund policies be abused to hedge currency transactions	Med
	Specific to merchants	B21	After accepting VC for payment, merchant is not reimbursed	Med
		B22	Unlike a FC, the merchant cannot be certain that they can spend the VCs received	Med
		B23	The merchant cannot be certain of the FC purchasing power of the VCs they have received	Med
		B24	Merchant faces compensation claims from customers if transactions have been wrongly debited	Med
	Specific to some other market participants	B31	Wallet provider loses e-wallets provided for individuals	High
		B32	Scheme governance authority fails to meet payment and other obligations	High
		B33	Scheme governance authority is subject to unexpected civil/criminal liability that brings the VC scheme to a halt	Med
		B34	E-wallet provider faces compensation claims from customers if functionality of wallet is compromised or fails to provide expected functionality	Med

		ID	Risk description	Rank
C) Risks to financial integrity	Money laundering and terrorist financing risks	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med
D) Risks to payment systems in FCs		D01	Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal	Low
		D02	PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations	Low
		D03	PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated	Med
		D04	Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc.	Low
E) Risks to regulatory authorities	Reputation risks	E01	Regulators decide to regulate VCs but the chosen regulatory approach fails	Med
		E02	Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs	Med
		E03	Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks	Med
	Legal	E11	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable	Low
	Risks to competition objectives	E21	Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge	Med
		E22	If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets	Med
		E23	Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive	Med
	To authority issuing FC (out of scope of	E31	Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict	Low

Source: See European Banking Authority 2014 p. 22

3.3.3 European Securities and Markets Authority

On January 1, 2011, the European Securities and Markets Authority (ESMA) was founded with the task of overseeing the European financial market. All the banking supervisory authorities of the European Union participate in it.

The Authority replaces the Committee of European Securities Regulators (CESR) and is based in Paris.

The Authority contributes to safeguarding the stability of the financial system of the European Union, guaranteeing the integrity, transparency, efficiency and regular functioning of the securities markets, as well as improving investor protection.

Call for evidence

In 2015, the ESMA published a paper entitled "Call for evidence: investment using virtual currency or distrubuited ledger technology"[34].

This paper focuses on instruments that have virtual currencies as underlying and on financial instruments registered in specific registers.

The paper explains the general functioning of the Blockchain and cryptocurrencies but, more than an explanatory paper, this publication aims to collect information about cryptocurrencies and the Blockchain. In fact, even though research was conducted in the six months prior to publication, the ESMA was unable to outline a complete picture of the situation.

Therefore it appeals to all experts and operators in virtual currencies to share data, information and know-how in their possession.

3.3.4 European Blockchain Association

After years of research the Blockchain is considered a disruptive technology, which could provide opportunities for innovation in the administrative procedure, in-

[34]See European Securities, Markets Authority 2015

cluding local ones. The interest in the use of these technologies in the public sector is evident in the important Declaration on Cooperation in a European Blockchain Partnership, signed on 10 April 2018 by twenty-one member states of the European Union[35] and to which six other states have subsequently joined[36].

In the Declaration, the signatory states recognize the potential of Blockchain for the transformation of digital public services in the European Union, pledge to work together to realize the potential of Blockchain-based services for the benefit of citizens, society and the economy and secure specific objectives for the Association.

Of particular interest is the view contained in the Statement that Blockchain-based services have the potential to enable decentralized, reliable and user-centric digital services and to stimulate new business models for the benefit of our society and the economy, and therefore believes that these services will create opportunities to improve services in both the public and private sectors, in particular by making better use of public sector information while preserving data integrity and providing better control of citizen data and organizations that interact with public administrations, reducing fraud, improving record keeping, access, transparency and verifiability, inside and outside the borders.

[35]Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK.

[36]Greece signed on 23 May 2018, Romania signed on 29 May 2018, Denmark signed on 1 June 2018, Cyprus signed on 4 June 2018, Italy signed on 27 September 2018, Liechtenstein signed on 1st of February 2019, Hungary signed on 18 February 2019, Croatia signed on 16 October 2019.

Mariya Gabriel, Commissioner for Digital Economy and Society, welcomed the signature of the declaration[37]:

> *"In the future, all public services will use Blockchain technology. Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies. The Partnership launched today enables Member States to work together with the European Commission to turn the enormous potential of Blockchain technology into better services for citizens".*

This is a vision that is completed with the possible European leadership in this field, in which the far-sightedness of the creation of a European Blockchain services infrastructure stands out.

3.3.5 Association for Trusted Blockchain Applications

On April 3, 2019 in Brussels, Belgium, a new association created by the European Commission is founded, called the International Association for Trusted Blockchain Applications (INATBA).

The official launch[38] of the organization takes place in the context of an event in which they participate as speakers who are members of the European Commission, together with the members of the new board of directors of INATBA, composed of several representatives of the companies that are part of the Blockchain ecosystem and the financial sector.

The new association is made up of 105 founding members. These are organizations based in Europe, North America and Asia. Among these companies there are some well-known in the Blockchain sector, such as IOTA Foundation,

[37]See European Commission 2018a

[38]See European Commission 2019

Sia, Ripple and Bitfury. Although traditional financial sector entities that have integrated the new technology into their systems also participate, such as the Spanish BBVA[39] and the German stock exchange Börse Stuttgart[40].

In this regard, the Head of Research and Development of New Digital Enterprises of BBVA, Carlos Kuchkovsky, confirmed the participation of the entity in the plan and stressed the importance of this new group, in an attempt to avoid fragmented actions at the European level. He also sees this as an opportunity for Europe to influence global standards for data protection and privacy management, as well as to provide greater clarity to the regulatory uncertainty currently surrounding this technology.

INATBA's goal is to offer developers and users of Blockchain technology a global space to interact with regulators and policy makers, in order to "take Blockchain technology to the next stage". The goal is to integrate more startups, small and medium-sized enterprises, as well as political leaders, international organizations, regulators and members of civil society.

In this way, it is intended to establish a dialogue with public authorities and regulators, in order to promote the convergence of the legal frameworks that apply to the Blockchain around the world. The development of interoperability specifications and standards will also be promoted in sectors such as financial services, health, energy, agriculture and public services.

Based on these ideas, the IATBA will join other initiatives carried out by the European Commission, in particular those carried out by the members grouped within the European Blockchain Partnership. The aim is to promote all efforts that support development and innovation in Distributed Ledger Technology.

On this, the Director General of Networks, Content and Communications Tech-

[39]Banco Bilbao Vizcaya Argentaria is a Spanish multinational banking group and in 2018 have partnered with energy company Repsol to develop blockchain-based financial solutions for corporate banking.

[40]In 2019 the Börse Stuttgart launches blockchain exchange for digital assets.

nologies of the European Commission, Roberto Viola, expressed his intention to stimulate greater trust in the Blockchain between authorities and citizens[41]:

> *"What makes this association special is its focus on promoting trust in Blockchain technology among public authorities and citizens. This association can also now become a natural interlocutor for all the regulators at EU and national level, for instance on standards and regulation. It will also be able to communicate with citizens about Blockchain, a technology which should not be associated with obscure cryptocurrencies but with transparency traceability and a secure environment".*

This new European Commission initiative also has the support of MEP Eva Kaili, author of the European Parliament's Blockchain report, as well as industry executives and startups that are developing and applying Blockchain based innovations to new services and products in the field of aeronautics, transportation, financial services, energy, technology suppliers, health and consumer goods.

3.4 Markets in Crypto Asset Regulation (MiCA)

The European Union wants to regulate cryptocurrencies and to do so, the European Commission published on 24 September 2020 the first proposal for a regulation for cryptocurrencies, in particular stablecoins, which will be applied in the member countries of the European Union. Called MICA, it finally answers the big questions posed by the blockchain ecosystem and the cryptocurrencies[42].

The MiCA is divided into a total of 9 titles, which are in turn divided into individual chapters.

In titles II-IV, the legislator sets out the regulatory requirements for crypto assets.

[41] See European Commission 2018b

[42] See European Commission 2020

Part V of the MiCA governs the regulatory requirements for so-called crypto asset service providers, followed by the provisions for the prevention of market abuse of title VI.

Titles VII and VIII are finally dedicated to the powers of the supervisory authorities. Both the competences of the national supervisory authorities and those of the EBA are regulated in detail. The subsequent transitional and final provisions form title IX.

3.4.1 Scope and definitions

MiCA regulation is intended to regulate licensing requirements, supervisory powers and general cryptocurrency trading in the future. In this context, the European Commission basically distinguishes between the so-called MiFID (Markets in Financial Instruments) and MiCA (Markets in Crypto Assets). This specific regime would also reassure large companies, institutions and large investors.

The following 4 main objectives are pursued:

- **Legal certainty**: for cryptocurrency markets to develop within the EU, a robust legal framework is needed for the regulatory treatment of all cryptocurrencies that do not fall under existing legislation for financial services;
- **Support innovation**: in order to encourage the development of crypto assets and the wider adoption of DLT, it is necessary to create a safe and proportionate framework to support innovation and fair competition;
- **Investor protection**: the aim is to achieve an adequate level of consumer and investor protection and market integrity in light of the fact that there are crypto assets not covered by existing financial services laws;
- **Ensure financial stability**: as some stablecloins have the potential to be widely accepted, financial stability and an orderly monetary policy are needed to be able to react to the risks that arise from them.

MiCA defines in art. 3 paragraph 1 n. 2 the concept of cryptocurrencies as: “Digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology”.

This broad legal definition creates an umbrella term for all types of digital assets. Therefore in article 1 paragraph 1 n. 3-4 MiCA there is a more precise specification through further legal definitions of the so-called “tokens with reference to assets” and “electronic money tokens”. The MiCA places special requirements on these in title III-IV.

If the product does not meet any of these special requirements, the general provisions of the MiCA apply. Therefore, these products are hereinafter referred to as “General Crypto Assets”. The exact legal classification of the product, as well as the technology used by it, are necessary to determine beyond any doubt the requirements for the issuer and the product itself under the MiCA.

If the product is classified as a “token with reference to an asset” or “e-money token”, it remains to be seen whether it can be classified as a so-called “significant crypto asset”. This is not an independent asset class, but special versions of referenced tokens and e-money which, according to the regulator, require special supervision by the EBA due to their economic importance in legal transactions. To this end, Art. 39 MiCA for tokens with reference to assets and Art. 50 MiCA for e-money tokens standardize special criteria that are used to determine whether the requirements for significant cryptocurrencies must be met. Examples of the newly created criteria are the size of the customer base or the number and value of transactions processed.

Various regulatory categories are created for all forms of cryptographic assets[43]:

- Cryptographic assets in general (e.g. Bitcoin, Ethereum, Avalanche, etc...);
- Utility Token;
- ART - are crypto-assets that purport to maintain a stable value by referring to the value of one or several fiat currencies that are legal tender (e.g. Diem);
- EMT - electronic money token (e.g. USDT).

