UCLouvain

LOUVAIN
School of Management

Louvain School of Management

Cryptocurrencies: a disruptive innovation.

Focus on the impact of a potential development of this technology in the economy.

Author : Gregory Ackermans
Advisor : Bruno Colmant
Academic Year 2018-2019

I would like to thank my thesis advisor, Bruno Colmant, for his support and great advices all along the redaction of this graduate thesis. His knowledge and experience represent a true source of inspiration to me.

I would also like to thank my family and friends who always believed in me and supported me during this thesis.

I would like to grant a special thank you to all the colleagues I had the chance to meet during my internship at Deloitte. Thank you for the great conversations we had around cryptocurrencies and for the valuable advices they provided me.

Finally, I would like to thank all the people who contributed to my development and personal improvement during this master in management sciences.

TABLE OF CONTENT

INTRODUCTION 1

PART I. UNDERSTAND CRYPTOCURRENCIES 3

CHAPTER 1. WHAT ARE CRYPTOCURRENCIES? 3
1.1. DEFINITION 3
1.2. TYPES OF CRYPTOCURRENCIES 4
CHAPTER 2. HOW IT WORKS 8
CHAPTER 3. CONDITIONS FOR BEING A CURRENCY 10
3.1. HISTORY OF MONEY 10
3.2. ROLES OF MONEY 12
CHAPTER 4. A TECHNICAL INNOVATION 14
4.1. BLOCKCHAIN OUTLOOK 15
CHAPTER 5. A MONETARY INNOVATION 17
5.1. CASH MONEY 17
5.2. CREDIT AND DEBIT CARDS 18
5.3. E-TRANSFERS 19
5.4. ONLINE PAYMENT PLATFORMS 19
5.5. CRYPTOCURRENCIES' ADDED VALUE 20

PART II. DEVELOPMENT OF CRYPTOCURRENCIES 24

CHAPTER 1. CURRENT STATE OF DEVELOPMENT 24
1.1. DRIVERS OF DEMAND 24
1.2. DRIVERS OF SUPPLY 26
1.3. COMPANIES AS EARLY ADOPTERS 28
1.4. FINANCIAL INSTITUTIONS AS EARLY ADOPTERS 29
1.5. GOVERNMENTS AS EARLY ADOPTERS 32
CHAPTER 2. A CHANGING ENVIRONMENT 34
2.1. NEW VALUE PROPOSITION 34
2.2. NEW TYPES OF CUSTOMERS 36
2.3. EMERGENCE OF FINTECH 36
2.4. GAFA ENTERING THE GAME 37
CHAPTER 3. USE CASE: CENTRAL BANK CRYPTOCURRENCIES 40

PART III. IMPLICATIONS **43**

CHAPTER 1. MACROECONOMICS EFFECTS **43**
1.1. ECONOMIC EFFICIENCY 44
1.2. FINANCIAL STABILITY 45
1.3. FISCAL POLICIES 48
CHAPTER 2. CHALLENGES **50**
2.1. REGULATION 50
2.2. ILLICIT ACTIVITIES 52
2.3. USER PRIVACY AND PROTECTION 55
2.4. VOLATILITY 56
CHAPTER 3. TECHNICAL LIMITS **58**
3.1. ELECTRICITY CONSUMPTION 58
3.2. INFRASTRUCTURES OVERLOAD 60
3.3. CYBER RISKS 63

CONCLUSION **66**

REFERENCES **69**

INTRODUCTION

Since their development in 2008, cryptocurrencies have raised a lot of questions and concerns. This new payment method arose in respond to the financial crisis as a solution against mistrust in financial institutions and inefficient processes. Cryptocurrencies came as an alternative to current payment processes often defined as too slow, too expensive, too risky and surrounded by rigid institutions. The development of this new payment method and its underlying technology bursts in a period characterized with key changes in the environment. The increasing digitalization of money, the changes in customers' expectations and the emergence of new players on the market have amplified the urgency to come up with new ways of transacting.

Together with strong technological innovations, the phenomenon has led to the creation of new ways to conceptualize and use money. Cryptocurrencies represent an unprecedented change in the paradigm of payments. The technology has the power to disrupt the whole payment ecosystem and indirectly the whole financial sector by questioning the role of financial institutions.

Satoshi Nakamoto's[1] dream of a revolutionary peer-to-peer payment system promises to offer key benefits allowing to improve the overall efficiency of payments and provide a more convenient way to settle transactions all round the world. However, the technology also has a considerable number of drawbacks that may have some important impacts if it was adopted globally. Such changes in the financial ecosystem also involves a lot of implications on multiple aspects of the economy and society.