ART and EMT include known stablecoins, depending on whether they are deposited with a single FIAT currency (EMT), or are linked to several FIAT currencies, commodities such as gold or other cryptographic values (ART). There are also additional requirements for these two categories if the token is viewed as "significant" i.e. high range and usage is expected. This addition was obviously made with the Diem project in mind.

3.4.2 Supervisory Authority

The project plans to create a team of supervisors with national authorities and EU bodies. These teams will be chaired by the European Banking Authority, an entity that will take a greater role in controlling the cryptocurrency industry.

The supervisory bodies will be the National Central Authority of the member State, the European Securities and Markets Authority and the European Central Bank. They will be tasked with reviewing the functioning and use of significant cryptocurrencies. The regulation will be applied on a large scale, imposing stricter rules, in terms of obligations, supervision and sanctions, on cryptocurrencies deemed risky.

[43]See Zetzsche Dirk A., Annunziata Filippo, Arner Douglas W., Buckley Ross P. 2020, p. 13

Token Type	Regulatory Focus	Tool	Supervision
Significant ART & EMT	Systemic Risk	Additional own funds, EBA supervision	EBA
Payment Tokens (ART & EMT)	Market Integrity, Investor / Client Protection	Authorization, Reserve & Safeguarding Rules, Own Funds, Disclosure	NCA (EBA)
Utility tokens (crypto-assets)	Investor / Client Protection	Disclosure	NCA
Investment Tokens	Systemic Risk, Market Integrity, Investor / Client Protection	EU financial law	NCA, ESMA

Source: See Dirk A. Zetzsche 2020 p. 10

Supervisors will have the power to both require cryptocurrency issuers to hold more of their own funds, and to revoke the transaction authorization in the event of serious breaches.

The regulation proposes that EBA assess the views of supervisors in each country. It will also have the power to conduct investigations, inspections and impose penalties of up to 5% of the annual turnover of the issuers or double the profits obtained or the losses avoided by the infringement.

The proposal states that cryptocurrency developers must produce a white paper with all relevant information about the issuer, token or trading platform to enable potential buyers to make an informed purchase decision and understand the risks associated with the offering. This paper is central because the MiCA permits the public offering of crypto assets or their admission to a trading platform only if such white paper has been created, published and not contested by the supervisor in accordance with the newly created requirements. Authorities may prohibit the issuer from trading in the market if the white paper or issuer does not meet the requirements of the MiCA.

The MiCA states in article 43 that issuers of "significant e-money tokens" (such as the Diem Association) will have stricter supervision. In fact, to issue the tokens, they must be approved as a credit institution or e-money institution and must comply with some requirements of Directive 2009/110/EC ("E-Money Directive").

Under the proposal, national laws for crypto assets, which have been put forward by countries like Germany, France and Malta, should operate under these EU rules.

This is how the European Commission intends to provide legal certainty, support innovation and protect consumers and investors, as well as ensuring financial stability and market integrity in the EU.

3.4.3 Regulations for Cryptocurrency Service Providers

In addition to the new regulation on cryptocurrencies and their issuance, the services and activities related to them will be subject to state supervision in the future. To this end, art. 3 paragraph 1 n. 9 MiCA defines the so-called "cryptocurrency services".

The legislator includes[44]:

- custody and management of crypto assets on behalf of third parties;
- the operation of a trading platform for cryptographic assets;
- the execution of crypto asset orders on behalf of third parties;
- the positioning of crypto assets;
- the receipt and transmission of crypto asset orders for third parties;
- advice on crypto assets.

The provision of cryptocurrency services is also subject to approval in the future and is largely regulated by the supervisory law. The regime envisaged by the MiCA is part of existing supervisory structures and is largely similar to them.

Pursuant to Article 57 MiCA, a register of cryptocurrency service providers must be created at the European Securities and Markets Authority.

[44]See Zetzsche Dirk A., Annunziata Filippo, Arner Douglas W., Buckley Ross P. 2020, p. 13

In article 60 and following, the capital requirements for cryptocurrency service providers are standardized and the reliability and suitability requirements of the managers, already known to the national supervisory legislation, are also implemented under the MiCA regime. Cryptocurrency service providers must also meet the requirements for the business organization and submit reports to the responsible authorities.

3.4.4 European States want to protect consumers

This plan for standard regulation was approved by Germany, France, Italy, Spain and the Netherlands who said they support the idea that stablecoins should not be allowed to operate in the European Union until until the legal, regulatory and supervisory challenges have been addressed[45].

The five EU members add to the proposals that stablecoins have a parity of 1:1 with reserve assets denominated in euros or currencies of the member states, and that they are deposited with an institution approved by the European Union. As the draft of the project points out, they believe entities running anchored cryptocurrency schemes should be registered in the EU.

The proposed regulation is based on the consultation of experts. For several years, the EC has been working on a regulatory framework for cryptocurrencies.

In December 2019 it opened a consultation with experts, receiving opinions on the regulatory needs of the sector. PayPal, which now supports the sale of cryptocurrencies, participated in the process[46]. Many of the ideas from the consultation were evaluated in a paper produced in April 2020, entitled "Crypto-assets: Key developments, regulatory concerns and responses"[47].

Based on this material, the EC team works on the regulatory proposal. Among the priorities is the definition of the types of cryptocurrencies and the introduc-

[45]See Kraemer Christian, Nienaber Michael 2020

[46]See PayPal 2019

[47]See European Parliament 2020a

tion of changes in Directive II on markets in financial instruments (MiFID II 2014/65/EU). This is to include crypto assets within this legal framework.

The report emphasizes the regulation of stablecoins, describing them as risky for the control of monetary policy. It plans to expand industry oversight and require anti-money laundering regulations to be enforced on cryptocurrency exchanges, wallet providers, and security token issuers. It is therefore aligned with the regulations of the Financial Action Task Force (FATF).

In a speech delivered in June 2020, the EC Executive Vice-President, Valdis Dombrovskis, had already referred to the need to apply a standard regulation in the countries of the European Union[48]:

> *"Lack of legal certainty is often cited as the main barrier to developing a sound crypto-asset market in the EU. We intend to change that, and here, I believe that Europe is in a position to lead the way on regulation. For this, we need a common approach: one that supports and stimulates innovation".*

3.5 US Banks and stablecoins

According to a letter published on January 4, 2020 by the Office of the Comptroller of the Currency (OCC), national banks and authorized US savings associations will be able to participate as nodes in public blockchains such as Bitcoin and Ethereum and process payments with stablecoins[49].

In its publication, the US regulator points out that federal financial institutions are now allowed to use new technologies, such as "independent node verification networks (INVNs[50] or blockchain networks) and stablecoins, to participate and

[48]See European Parliament 2020b

[49]See Office of the Comptroller of the Currency 2020, p. 4

[50]INVN is a general term used to describe a database where copies of information are shared and maintained across multiple computers, or nodes

facilitate payment activities". In this way, it allows banks to participate as nodes in a public and open blockchain to validate, store, record and settle payment transactions, as long as they comply with existing laws.

In the paper, the OCC emphasizes that, with blockchain interaction, financial institutions will be able to mitigate the costs of remittances and process them in a "cheaper, faster and more efficient way". For this, they can use stablecoins such as Tether (USDT), TrueUSD (TUSD) or USD Coin (USDC), which have a 1:1 parity with the dollar. The decentralized nature of stablecoins is also elected[51]:

> *"INVN and stablecoins present both benefits and risks. Among the potential benefits is the fact that INVNs may enhance the efficiency, effectiveness, and stability of the provision of payments. For example, they may be more resilient than other payment networks because of the decentralized nature of INVNs. Rather than relying on a single entity (or a small number of parties) to verify payments, INVNs allow a comparatively large number of nodes to verify transactions in a trusted manner. Simply put, these networks may be more resilient because they have no single point of failure and can continue to operate even if a number of nodes cease to function for some reason and may be more trusted because of their consensus mechanisms requiring more nodes to validate the underlying transactions."*

Several members of the cryptocurrency ecosystem reacted on Twitter to the letter OCC. In this regard, Jeremy Allaire, CEO of Circle underlined the importance of the paper, underlining that with its authorization the US regulator is granting blockchains the same status as other global networks, such as SWIFT, ACH and FedWire in the traditional financial system[52]:

[51] See Office of the Comptroller of the Currency 2020, p. 8

[52] https://twitter.com/jerallaire/status/1346233132396257282

"Breaking major news from US Treasury OCC, the largest US banking regulator, with new guidance allowing US banks to use public blockchains and dollar stablecoins as a settlement infrastructure in the US financial system. This is a huge win for crypto and stablecoins. Decentralized, permissionless, open source and internet mediated software is literally becoming the foundation for not just the US financial system but for the global economy. We are on a path towards all major economic activity being executed on-chain. It is tremendous to see such forward thinking support from the largest regulator of national banks in the United States."

Chapter 4

Central Bank Digital Currency

"You can't stop things like Bitcoin. It will be everywhere and the world will have to readjust. World governments will have to readjust."

– John McAfee[1]

4.1 A new financial system

Bitcoin will not change the financial world as we know it, it has already changed it. The best proof of this is Central Bank Digital Currencies (CBDC), a project with implications that would change the traditional financial system and would not have been considered if Bitcoin hadn't changed the rules of the game.

Bitcoin has brought to the world the ability to transfer digital value globally without the need for intermediaries, without asking for permissions and without censorship. Many have wanted to replicate this idea by creating other cryptocurrencies. The world's Central Banks, some to a greater extent than others, have underestimated these experiments, posing small obstacles, but without a coordinated international attack to show their concern, until Facebook announced

[1]John David McAfee (born September 18, 1945) is an English-American computer programmer and businessman. He founded the software company McAfee Associates.

Libra[2] (now called Diem).

Investigations into CBDC have been ongoing since at least 2014, when the scenario was established by the Bank of England with a paper titled "The economics of digital currencies"[3]. Since then, several Countries and organizations have investigated this possibility, created prototypes and conducted tests.

But it was only when Facebook announced Libra that Central Banks realized the inevitability of the ongoing change and the need to step in and reignite the CBDC debate.

The practical implications of implementing CBDC are profound, not just for users but for the entire financial structure.

Since Central Banks are institutions whose primary responsibility is to ensure economic stability, it is not possible to take the liberty of making drastic and imprudent decisions. Agustín Carstens, general manager of the Bank for International Settlements (BIS), was of this opinion when he thought about the future of money and payments[4].

Calibrating the costs and benefits of adopting a CBDC-based model involves projecting scenarios and potential consequences for the financial system as a whole.

However, delays for some are beneficial for others, as the cross-border nature of these currencies could change the current landscape in terms of international reserve currencies and foreign trade, even more so at this critical time for the global economy.

[2]See Boorstin Julia 2019

[3]See Bank of England 2014

[4]See Carstens Agustín 2019, p. 7

4.2 Definition of CBDC

Central Bank digital currency would be a more flexible and programmable form of Central Bank money and, depending on how it is designed, could both maintain cash anonymity and eliminate the need for financial intermediaries, such as increasing the supervision and monitoring of private monetary policy, maintaining the presence of private banks. In addition, it could imply digital cash subject to interest rates, a greater monopoly of the Central Bank's financial activity and more instruments for its monetary policies.

Current literature and research on the subject contemplates the use of distributed databases such as those used in Blockchain networks such as Bitcoin for the technical architecture of CBDCs. The main difference from Bitcoin would be that decentralization would not be desirable. Rather, network security and transaction verification would be the sole responsibility of the Central Bank and, in any case, of the bank's trusted institutions.

Depending on the goal to be achieved with the CBDC, its potential attributes vary. For example, as regards its scope, it could be universal/retail, in the event that its use is open to anyone, or limited/wholesale, when its use is limited to financial intermediaries.

In the universal case, the CBDC could allow any person or business to make electronic payments using money issued by Central Banks using the means of payment provided by the institution, as well as deposit their money directly into their accounts. The Central Bank would then become the custodian and provider of legal tender digital money services.

In the limited case, the reality would not be much different from what it is today for individuals in their daily lives, even if they could benefit from improvements in the efficiency of banking institutions.

Regarding the approach that is given to financial information, i.e., if it is inclined to maintain the anonymity of cash or if, on the contrary, it tries to link

money to identity, the CBDC would use a token system, for the first case, and a system of accounts, for the second. Most likely, the general orientation tends towards the system of accounts, not only because it increases supervision and control, but because it has been tested for more years than the one based on tokens.

Finally, the CBDC may or may not earn interest. Introducing an interest rate on this form of digital money would broaden the scope of Central Bank monetary policy. For example, it can be used for anti-deflationary policies by encouraging consumption and discouraging savings. However, this is an unlikely scenario as it would face criticism of excess power from the Central Bank, and could also be seen as a hidden tax.

4.3 Central Banks and financial intermediation

Money has been electronic for many years. Debit and credit cards were means of payment that transferred money in bits to the computer.

The Central Bank, as a public institution and monetary authority, has the main functions of preserving the value of the national currency, maintaining price stability and the financial system as a whole. Its main tool for managing monetary policy is the interest rate.

Central Banks have the task of guarding and managing gold and foreign currency reserves, issuing legal tender currency, acting as treasurers and financial agents of public debt, and are also accountants and lenders of private banks.

The Central Bank is the bank of private banks. By simplifying a Country's complex financial system, it can be seen that it is made up of two tiers, where Central Banks act as intermediaries between individuals and the Central Bank. Central Banks exercise their monetary policy through private ones, raising or lowering interest rates, using them as a vehicle to increase liquidity.

There has been a growing interest in the elimination of cash lately from the

traditional financial system. Perhaps the main argument for this has been to combat the criminal use of cash which facilitates its anonymity and fungibility, both to avoid taxes and money laundering, and to finance illegal activities. There is also the high cost of manufacturing new units, even more so in hyperinflationary or devaluation scenarios and frequent exchange of currency cones.

Liquidity also limits the scope of monetary policies based on negative interest rates, as it provides a zero-rate alternative on deposit. Now, after the declaration of a COVID-19 pandemic, the potential of cash as a disease propagator has been added to the arguments.

The only partially direct relationship between individuals, be it a company or a person, and Central Banks is cash, so eliminating it would further increase the need for and dependence on financial intermediaries. Furthermore, money has advantageous properties that would mean a loss, in particular its availability outside the network, its ease of use which does not require transaction costs and its liquidation is immediate. However, with the introduction of CBDCs, the picture changes.

The likelihood of creating a CBDC greatly depends on the different objectives of both Central Banks and the authorities of the specific Country. Since the authorities of the Countries do not share the same goals, there will always be those who advance before the others.

However, the possibility of cross-border competition from different CBDCs is a major concern when falling behind in this technology race, as it could undermine dominant positions in the global market.

At the moment, this is limited by the portability of physical money, but by going digital these logistical difficulties would disappear. In the event that CBDCs are designed to emulate cash, while maintaining anonymity, it will not be possible to limit their use to residents of a Country. This could lead to an increase in demand for foreign currencies, especially in Countries with currency instability.

Another of the conclusions that can be drawn from this study is that the

obsolescence of traditional financial intermediaries depends on a decision by the Central Banks. Being true to their principles of stability, they are unlikely to take such disruptive action. But it is still surprising that even outside the scope of Bitcoin, and thanks to the technology it has put on the table, in the traditional financial field, financial intermediaries have become optional. Their existence is for the sole purpose of maintaining the current status quo, but they are no longer necessary.

Of course, its elimination has many other consequences. Not only does it mean an increase in the costs and responsibilities of Central Banks, which would have to assume all functions of financial service providers. This could degrade the service as concentrated in a single entity, which means increasing the monopoly of the Central Bank, not only in the creation of money, but also in its administration.

Above all, one of the biggest risks of this monopoly is in individual privacy. The Central Bank, with the risk of becoming politically biased as it has happened several times throughout history, but more recently in Venezuela[5], would maintain full surveillance and control over transactions, so its censorship capacity would be greater than it is currently. Additionally, creating a single centralized node increases the risk of system hacking, remembering that all software and hardware, no matter how secure, is always susceptible to attack.

It can be seen that the debate on CBDCs is not so much about affordability and digitalisation as it is about fundamental change in the financial system, at least in terms of money and payments.

[5]See Zupi Marco 2017, p. 1

4.4 Possible scenarios

To analyze the implications of CBDCs in the traditional financial system, BBVA researchers proposed four possible scenarios[6]:

- The first option would be a scheme where the use of CBDCs is limited to financial intermediaries. This scenario would increase the efficiency of the wholesale payment system, would not change monetary policy making and could increase competition for banks from non-bank payment institutions;
- The second option opens the CBDC to the general public, maintains the anonymity of cash based on a token system. The efficiency gains outweigh those of the first option by eliminating financial intermediaries from money transfers. Its role would be reduced to other financial services such as credit and loans, although its capacity would be weakened;
- The third option introduces the possibility of CBDC with interest rates. This option focuses on increasing the scope of monetary policies. It involves the total elimination of cash, which has high costs in educational processes and in the distribution of devices;
- The fourth option raises a universal CBDC linked to identifiable accounts. It would be like having an account in a Central Bank. This would increase the supervisory powers of the monetary authority over individuals but this would risk that, in times of instability, individuals turn to the Central Bank and not to private banks that would find themselves in trouble.

Due to the conservative bias of Central Banks, it is very likely that the first option will be the first to be implemented in the short term.

Central Bank digital currencies (CBDCs) present many challenges, so their implementation has been quite limited, although it has been extensively studied.

[6]See BBVA Research 2017, p. 2

Studies conducted by the BIS showed that 80% of banks are interested in researching and studying CBDCs, while only 50% have devoted efforts to Proofs of Concept and Experimentation, and only 10% have tried to develop pilot projects. with Sweden and China as the main exponents[7].

4.5 Diem

Diem (ex-Libra) is the name given to the future cryptocurrency initiated by Facebook. "The Libra mission is to enable a simple global payment system and financial infrastructure that empowers billions of people.", summarizes the project's white paper[8], which was revealed on June 18, 2019.

In other words, it is a new currency, totally digital, supported by a Blockchain, already used by other digital currencies such as Bitcoin. The Diem cryptocurrency will be based on a "permission" Blockchain, which means that access to the protocol must be validated, unlike the Bitcoin Blockchain which is open to everyone.

Thanks to this technology, every transaction made in Diem is authenticated, encrypted and validated by multiple servers before being recorded in an open ledger and hosted on these same servers. One way to protect yourself from criminals who would like to hack the system to credit your personal account, doing without an organization such as a Central Bank.

The Diem will be a stable currency, i.e. a stablecoin, and it will be traded instantly as it will not have to go through the banking network. In addition to a Diem backed by a basket of currencies, there will be several Diems: a USD Diem, a EUR Diem, a GBP Diem, and an SGD Diem. "We hope to work with regulators, Central Banks, and financial institutions around the world to expand over time the number of single-currency stablecoins available on the Diem network" reads

[7]See Barontini Christian, Holden Henry 2019, p. 8

[8]https://www.Diem.com/en-us/white-paper/#the-libra-payment-system

the updated white paper.

In order to reassure authorities and people who might be scared by the extreme volatility of cryptocurrencies like Bitcoin, Facebook promises that Diem's value will remain stable. To fulfill this promise, the social network decided to tie its currency to a reserve of real assets made up of hard currencies. The Diem Association will then put this currency on deposit with a repository or use it to buy highly liquid government bonds and entrust them to the repository. At this point, there is very limited detail regarding the composition of the reserve: it will be along the lines of an SDR (IMF Special Drawing Rights, comprising the US dollar, Euro, Yen, Pound Sterling and RMB) or trade or otherwise weighted[9].

To use this new cryptocurrency, you will first have to create an account on an application that will act as a virtual wallet, which can be credited by purchasing Diem with a traditional currency. Facebook has already taken the initiative by creating a wallet, Calibra, which will offer a service of this type.

Once the wallet has been created, it will be possible to exchange Diem with contacts from the ad hoc application or from the various Facebook messengers. The social network also intends to offer a professional version of Calibra to merchants and online stores who wish to accept this payment method. It is possible to imagine that thanks to the perfect integration it is possible to order the dress worn by a favorite influencer directly in Diem, without leaving the application for a second. Or pay for a Diem trip on the Uber app while abroad, eliminating the hassle of exchange fees[10].

A possible concern is the possible use of Diem for illicit purposes (money laundering, terrorist financing, etc.), however, these fears are not justified. On its official Calibra website, it is explained that to create a wallet, identification of its users will be required before they can create an account.

The Diem is expected to be released in early 2021, at the same time as Face-

[9]See Zetzsche Dirk A., Buckley Ross P., Arner Douglas W. 2019, p. 14

[10]Ibidem, p. 15

book's wallet, Calibra. Its launch is necessary for the approval of the Swiss financial guardian, Finma, who received the request for approval of the association's payment system in April 2020[11].

4.5.1 Diem association

Contrary to what one might think, Facebook is not alone in this project. The Diem association, responsible for the development and proper functioning of the network, is currently composed of 21 founding members, who form the Council of Diem, a sort of Parliament of this new institution based in Geneva (Switzerland). One way to prove that the American giant will not have total control of the cryptography since it is a member among others[12].

To join the association, members must pay an investment of $10 million. This investment allows them to own a Blockchain node, which underlies the cryptocurrency. Any participant can sit in the foundation that Facebook created in Switzerland to manage cryptography. "Important decisions about policies or technical choices require obtaining two-thirds of the votes, which is the absolute majority of the network required by the consensus protocol" indicates the white paper.

Among the members of this selected association are the online payment company PayU, the telecommunications groups Vodafone and Iliad, the platforms Uber, Spotify or Farfetch, companies in the blockchain sector such as Anchorage, Xapo and Coinbase, venture capital funds such as Andreessen Horowitz and Ribbit Capital, or non-profit organizations like Kiva and Mercy Corps.

Initially involved in the Diem project, Visa, Mastercard, eBay and Stripe announced their withdrawal from the association on Friday 11 October, a week after PayPal, another Facebook partner in the operation. Most justified their

[11]https://www.finma.ch/en/news/2020/04/20200416-mm-lb

[12]Boorstin Julia 2019

choice with doubts about the project's ability to fully satisfy all the expectations of the regulators[13].

4.5.2 Risks

As explained in the white paper, Diem will be a fully pooled asset backed cryptocurrency, it will be issued only on request, and its value will be given by a basket of reserves whose composition will be diversified, favoring safe assets and stable international currencies.

In other words, while commercial bank money (i.e. deposits) can be created simply by granting a loan, Diem will only be created as consideration for an existing monetary unit, whether issued by a central bank or commercial banks[14].

This means that the fear, expressed by some, that a sudden banking panic could cause Diem to collapse is irrational. In fact, since Diem is 100% guaranteed, it is at least as safe as the commercial bank deposits we accept as payment on a daily basis. It will always be redeemable in currency and this refund will not only be theoretical (as is the case with commercial bank money and fractional reserves) but also practical, as a Diem unit can only be created when new reserves are deposited.

Other people worry that Facebook's entry into retail payment will reduce competition. The experience of past payments-related innovations, particularly the payment card market, however, suggests that Facebook will have a hard time expanding its domain in this area without partnering with other Diem project players.

The members of the Diem Association have different complementarities and specialties. All members will cooperate in the governance of the association while remaining competing in other sectors. Some will compete with others in providing

[13]Del Castillo Michael 2019

[14]See Zetzsche Dirk A., Buckley Ross P., Arner Douglas W. 2019, p. 21

Diem-denominated payments. Thus, one would expect a different ecosystem to emerge, in which different members do different things. Even if Facebook were to gain an advantage in this area, competition inside and outside Diem should help mitigate its monopoly impulses.

4.6 Digital Euro

New technologies and the need for speed and immediacy have a profound effect on the way payments are made, and the EU knows this. In the digital age, electronic, contactless payments and digital currencies are on the rise. A digital euro is therefore a logical continuation, which must emerge in a safe, secure, solid and accessible form.

The European Central Bank in October 2020 through a paper revealed the first decisions on the matter. Christine Lagarde also stated[15]:

> *"The euro belongs to Europeans and we are its guardian. We should be prepared to issue a digital euro, should the need arise."*

The paper states that the ECB has come to the conclusion that most of the desirable features of the digital euro could meet the emerging payment needs of a modern economy by offering, alongside cash (which the EU does not want to abolish), a secure digital asset with advanced features.

4.6.1 The Digital Euro must meet the needs of change

Today, more than ever, this is the case, with a pandemic that has shocked the world economy, the perception and public use of cash, with respect to electronic payments, is changing[16]. While it remains the dominant means of payment across

[15]See European Central Bank 2020a

[16]See The Economist 2020

the euro area, cash is on the decline in some countries and preferences are changing rapidly in the current health and technology environment.

Other key issues raised by the October 2020 paper are those of confidentiality, including improving user privacy, as well as concerns related to money laundering and terrorist financing.

The establishment of a CBDC could respond in this sense to the new contemporary needs and the challenges they have imposed.

Some basic guiding principles for the design of a digital euro can be identified on the basis of the recent paper[17] of the ECB and the declarations[18] of the EU which, since 2016, have been studying these payment systems.

A digital euro would be just another way to issue and supply the euro, not to create a parallel currency. It should therefore be convertible to other forms of euro, such as Central Bank notes and reserves and commercial deposit banks. The European Central Bank makes it clear in the paper that cash does not want to be abolished by the EU.

Furthermore, as the paper explains, the Eurosystem would retain control over the issuance of the digital euro and supervised private intermediaries would be best placed to provide ancillary services to users. As private intermediaries, we may also find entities that manage Blockchains such as Ethereum or Avalanche. A model in which access to this digital currency is mediated by the private sector is therefore, according to the ECB, preferable.

To illustrate the possibilities for collaboration envisaged by the ECB, the paper cites several. The more restrictive approach is to create a constrained framework in which the systems and software used by intermediaries and users are provided by the Central Bank itself. In this way, all possibilities are coded by the Central Bank. With such a solution, the systems of intermediaries could not create or destroy the digital euro units, the creation of money would always be the task of

[17]See European Central Bank 2020b

[18]See Panetta Fabio 2020

the Central Bank.

However, this solution would impose a heavy operational burden on the Eurosystem. For this reason another approach is considered, which consists in allowing external companies to carry out audits in real time on all systems belonging to intermediaries and user devices. In practice, this would mean that payments would be delegated to an intermediary company, but that many automated systems and controls, managed by the Central Bank, will be put in place.

4.6.2 How the Digital Euro will work

For the consumer, as for the merchant, it should take a habitual form. Practical solutions for payment in CBDC would be made possible, according to the latest ECB paper, by apps, digital wallets and virtual cards.

Today mobile or online banking are the order of the day and companies (online or physical) rely heavily on various payment methods, which are increasingly modern and connected. For professionals, we can think of POS systems, present everywhere, and thanks to which we can pay by card.

The European CBDC would use the same scheme and use the same tools, consumers will be able to use a physical or virtual credit card such as Apple Pay. companies will have a payment receipt solution, with a POS terminal or directly integrated into their e-commerce site.

Uses do not need to be transformed, only constraints related to security, commissioning or design of payment solutions need to be adapted.

4.6.3 Benefits

Using the Blockchain, interbank payments would simply be faster and safer. In addition to speed and security, a CBDC would be a way to transfer money without bank charges when sent around the world. As stated by Benoît Coeuré, Head of

the BIS Innovation Hub[19]:

> *"Central banks around the world are stepping up efforts to study CBDCs with the aim of creating secure and reliable settlement tools for transactions in the digital economy, both wholesale and retail. In parallel, international coordination of policies can ensure that all advances in payment systems facilitate greater efficiency, cross-border integration, security, financial inclusion and innovation".*

The Blockchain represents the opening and promotion of technological innovations that integrate or use it. The creation of a Blockchain-based infrastructure would allow the integration of features such as "smart contracts". It is similar to a paper contract, but where the terms of the agreement between the buyer and the seller are written in lines of code. Therefore, due to its presence on a Blockchain, its application is protected. Finally, the use of the Blockchain would give space to potential innovations to improve the system.

4.6.4 Areas of uncertainty

In terms of confidentiality, the digital euro raises questions. The issuance of a digital euro would require the Central Bank to be able to innovate, without compromising the fundamental aspects of security. Some concerns have been raised that, by introducing their own digital currency, banks can acquire sensitive information about users. Most users and investors are also worried that the private payment solutions that will emerge (especially if this currency is not regulated) could lead to cyber risks.

In the case of a digital euro, these risks could be mitigated by the involvement of the Central Bank, which would control and protect the currency and its transactions. Finally, according to the ECB paper, the digital euro could stimu-

[19]See Bank for International Settlements 2020

late the offer of new payment services and functionalities, thus creating business opportunities.

According to experts from the European Central Bank, the digital euro should be an alternative means of payment, but above all it should be designed in such a way as to avoid its use as a form of investment. Depending on its characteristics as a form of investment, it could encourage citizens to convert their deposits in commercial banks into CBDCs. These phenomena could create instability and reduce the funds stored in private banks. As a result, private banks would be more dependent on the Central Bank for funding and could raise interest rates on bank loans, reducing the volume of bank credit and stopping consumption.

However, according to the paper, and in response to these dangers signaled by the public debate, experts assure that the issuance and circulation of a digital euro should not create financial risks for the Eurosystem. In the interest of sustainability, it is noted and emphasized that the new currency should be widely accessible to users in all countries in the area. The European Union will need to remain alert to digital divisions within and between countries in order to best promote access to the digital euro and the transition to a digital economy.

The emphasis therefore needs to be placed on accessibility across the euro area. The digital euro should be made available through standardized solutions. It should be easily accessible to everyone, including citizens who do not participate in the financial system (for example, those who do not have an account in a commercial bank) and easy to use.

A retail digital euro would inevitably have implications for the functioning of the new payment system established. It must therefore be designed in a way that does not hinder, but rather improve the proper functioning of this system, so as to maintain confidence in the euro and promote an efficient market economy.

To get an opinion from its population, the EU launched its public consultation on Central Bank digital currencies in October 2020[20]. In the form of a question-

[20]See European Central Bank 2020a

naire, it invites companies, associations and citizens to express their opinions and concerns. The answers will allow in particular to obtain the guidelines for the future design of the CBDC, since it will be possible to deduce the priorities of the European population in terms of monetary and digital use.

In mid-2021, following the results of the public consultation, the Governing Council of the ECB will consider more closely whether to launch a digital euro project. The investigation would aim to identify at least one viable product capable of meeting the requirements outlined in the October 2020 paper. Before a decision can be made on issuing a potential digital euro, it is necessary to seriously quantify the scope and cost of such a project, in order to compare this solution with the possible alternatives. It is obvious that the costs are not only financial, but also organizational, and must all be carefully evaluated.

4.7 Digital Yuan

The digital yuan, also known as DCEP[21], is a new virtual version of the yuan, China's national currency. The country has been working on it for years and has clearly stepped up its efforts in 2020 so that it can be the first country in the world to make CBDC its official currency, a perfect replacement for physical currency. Researching and evaluating central bank digital currencies since 2014, China set up the "Digital Currency Research Institute" in 2017[22], then launched a series of tests in 2020.

Today, thanks to a new law on the organizational structure, powers and restrictions of the People's Bank of China on the digital yuan, new projects are born[23]. The digital yuan thus takes its first steps as a useful and used currency.

This Law, which officially legalized electronic payment in digital yuan, had

[21]Digital Currency Electronic Payment

[22]See China Banking News 2018

[23]See Fatiguso Rita 2020

already opened the door to more widespread use.

This use did not take long and the first public and private bodies took the opportunity that was made available to them. JD.com, one of the country's leading online shopping platforms, now accepts payments in digital yuan[24] while Hong Kong could become the first partner jurisdiction to use China's CBDC for its cross-border payments.

4.7.1 Cross-border payments

China's ambitions for developing an innovative financial and monetary instrument that can compete with the dollar and celebrate Chinese superiority are no longer a secret. By providing an answer to the slowness of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) cross-border payment system, the digital currency contains interesting diplomatic potential. As the Australian Strategic Policy Institute (ASPI) wrote in a recent report[25]:

> *"Over time, it is not far-fetched to speculate that the Chinese party-state will incentivise or even mandate that foreigners also use DCEP for certain categories of cross-border RMB transactions as a condition of accessing the Chinese marketplace."*

The first step in this direction has been taken, as the country has found its first potential partner in Hong Kong to accept the digital yuan in its cross-border payments. Hong Kong Monetary Authority (HKMA) head Eddie Yue published a paper titled "A New Trend for Fintech - Cross-border Payment" on December 2020 which outlined the various channels through which Hong Kong wants improve their payment systems[26]. Among them is the digital yuan, which China and Hong Kong are preparing to use for their mutual payments.

[24]See Kharpal Arjun 2020

[25]See Australian Strategic Policy Institute 2020

[26]See Yue Eddie 2020

The paper states that "as the renminbi is already in use in Hong Kong and the status of e-CNY is the same as cash in circulation, it will bring even greater convenience to Hong Kong and Mainland tourists", before noting that the discussions are preliminary and that there is no timetable yet.

This first potential use of the digital yuan for international payments embraces China's aspirations to shape technological, financial and business standards around the world. The promotion of the internationalization of China's CBDC joins the various other companies in the country to compete with the United States and dollar hegemony in payments.

The news of Hong Kong's joint entry into the digital yuan is therefore significant, which is part of China's strategic plan against the United States, with which relations are deteriorating. Hong Kong's status as a major financial services hub makes the announcement of the collaboration even more significant and predicts a bright future for China's new digital yuan.

4.7.2 The first tests

In Shenzhen, on October 12, 2020, the country has already started a life-size test in the form of a lottery, to evaluate the consumption behavior of citizens. Designed to promote the digital yuan, this pilot project then distributed a value of 200 digital yuan to the selected candidates to see how they would spend it and how easily[27].

The lottery invites citizens to register through the official application of the organizing city services. The winners will then receive their prize: packages of 200 yuan, the equivalent of 25 euros. In its statement on the event, Shenzhen city officials said they would distribute a total of 20 million yuan (2.5 million euros) to residents. Of course, it didn't take long for Chinese companies to start offering the use of CBDC as a means of payment in their point of sale or online

[27]See Akhtar Tanzeel 2020

service. All this, accompanied by tempting offers available to the lucky winners of this lottery.

This lottery was then replicated in Suzhou last December 2020, where JD.com, China's second largest online retailer, allowed MNBC package winners to spend them by purchasing some of its items[28].

JD.com thus contributes to promoting the development of the digital and real economy, helping the People's Bank of China and local governments to carry out their studies on consumer behavior, as part of the tests on the digital yuan.

Today a third pilot project is underway in the country, since 1 January the Futian district has distributed 20 million yuan to its population[29]. Small difference from previous tests, the number of physical stores accepting payments in digital yuan has increased significantly and the trial version now includes the function of depositing and withdrawing digital yuan via ATMs. This new feature is offered by the Agricultural Bank, one of the four largest state-owned banks in China.

With the use of the ATM and the smartphone that contains the digital wallet, China hopes that, thanks to the familiarity of these means, it will increase the coverage of merchants who accept digital payments.

In addition to shopping malls, supermarkets or local services, the type of transaction that can be performed using the Chinese CBDC can also be of low frequency and amount. For example, to top up a subway card or pay a phone bill.

4.7.3 China wants to be a pioneer

For China, this somewhat original experiment takes place in the context of its rapid progress in the Central Bank's digital currency. A report from the Bank for International Settlements, released in January, found that 20% of the world's

[28]See Akhtar Tanzeel 2020

[29]See Lee Amanda 2020

central banks plan to launch their digital currency within the next six years[30]. Of course, China wants to be a pioneer.

The digital yuan in China is making encouraging progress and has already covered more than 6,700 payment scenarios, according to the country's deputy central bank governor, Fan Yifei. The tests integrated seamlessly with existing payment methods such as QR codes and NFCs. According to Fan Yifei, more than 120,000 personal and business digital wallets have been created for the digital yuan since testing began[31]. The country must be guaranteed its speed and its position in the increasingly populated CBDC sector. China is in a phase of active experimentation and characterization of its currency, which should be operational by 2022.

Unlike other central banks in the design it offers its digital currency, the BPC wants to go all the way by adopting a retail CBDC, giving commercial banks a crucial role. Four large commercial banks, as well as the country's leading telecommunications companies, have been involved in pilot projects such as electronic payments in digital currency in Shenzhen. For the moment, China wants to make this new digital currency accessible to citizens, while maintaining the intermediation of commercial banks. Additionally, the CBDC will be account-based rather than symbolized as a token. The digital yuan will be used to top up bank accounts, make bank transfers and payments. Enough to provide jobs to banks while competing with the two giants Alipay and WeChat.

Indeed, the Chinese authorities continue to insist that the digital yuan is simply a means for the authorities to fight criminal activities such as money laundering and to help the Chinese Central Bank control the circulation of physical money. However, the digital currency will clearly compete with a number of local digital payment systems such as Alipay and WeChat Pay.

The Chinese mobile payments market is currently dominated by the two giants,

[30]See Bank for International Settlements 2020

[31]See Hui Ada 2020

this means for the Central Bank a loss of control of the liquidity circulating in the territory: users deposit their money in these two companies, subsequently draining the money from the traditional banking system. The governor of the BPC, Yi Gang, declares in this regard that large technology companies carry many financial challenges and risks[32].

As agents, banks can monitor accounts and ensure control of working liquidity, however, this monitoring also allows them to collect data. Implementing the digital yuan in the currently desired form would give authorities full traceability of the use of the currency, which clearly marks one of the biggest differences with cryptocurrencies.

Many issues thus constitute the creation of the Chinese yuan, which China is determined to develop at all costs, taking into account obvious domestic and foreign policy reasons. However, and as these curious ongoing pilot projects show, China is far more advanced in its tests than the European Union.

[32]See Tudor-Ackroyd Alison 2020

Conclusions

Since the internet has become part of our lives, digital has really imposed itself and has constantly changed our lives in social, professional, economic, political or even judicial composition. All levels are at stake: our organizations, our communications, our interactions, our movements and most of all our business.

The new payment methods are attractive, and this is particularly the case with cryptocurrencies, whose advantages and designs have fueled interest since the creation of Bitcoin in 2008. So there was the beginning of an ascent, for Bitcoin. and for cryptocurrencies that will be born later. They are an alternative method of storing money and making payments, without relying on the traditional banking system.

Going further, we can even trace the origin of CBDCs back to the 2008 financial crisis that led to the digitization of transactions and the diminishing role of cash. Indeed, the crisis has significantly changed the relationship of the world population with banks and money: overall, trust in the banking system (and in particular in private banks) has since decreased.

What is certain today is that it is thanks to all the advances and innovations that cryptocurrencies have allowed that today we can talk about CBDC. And it is precisely in reaction to the success of these decentralized private currencies and, specifically, when Facebook announced the development of its Libra cryptocurrency in 2019, that central banks became aware of the threat it posed.

Witnessing an increasingly digital and changing economy and the rise of these private currencies, the Central Banks of the States of the world have therefore

undertaken research on potential digital, but public currencies. To respond to the threats of the rise of digital private currencies, many governments are redoubling their efforts to create a digital currency, in its most centralized and sovereign version.

Being controlled by the state, a question then arises: how does it benefit, exactly? Beyond the aspect of regaining monetary sovereignty, countries could benefit from many benefits by opting for a CBDC.

First, using a Blockchain, CBDC would be a safe, fast, and intermediary-free way to transfer money, without bank charges even if sent from the other side of the world.

However, this is not without forgetting the limitations of these digital currencies, made up of dangers and challenges. These dangers are mainly financial in nature, as the digitization of the currency could compromise financial stability, offering attractive substitutes for depositing money.

The availability of CBDC could facilitate bank purchases, but also structurally deprive banks of an important source of funding and thus reduce their ability to provide credit.

Monetary stability must also be taken into account. The widespread availability and accessibility of CBDCs could exacerbate the flight of international capital to safe haven CBDCs during crises, thus creating situations of monetary instability.

Also worth mentioning is the risk of loss in case of accidents or cyber attacks. In fact, a new type of crime could develop, adapting as always to new technologies. We can therefore think of the difficulty that will be the implementation of effective means to counter them.

A concept far from being without problems, as it represents some advantages.

the central bank's digital currency covers all kinds of issues and can be a cause for concern for a population that is increasingly fragmented around technology. Accused of damaging monetary stability, financial stability and even compro-

mising the privacy of its users, the contours of this currency must be patiently researched and researched.

The establishment of a CBDC could change many things: from the creation of money to the banking system, including the instruments of control and surveillance available to the state, order and diplomatic relations could be affected.

Motivated by a recapture of digital and monetary sovereignty, the race for the central bank's digital currency is well underway and awaits only its winner. It remains only to hope that decision makers design an inclusive, efficient and secure currency and, taking into account all the threat factors, citizens are also the winners of this digital gamble.

Glossary

Address: A string of letters and numbers that people use to send and receive Bitcoins. An address is generated from a public key, which in turn is generated from a private key.

Block: A set of transactions that are added to the Blockchain.

Blockchain: A decentralized and distributed ledger that makes the history of any digital resource unalterable and transparent through the use of cryptography.

CBDC: Central Bank Digital Currency.

Centralized: The process by which the activities of an organization, especially decision-making, are concentrated in a place or by a small group of people. Some examples of centralized payment systems can be Mastercard, Visa, American Express, etc...

Coinbase: The reward that is given to a miner for confirming a block.

Cold Wallet: A wallet that allows you to store a digital asset offline. An example of a cold wallet is the hardware wallet.

Commissions: Also called fees, they are a sum to be paid to the miners in order to send cryptocurrencies.

Confirmations: A cryptocurrencies transaction is confirmed when it has been included in a block by a miner. Each subsequent block added to the Blockchain is another confirmation for that transaction.

Decentralized: The opposite of centralized. A form of organization in which decision-making is not concentrated in one place or by a small group of people. Bitcoin is a decentralized network because no central authority can control or block it.

DLT: Distributed Ledger Technology.

EBA: European Banking Authority.

ESMA: European Securities and Markets Authority.

Exchange: A platform that allows people to buy and sell cryptocurrencies.

Fiat: Term used to refer to legal tender currencies (euro, dollar, etc. . .).

Hash: A mathematical process used by miners to maintain network security. "Hash" also refers to the unique identifier of a cryptocurrencies transaction/block.

Hashrate: Unit of measurement of the processing power of a cryptocurrencies network.

Hot Wallet: Any wallet running on an internet connected device is considered a hot wallet (as opposed to a cold wallet).

Halving: The halving of the reward (coinbase) that is awarded to miners for carrying out the work of confirming the blocks. It occurs every 210,000 blocks which, considering an average of 10 minutes each, are approximately 4 years.

Ledger: Ledger. In the case of Bitcoins it is the complete and public list of all

transactions that are carried out on the Blockchain.

Mempool: short for memory pool. The mempool is where all valid transactions wait to be confirmed by the Bitcoin network. A large mempool size indicates higher network traffic which will result in longer average confirmation times and higher priority fees.

Miner: A user who, through a computer and hardware, confirms blocks and verifies those created by other miners. Miners are incentivized to do this work because along with the transaction fees they also receive new Bitcoins (coinbases) for each block they confirm.

Multi-Signature Wallet: It is a type of wallet in which exit transactions must be authorized by several people.

NCA: National Central Authority.

Nodes: They are the participants within the cryptocurrencies network who keep a complete copy of the Blockchain.

Open Source: Freely distributed software whose code is available to the public for modification, use and sharing.

Paper Wallet: A type of cold wallet in which private keys are printed on a sheet of paper. Although it is one of the safest and most of all economical methods to store cryptocurrencies, it is difficult to create completely safely.

Peer-to-Peer: Often abbreviated to P2P is a type of network where participants communicate directly with each other rather than through a centralized server. The Bitcoin network is a Peer-to-Peer network.

Proof of Work: The protocol behind Bitcoin mining. It is used to confirm new

blocks and add them to the Blockchain.

Protocol: A set of rules that must be followed by people who intend to use a particular network.

Public Key: A string of letters and numbers that is generated from private keys. An address is generated from a public key which is used to receive Bitcoin.

Private Key: A string of numbers and letters that is used to use the Bitcoins stored on a wallet.

Satoshi Nakamoto: The creator of Bitcoin, who disappeared from the web in 2011, nobody knows who he is.

SHA-256: The SHA-256 algorithm is a hash function used for Bitcoin mining.

Wallet: A digital wallet that allows you to store, receive and send cryptocurrencies. There are two types of wallets: cold wallet and hot wallet.

Bibliography

Adrian Tobias, Mancini-Griffoli Tommaso (2019). *The rise of digital money.* International Monetary Fund. ISBN: 9781498324908.

Akhtar Tanzeel (2020). *Shenzhen to Double Digital Yuan Giveaway in China's Latest Lottery Test.* URL: https://www.nasdaq.com/articles/shenzhen-to-double-digital-yuan-giveaway-in-chinas-latest-lottery-test-2021-01-04.

Asian Development Bank Institute (2019). *Money and central bank digital currency.* URL: https://www.adb.org/sites/default/files/publication/485856/adbi-wp922.pdf.

Assange Julian, Appelbaum Jacob, Muller-Maguhn Andy, Zimmermann Jeremie (2016). *Cypherpunks: Freedom and the Future of the Interne.* Or Books Llc.

Australian Strategic Policy Institute (2020). *The flipside of China's central bank digital currency.* URL: https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency.

Banca d'Italia (2015). *Avvertenza sull'utilizzo delle cosiddette "valute virtuali".* URL: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf.

Bank for international Settlement (2019). *Investigating the impact of global stablecoins.* URL: https://www.bis.org/cpmi/publ/d187.pdf.

Bank for International Settlements (2020). *BIS encourages central banks to continue adapting to the challenge of digital payments.* URL: https://www.bis.org/press/p200624.html.

Bank of England (2014). *The economics of digital currencies.* URL: https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies.

Barontini Christian, Holden Henry (2019). *Proceeding with caution – a survey on central bank digital currency.* URL: https://www.bis.org/publ/bppdf/bispap101.pdf.

Barrdear John, Kumhof Michael (2016). *The macroeconomics of central bank issued digital currencies.* URL: http://smartledger.io/wp-content/uploads/2016/10/Staff-Working-Paper-No.-605-The-macroeconomics-of-central-bank-issued-digital-currencies-John-Barrdear-and-Michael-Kumhof-July-2016.pdf.

Basel Institute on Governance (2016). *Basel AML Index 2016 Report.* URL: https://baselgovernance.org/sites/default/files/2020-06/2016_report.pdf.

BBVA Research (2017). *Central Bank Digital Currencies: assessing implementation possibilities and impacts.* URL: https://www.bbvaresearch.com/wp-content/uploads/2017/09/WP_CBDC_mod.pdf.

Benigno Pierpaolo (2019). *Monetary Policy in a World of Cryptocurrencies.* URL: http://docenti.luiss.it/benigno/files/2007/01/Bitcoin-290819.pdf.

Bocchini Roberto (2017). *Lo svilpuio della moneta virtuale:primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche.* Diritto dell'Informazione e dell'Informatica (II) February 2017 p.27.

Boorstin Julia (2019). *Facebook launches a new cryptocurrency called Libra.* URL: https://www.cnbc.com/2019/06/17/facebook-announces-libra-digital-currency-calibra-digital-wallet.html.

Bordo Michael D., Levin Andrew T. (2017). *Central Bank Digital Currency and the Future of Monetary Policy.* URL: https://www.hoover.org/sites/default/files/research/docs/17104-bordo-levin_updated.pdf.

Brunnermeier Markus K., James Harold (2019). *The Digitalization of Money.* URL: https://www.bis.org/events/confresearchnetwork1909/brunnermeier_2.pdf.

Brunnermeier Markus K., Niepelt Dirk (2019). *On the Equivalence of Private and Public Money.* URL: https://www.bis.org/events/confresearchnetwork1909/brunnermeier.pdf.

Caloni Andrea (2020). *Deposito di criptoattività presso una piattaforma exchange: disciplina e attvità riservate.* Giurisprudenza Commerciale, October 2020, p. 1073.

Carstens Agustín (2019). *The future of money and payments.* URL: https://www.bis.org/speeches/sp190322.pdf.

Chapman James, Wilkins Carolyn A. (2019). *Crypto "Money": Perspective of a Couple of Canadian Central Bankers.* URL: https://www.bankofcanada.ca/wp-content/uploads/2019/02/sdp2019-1.pdf.

China Banking News (2018). *Digital Currency Research Institute of the People's Bank of China.* URL: https://www.chinabankingnews.com/wiki/digital-currency-research-institute-peoples-bank-china/.

Chiu Jonathan, Davoodalhosseini Mohammad, Jiang Janet, Zhu Yu (2019). *Central bank digital currency and banking.* URL: https://www.econstor.eu/bitstream/10419/197934/1/166660724X.pdf.

Ciphertrace Cryptocurrency Intelligence (2018). *Cryptocurrency Anti-Money Laundering Report.* URL: https://ciphertrace.com/cryptocurrency-anti-money-laundering-report-q4-2018/.

Clrarke Stephen V. O. (1967). *Central Bank Cooperation 1924-1931.* New York: Federal Reserve Bank of New York.

Davies Glyn (2002). *A History of Money: From Ancient Times to the Present Day.* University of Wales Press. ISBN: 9780708317174.

Del Castillo Michael (2019). *Visa Exits Facebook's Libra Cryptocurrency Group.* URL: https://www.forbes.com/sites/michaeldelcastillo/2019/10/11/visa-exits-facebooks-libra-cryptocurrency-group/.

Deutsche Bank (2019). *Imagine 2030.* URL: https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000503196/Imagine_2030.PDF.

Eichengreen Barry, Flandreau Gunnar (1999). *The Gold Standard in Theory and History.* London and New York: Routledge.

Europaen Central Bank (2015). *Virtual currency schemes – a further analysis.* URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

European Banking Authority (2013). *Warning to consumers on virtual currencies.* URL: https://eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%5C%20Warning%5C%20on%5C%20Virtual%5C%20Currencies.pdf?retry=1.

European Banking Authority (2014). *Opinion on virtual currencies.* URL: https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%5C%20Opinion%5C%20on%5C%20Virtual%5C%20Currencies.pdf?retry=1.

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

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

European Central Bank (2019). *Occasional Paper Series Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures.* URL: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

European Central Bank (2020a). *A digital euro.* URL: https://www.ecb.europa.eu/euro/html/digitaleuro.en.html.

European Central Bank (2020b). *Report on a digital euro.* URL: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

European Commission (2018a). *European countries join Blockchain Partnership.* URL: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-Blockchain-partnership.

European Commission (2018b). *The EU Blockchain Roundtable supports efforts to deploy blockchain technologies in the EU.* URL: https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-roundtable-supports-efforts-deploy-blockchain-technologies-eu.

European Commission (2019). *Launch of the International Association of Trusted Blockchain Applications - INATBA.* URL: https://ec.europa.eu/digital-single-market/en/news/launch-international-association-trusted-blockchain-applications-inatba.

European Commission (2020). *Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MICA).* URL: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF.

European Parliament (2015). *Virtual currencies.* URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_EN.pdf.

European Parliament (2020a). *Crypto-assets: Key developments, regulatory concerns and responses.* URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU%5C%282020%5C%29648779_EN.pdf.

European Parliament (2020b). *Speech by Executive Vice-President Valdis Dombrovskis.* URL: https://ec.europa.eu/commission/commissioners/2019-2024/dombrovskis/announcements/speech-executive-vice-president-valdis-dombrovskis-digital-finance-outreach-2020-closing-conference_en.

European Securities, Markets Authority (2015). *Call for evidence: Investment using virtual currency or distributed ledger technology.* URL: https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-532_call_for_evidence_on_virtual_currency_investment.pdf.

Fatiguso Rita (2020). *Yuan virtuale, la Banca del popolo in concorrenza con i privati.* URL: https://www.ilsole24ore.com/art/yuan-virtuale-banca-popolo-concorrenza-i-privati-ADlb5Hy.

Findings from a conference organised by SUERF (2018). *Do we need central bank digital currencies? Economics, Technology and Institutions.* URL: https://www.suerf.org/docx/r_ffd2257b586a72d1fa75f4ba2ad914e6_5175_suerf.pdf.

Fung Ben S. C., Halaburda Hanna (2016). *Central Bank Digital Currencies: A Framework for Assessing Why and How.* URL: https://www.econstor.eu/bitstream/10419/173375/1/sdp2016-22.pdf.

Gazdecki Andrew (2018). *Five Ways Blockchain Could Change The World.* URL: https://www.forbes.com/sites/forbestechcouncil/2018/09/07/five-ways-blockchain-could-change-the-world/?sh=42d033b73d70.

Gregori Gitti (2020). *Emissione e circolazionedi criptoattività tra tipicità e atipicità nei nuovi mercati finanziari.* Banca Borsa Titoli di Credito, February 2020, p. 13.

Huberman Gur, Leshno Jacob D., Moallemi Ciamac (2017). *Monopoly without a monopolist: an Economic analysis of the bitcoin payment system.* Bank of Finland.

Hui Ada (2020). *China Central Bank Official Reveals Results of First Digital Yuan Pilots.* URL: https://finance.yahoo.com/news/china-central-bank-official-reveals-220301197.html.

Ingham Geoffrey (2004). *The nature of money.* URL: https://www.econstor.eu/bitstream/10419/155831/1/vol05-no02-a2.pdf.

Kaplanov Nikolei M. (2012). "Nerdy Money: Bitcoin, The Private Digital Currency, and The Case Against its Regulation." In: *Loyola Consumer Law Review* 25.1, pp. 111–174.

Keynes John M. (1925). *Economic Consequences of Sterling Parity.* New York: Harcourt, Brace and Co.

Kharpal Arjun (2020). *China hands out $3 million of digital yuan as JD.com becomes first online platform to accept it.* URL: https://www.cnbc.com/2020/12/07/china-hands-out-digital-yuan-in-trial-as-jdcom-accepts-the-currency.html.

Koumbarakis Antonios, Dobrauz Guenther (2019). *Central Bank Digital Currency. Benefits and drawbacks.* URL: https://www.pwc.ch/en/publications/2019/Central%20Bank%20Digital%20Currency_EN-web.pdf.

Kraemer Christian, Nienaber Michael (2020). *Big European states call for cryptocurrency curbs to protect consumers.* URL: https://www.reuters.com/article/us-eu-economy-cryptoassets-idUSKBN26219G.

Lanz Jose Antonio (2019). *Colombia is slowly moving toward Bitcoin-friendly regulations.* URL: https://finance.yahoo.com/news/colombia-slowly-moving-toward-bitcoin-223024164.html.

Lee Amanda (2020). *China's digital currency trial returns to Shenzhen for round two, with twice the participants and double the payout.* URL: https://www.scmp.com/economy/china-economy/article/3116521/chinas-digital-currency-trial-returns-shenzhen-round-2-twice.

LenerRaffaele, FurnariSalvatore L. (2020). *Cripto-attività: prime riflessioni sulla proposta della commissione europea. Nasce una nuova disciplina dei servizi finanziari "crittografati"?* URL: https://www.dirittobancario.it/approfondimenti/fintech/cripto-attivita-prime-riflessioni-sulla-proposta-della-commissione-europea-nasce-una-nuova-disciplina.

Malta (2018). *Digital Innovation Authority Act.* URL: https://legislation.mt/eli/bill/2018/45/eng/pdf.

McIntosh Rachel (2019). *Will 2020 Be the Year of the CBDC?* URL: https://www.financemagnates.com/cryptocurrency/news/will-2020-be-the-year-of-the-cbdc/.

Murphy Austin (2008). *An Analysis of the Financial Crisis of 2008: Causes and Solutions.* URL: https://ssrn.com/abstract=1295344.

Muth Tomoko (2021). *Building a digital assets corridor between Switzerland, Japan and Singapore.* URL: https://www.swissinfo.ch/eng/business/building-a-digital-assets-corridor-between-switzerland--japan-and-singapore/46283590.

Nakamoto Satoshi (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* URL: https://bitcoin.org/bitcoin.pdf.

NisticòSalvatore (2019). *Criptovalute, sovranismo e sistema monetario.* URL: http://www.diss.uniroma1.it/sites/default/files/allegati/DiSSE_Nistico_wp8_2019.pdf.

Office of the Comptroller of the Currency (2020). *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities.* URL: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf.

Panetta Fabio (2020). *We must be ready to create a digital euro.* URL: https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog201002~12ab1c06b5.en.html.

PayPal (2019). *PayPal response to the European Commission's public consultation.* URL: https://www.tbstat.com/wp/uploads/2020/07/PayPal.pdf.

Pfister Christian (2019). *Central Bank Digital Currency: One, Two or None?* URL: https://publications.banque-france.fr/sites/default/files/medias/documents/wp-732.pdf.

Pitta Julie (1999). *Requiem for a Bright Idea.* URL: https://www.forbes.com/forbes/1999/1101/6411390a.html?sh=38dcaaf1715f.

Polk Davis (2015). *New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal.* URL: https://www.davispolk.com/sites/default/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf.

Pronina Lyubov (2018). *EU Tells Malta to Step Up Crackdown on Money Laundering by Banks.* URL: https://www.bloomberg.com/news/articles/2018-11-08/eu-tells-malta-to-step-up-crackdown-on-money-laundering-by-banks.

Rimkus Ron (2016). *The Financial Crisis of 2008.* URL: https://www.econcrises.org/2016/08/17/the-financial-crisis-of-2008/.

Ryan Andrea, Trumbull Gunnar, Tufano Peter (2011). *A Brief Postwar History of U.S. Consumer Finance.* Business History Review 85.

Scammell William M. (1965). *The Working of the Gold Standard.* Yorkshire Bulletin of Economic and Social Research.

Stevens A. (2017). *Digital currencies : Threats and opportunities for monetary policy.* URL: https://www.nbb.be/doc/ts/publications/economicreview/2017/ecorevi2017_h5.pdf.

The Economist (2020). *The COVID-19 crisis is boosting mobile money.* URL: https://www.economist.com/middle-east-and-africa/2020/05/28/the-covid-19-crisis-is-boosting-mobile-money.

The Law Library of Congress (2018). *Regulation of Cryptocurrency Around the world.* URL: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

Tudor-Ackroyd Alison (2020). *What will China's central bank digital currency mean for Alipay and WeChat Pay?.* URL: https://www.scmp.com/business/banking-finance/article/3100285/what-will-chinas-central-bank-digital-currency-mean-alipay.

Wolfson Rachel (2018). *Maltese Parliament Passes Laws That Set Regulatory Framework For Blockchain, Cryptocurrency And DLT.* URL: https://www.forbes.com/sites/rachelwolfson/2018/07/05/maltese-parliament-passes-laws-that-set-regulatory-framework-for-blockchain-cryptocurrency-and-dlt/?sh=14e2f1b649ed.

World Economic Forum (2019). *Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today?* URL: http://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf.

Yue Eddie (2020). *A New Trend for Fintech - Cross-border Payment.* URL: https://www.hkma.gov.hk/eng/news-and-media/insight/2020/12/20201204/.

Zetzsche Dirk A., Annunziata Filippo, Arner Douglas W., Buckley Ross P. (2020). *The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725395.

Zetzsche Dirk A., Buckley Ross P., Arner Douglas W. (2019). *Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414401.

Zupi Marco (2017). *Venezuela: ultimi sviluppi.* URL: http://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/note/PI0074Not.pdf.

Abstract

The different means of payment, and in particular money, in the course of their evolutionary history, have had the characteristic of influencing all the dimensions of collective and individual work, thus obtaining a profound impact on the human societies that use them.

The currency was not born in a day but is the result of a long process of evolution of the means of payment, determined by the search for more effective methods to facilitate trade. Once the currency did not exist, people in that period lived in small settlements, grew vegetables and raised livestock. The human needs for the exchange of goods have led to the search for quantifiable and lasting means to carry out this exchange, or as it is better known: barter.

Over time, however, the need for an item that was generally accepted in exchange for goods and that was easy to handle began to grow. This is how money was born. Over the centuries, many different objects have been used as money. Livestock, salt, as well as pearls and shells were once used in a similar way to our coins and bills.

With the passage of time, the usefulness of the old means of exchange diminished when the metal was discovered, as it was a scarce and difficult to find commodity, its shelf life was much greater, it did not disappear when consumed and could be segregated into small pieces. It should be noted that the metals whose importance and use transcended others were gold and silver, which would form the basis for forging the new means of payment: money.

Of course, people who had money wanted to keep it safe. Goldsmiths have

always had a safe home for fear of theft, this is why they often acted as cashiers and for a fee they took coins and other valuables for safekeeping for others. The Goldsmiths had a book in which he wrote how much money he kept and for whom. Customers of course received a receipt and could later exchange that receipt for their own money. Soon people, thanks to the ease of use, started paying each other with these receipts just like we do today with bills. Paper money, initially convertible into metallic currency, are finally transformed into “fiduciary” or “fiat currency”.

The heyday of gold in the monetary system lasted from 1870 until the outbreak of the First World War. During this period, a worldwide fixed exchange system was established based on a fixed exchange of individual currencies in relation to gold and clear rules for redemption and hedging of gold.

In the interwar period, some countries sought to further extend gold reserves by introducing the gold bar base, under which only amounts corresponding to full gold bars could be redeemed. Gold therefore played only a limited role for the individual citizen, but was nevertheless the guiding principle of the monetary system. In the early 1930s, more and more countries had to abolish gold conversion.

After World War II, the Bretton Woods system was established, in which currencies were pegged to the dollar or directly to gold. In general, the redemption of gold was now limited to central banks. The Bretton Woods system collapsed in 1971. Most central banks today still hold gold as part of the foreign exchange reserve, but gold’s share of total foreign exchange reserves has decreased.

The genesis of cryptocurrencies stems from the cypherpunk movement of the early 1990s. The cypherpunk dream of an electronic currency foreign to any government or institution seemed like a utopia. However, an event set the stage for that dream to come true. That event was the 2008 financial crisis.

A global economic crisis erupted in 2008 following the collapse of the financial market in the United States. The origin of this crisis is mainly due to the fact that

in the early 2000s, banks and financial institutions created subprime mortgages as a type of structured financial product to obtain large economic benefits from what was initially believed, very low risk. These were variable rate mortgages aimed at users with bad credit histories and precarious financial resources, for that these users were at high risk of default in the payments of these mortgages.

Two weeks after the Lehman Brothers bankruptcy, a cryptographic mailing list user whose true identity still remains a mystery, Satoshi Nakamoto, published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" proposing a computer protocol to create the first cryptocurrency.

Cryptocurrencies have a number of advantages over the current financial system. First of all, the Blockchain system makes the transaction costs practically free and the transfer of value is instantaneous, while transactions in the financial system are subject to high percentage fees and charges, and due to centralization, validating a transaction or transfer takes much longer.

Cryptocurrencies have the ability to make transfers regardless of the size of the transfer, for example, it is possible to send five or ten dollars from one account to another in different continents while, in the current financial system, the same transfer would not be possible for the high percentage of commission charged by the intermediary financial institution of the transaction.

The second benefit provided by cryptocurrencies is that it would allow millions of people who don't have a bank to participate in the financial market. By not asking for any kind of requirements, this would make it easier for millions of people to be able to make money transfers.

The third advantage that cryptocurrencies offer is the privacy to its users in their purchases, as they act in a similar way to cash. The fourth advantage that cryptocurrencies provide through its Blockchain system is transparency and security in transactions since all these are stored in a public ledger that is replicated in all nodes of the network.

Finally, many cryptocurrencies are resistant to inflation since, like gold or

silver, there are a finite number of them, unlike fiat money which can be printed indefinitely by a central bank.

All of the above features make this technology ideal for money transfer, but this is only the first application that has been used for this new technology.

Unfortunately, cryptocurrencies are not always used for legal purposes, in fact, today they are the most efficient tool for illegal transactions. Cryptocurrencies are more efficient for recycling even than cash due to the great ease and speed of movement that cash cannot possibly have in the face of an almost comparable level of anonymity.

Cryptocurrencies are currently going through a period of accelerated growth, as, together with the Blockchain, they have demonstrated their high potential. However, they have proved impractical in common use for several reasons, mainly due to the volatility of their price.

The stablecoins have been introduced to contain price movements and bring some stability to a market that has, up to now, been quite difficult to control.

A stablecoin is a cryptocurrency with a fixed price, i.e. it maintains a constant value with respect to a target price. The price of most cryptocurrencies is determined by the market, on the contrary, stablecoins aim to maintain a fixed price which must be maintained through different mechanisms.

The stablecoins are therefore a very interesting proposal because, maintaining all the advantages of the Blockchain, they provide the necessary stability that makes them usable in real life.

Now, as cryptocurrencies can be used for the commission of crimes, countries to solve this new problem have taken different positions that can be grouped in three different ways of dealing with: inaction, prohibition and regulation.

The first paper issued by the European Union in which reference is made to cryptocurrencies dates back to 2012 with the paper entitled “Virtual Currency Scheme”. With this paper, the legislator warns European countries of the possible risks associated with this new type of digital currency, urging them to find

adequate regulation. The text explains how people who use Bitcoin are often linked to the Austrian school. This school of thought criticizes fiat money subject to government decisions and, although it is based on the use of the gold standard, people who use Bitcoin see it as a first step in removing the monopoly from Central Banks regarding monetary policy decisions.

Through this paper, the ECB shows that it is afraid that cryptocurrencies could negatively interfere with the demand and use of legal tender, but explains that problems would arise only if Bitcoin began to be used on a large scale. While the ECB is clearly very concerned, it states that due to the decentralized nature of the system, cryptocurrencies are impossible to block.

Cryptocurrencies continue to gain popularity among people on the internet also due to the economic crisis that is shaking the whole world. This prompts the European Banking Authority 26 to publish two new papers in 2013 and 2014 entitled respectively "Warning to consumers on digital currencies"and "Opinion on virtual currencies".

The first paper is not very long but draws attention to the risks associated with the purchase, possession and exchange rate of cryptocurrencies.

Above all, the risk that users run due to exchanges is emphasized. In fact, the exchange platforms, not being banks that store cryptocurrencies and, not being regulated, can cease their activity without notice. The reasons can be various, from scams to cyber attacks, and all of this results in a loss on the part of users who held cryptocurrencies deposited on those exchanges.

One year after the publication of the paper seen previously, the EBA publishes the second paper entitled "Opinion on virtual currencies".

Basically, compared to the previous paper, the EBA now focuses on the advantages that cryptocurrencies can bring to the modern economic system without neglecting some criticisms.

An example can be the cheapness and speed of transactions. The EBA, in fact, mentions the settlement in virtual currencies which takes place within 60

minutes, 24 hours a day, every day, against the 24-hour execution deadline and the general availability of 5 bank days out of 7 within SEPA.

While these benefits are praised, the EBA argues that the slowness and cost of traditional transactions are justified by the security that the banking system offers its customers. Moreover, the EBA explains that the cost-effectiveness of transactions is canceled out as, to return to a fiat currency, you have to pay commissions for the conversion of cryptocurrencies.

After years of research the Blockchain is considered a disruptive technology, which could provide opportunities for innovation in the administrative procedure, including local ones. The interest in the use of these technologies in the public sector is evident in the important Declaration on Cooperation in a European Blockchain Partnership, signed on 10 April 2018 by twenty-one member states of the European Union and to which six other states have subsequently joined.

In the Declaration, the signatory states recognize the potential of Blockchain for the transformation of digital public services in the European Union, pledge to work together to realize the potential of Blockchain-based services for the benefit of citizens, society and the economy and secure specific objectives for the Association.

On April 3, 2019 in Brussels, Belgium, a new association created by the European Commission is founded, called the International Association for Trusted Blockchain Applications (INATBA). INATBA's goal is to offer developers and users of Blockchain technology a global space to interact with regulators and policy makers, in order to "take Blockchain technology to the next stage". The goal is to integrate more startups, small and medium-sized enterprises, as well as political leaders, international organizations, regulators and members of civil society. In this way, it is intended to establish a dialogue with public authorities and regulators, in order to promote the convergence of the legal frameworks that apply to the Blockchain around the world.

The European Union wants to regulate cryptocurrencies and to do so, the

European Commission published on 24 September 2020 the first proposal for a regulation for cryptocurrencies, in particular stablecoins, which will be applied in the member countries of the European Union. Called MICA, it finally answers the big questions posed by the blockchain ecosystem and the cryptocurrencies.

MiCA regulation is intended to regulate licensing requirements, supervisory powers and general cryptocurrency trading in the future. In this context, the European Commission basically distinguishes between the so-called MiFID (Markets in Financial Instruments) and MiCA (Markets in Crypto Assets). This specific regime would also reassure large companies, institutions and large investors.

The project plans to create a team of supervisors with national authorities and EU bodies. These teams will be chaired by the European Banking Authority, an entity that will take a greater role in controlling the cryptocurrency industry.

The supervisory bodies will be the National Central Authority of the member State, the European Securities and Markets Authority and the European Central Bank. They will be tasked with reviewing the functioning and use of significant cryptocurrencies. The regulation will be applied on a large scale, imposing stricter rules, in terms of obligations, supervision and sanctions, on cryptocurrencies deemed risky.

The proposal states that cryptocurrency developers must produce a white paper with all relevant information about the issuer, token or trading platform to enable potential buyers to make an informed purchase decision and understand the risks associated with the offering.

This paper is central because the MiCA permits the public offering of crypto assets or their admission to a trading platform only if such white paper has been created, published and not contested by the supervisor in accordance with the newly created requirements. Authorities may prohibit the issuer from trading in the market if the white paper or issuer does not meet the requirements of the MiCA.

The MiCA states in article 43 that issuers of “significant e-money tokens”

(such as the Diem Association) will have stricter supervision. In fact, to issue the tokens, they must be approved as a credit institution or e-money institution and must comply with some requirements of Directive 2009/110/EC ("E-Money Directive").

Under the proposal, national laws for crypto assets, which have been put forward by countries like Germany, France and Malta, should operate under these EU rules.

This is how the European Commission intends to provide legal certainty, support innovation and protect consumers and investors, as well as ensuring financial stability and market integrity in the EU.

In addition to the new regulation on cryptocurrencies and their issuance, the services and activities related to them will be subject to state supervision in the future.

Bitcoin has brought to the world the ability to transfer digital value globally without the need for intermediaries, without asking for permissions and without censorship. Many have wanted to replicate this idea by creating other cryptocurrencies. The world's Central Banks, some to a greater extent than others, have underestimated these experiments, posing small obstacles, but without a coordinated international attack to show their concern, until Facebook announced Libra (now called Diem).

Investigations into CBDC have been ongoing since at least 2014, when the scenario was established by the Bank of England 3 . Since then, several Countries and organizations have investigated this possibility, created prototypes and conducted tests.

But it was only when Facebook announced Libra that Central Banks realized the inevitability of the ongoing change and the need to step in and reignite the CBDC debate.

The practical implications of implementing CBDC are profound, not just for users but for the entire financial structure.

Since Central Banks are institutions whose primary responsibility is to ensure economic stability, it is not possible to take the liberty of making drastic and imprudent decisions.

Central Bank digital currency would be a more flexible and programmable form of Central Bank money and, depending on how it is designed, could both maintain cash anonymity and eliminate the need for financial intermediaries, such as increasing the supervision and monitoring of private monetary policy, maintaining the presence of private banks. In addition, it could imply digital cash subject to interest rates, a greater monopoly of the Central Bank's financial activity and more instruments for its monetary policies.

Current literature and research on the subject contemplates the use of distributed databases such as those used in Blockchain networks such as Bitcoin for the technical architecture of CBDCs. The main difference from Bitcoin would be that decentralization would not be desirable. Rather, network security and transaction verification would be the sole responsibility of the Central Bank and, in any case, of the bank's trusted institutions.

Depending on the goal to be achieved with the CBDC, its potential attributes vary. For example, as regards its scope, it could be universal/retail, in the event that its use is open to anyone, or limited/wholesale, when its use is limited to financial intermediaries.

In the universal case, the CBDC could allow any person or business to make electronic payments using money issued by Central Banks using the means of payment provided by the institution, as well as deposit their money directly into their accounts. The Central Bank would then become the custodian and provider of legal tender digital money services.

In the limited case, the reality would not be much different from what it is today for individuals in their daily lives, even if they could benefit from improvements in the efficiency of banking institutions.

To analyze the implications of CBDCs in the traditional financial system,

BBVA researchers proposed four possible scenarios:

- The first option would be a scheme where the use of CBDCs is limited to financial intermediaries. This scenario would increase the efficiency of the wholesale payment system, would not change monetary policy making and could increase competition for banks from non-bank payment institutions;
- The second option opens the CBDC to the general public, maintains the anonymity of cash based on a token system. The efficiency gains outweigh those of the first option by eliminating financial intermediaries from money transfers. Its role would be reduced to other financial services such as credit and loans, although its capacity would be weakened;
- The third option introduces the possibility of CBDC with interest rates. This option focuses on increasing the scope of monetary policies. It involves the total elimination of cash, which has high costs in educational processes and in the distribution of devices;
- The fourth option raises a universal CBDC linked to identifiable accounts. It would be like having an account in a Central Bank. This would increase the supervisory powers of the monetary authority over individuals but this would risk that, in times of instability, individuals turn to the Central Bank and not to private banks that would find themselves in trouble.

Due to the conservative bias of Central Banks, it is very likely that the first option will be the first to be implemented in the short term. Central Bank digital currencies (CBDCs) present many challenges, so their implementation has been quite limited, although it has been extensively studied.

While central banks are studying ways to implement their cryptocurrency, Facebook is already one step away from launching their own stablecoin.

Diem (ex-Libra) is the name given to the future cryptocurrency initiated by Facebook. “The Libra mission is to enable a simple global payment system

and financial infrastructure that empowers billions of people.", summarizes the project's white paper, which was revealed on June 18, 2019.

In other words, it is a new currency, totally digital, supported by a Blockchain, already used by other digital currencies such as Bitcoin. The Diem cryptocurrency will be based on a "permission" Blockchain, which means that access to the protocol must be validated, unlike the Bitcoin Blockchain which is open to everyone.

The Diem will be a stable currency, i.e. a stablecoin, and it will be traded instantly as it will not have to go through the banking network. In addition to a Diem backed by a basket of currencies, there will be several Diems: a USD Diem, a EUR Diem, a GBP Diem, and an SGD Diem. "We hope to work with regulators, Central Banks, and financial institutions around the world to expand over time the number of single-currency stablecoins available on the Diem network" reads the updated white paper.

Contrary to what one might think, Facebook is not alone in this project. The Diem association, responsible for the development and proper functioning of the network, is currently composed of 21 founding members, who form the Council of Diem, a sort of Parliament of this new institution based in Geneva (Switzerland).

The European Central Bank is also very interested, in fact, in October 2020 through a paper, titled "A digital euro", revealed the first decisions on the matter. Christine Lagarde also stated:

> *"The euro belongs to Europeans and we are its guardian. We should be prepared to issue a digital euro, should the need arise."*

The paper states that the ECB has come to the conclusion that most of the desirable features of the digital euro could meet the emerging payment needs of a modern economy by offering, alongside cash (which the EU does not want to abolish), a secure digital asset with advanced features.

Many states are studying the issuance of a CBDC but there is one in particular

that is in a very advanced state: China.

The digital yuan, also known as DCEP, is a new virtual version of the yuan, China's national currency. The country has been working on it for years and has clearly stepped up its efforts in 2020 so that it can be the first country in the world to make CBDC its official currency, a perfect replacement for physical currency. Researching and evaluating central bank digital currencies since 2014, China set up the "Digital Currency Research Institute" in 2017, then launched a series of tests in 2020.

The digital yuan in China is making encouraging progress and has already covered more than 6,700 payment scenarios, according to the country's deputy central bank governor, Fan Yifei. The tests integrated seamlessly with existing payment methods such as QR codes and NFCs. According to Fan Yifei, more than 120,000 personal and business digital wallets have been created for the digital yuan since testing began.