The disruptive potential of this new technology pushed me to analyse more into details the different impacts and limits that we would face if cryptocurrencies were adopted more widely as an alternative payment method. In a period characterized by important changes in our way of living and exchanging, it is absolutely essential to understand the full scope, potential and implications underlying cryptocurrencies. It is key to take a step back from the mediatic

[1] Bitcoin's founder.

attention of Bitcoin in order to have a clear view on what cryptocurrencies really are and to what extent they might disrupt the current financial system.

Therefore, the first part of this thesis will focus on defining cryptocurrencies and understanding why they represent a disruptive innovation compared to the current payment system. We'll have a broader explanation on the different kinds of cryptocurrencies that exist in order to have a better idea of the full scope of this new type of currencies. This first part will also take a more technical perspective by explaining how cryptocurrencies work and how promising is the underlying technology, the blockchain. In order to talk about the impact of cryptocurrencies, it is first important to understand how cryptocurrencies are currently evolving and what may drive their further development. The second part of this thesis will hence focus on the current state of development by explaining what drives supply and demand for cryptocurrencies, and by presenting the multiple parties who already adopted the technology. This theoretical and practical background will thus allow us to deep dive into the whole implications arose in case of a future development of cryptocurrencies. The last part will focus on some key macroeconomic effects that will need to be monitored closely if such changes happened. We'll then go through the most problematic challenges that cryptocurrencies are facing and we'll try to understand to what extent these challenges might have an impact on our ways of exchanging goods and services. Finally, this last part will discuss about some key technical limits of cryptocurrencies that might affect the economy and its individuals if cryptocurrencies were adopted as an alternative medium of exchange.

In order to be able to deliver the best analysis as possible, this thesis leans on a great quantity of reports, literatures and scientific articles coming from financial institutions, governments and other highly valuable sources. Moreover, the facts and affirmations stated in this thesis are usually backed by relevant statistical analysis retrieved from reliable scientific databases. However, it is important to keep in mind that this thesis discusses the "potential development" of cryptocurrencies. Since the technology is still in an early development stage, it is hard to be able to predict exactly how and where cryptocurrencies will develop. Hence, the analysis of the potential implications will remain quite global in order to cover the different options of development. The reader will be provided with insights on the impacts of cryptocurrencies based on critical analysis of scenarios that are likely to happen and will be able to understand to what extent cryptocurrencies represent a disruptive innovation in the economy.

PART I. UNDERSTAND CRYPTOCURRENCIES

This first part will focus on defining cryptocurrencies and have a better idea of how the technology really works. We will also analyse some key questions in order to determine if cryptocurrencies can be considered as currencies and if they have the potential to be used as so. We will then see to what extent cryptocurrencies can be considered as an innovation by comparing their benefits with the current payment methods.

Chapter 1. What are cryptocurrencies?

1.1. Definition

When it comes to defining cryptocurrencies, here comes a lot of different definitions and interpretations. Most people usually generalize Bitcoin's definition for all cryptocurrencies even though it represents only one of many types of cryptos. In order to understand what cryptocurrencies are, let's define them as a set of three characteristics. (BIS, 2018)

The first characteristic defines cryptos as a type of virtual currency, meaning that they are created, stored and used digitally. They are actually the electronic representation of fiduciary currencies, with the only difference that they don't have any legal status for exchange.
The second characteristic is that most cryptocurrencies are supported by a decentralized system, meaning that tokens[2] are transferred electronically via a peer-to-peer network. In other words, tokens are not issued and stored in a central bank. This means that transactions can be done between two individuals without the intervention of a financial institution as counterparty. Of course, this pattern has a lot of implications and arouse many debates regarding the role of financial institutions, which will be covered later in the document.
Finally, the last characteristic (maybe the most important one) is that the issuing and usage of cryptocurrencies rely on cryptography. It means that transactions are supported by cryptographic algorithms allowing online transactions of value to be performed in a safe and open environment. This actually represents one of the biggest innovation patterns of cryptocurrencies and is probably the best way to avoid tokens to be counterfeited.

[2] Tokens are digital assets representing a unit of value in a specific blockchain network or environment.

Providing a full definition of what cryptocurrencies are is not an easy task. Indeed, in addition of the three basic characteristics mentioned above, cryptos can also be classified according to different factors.

1.2. Types of cryptocurrencies

One single definition is not enough to be able to understand the full scope covered by cryptocurrencies. They can be found in lot of different declinations depending on the features they adopt. In order to have a clear view on the different types of cryptocurrencies, we can classify them according to three important factors; their global architecture, their underlying technology and the goal they try to seek.

Global architecture

The global architecture is probably the most important factor allowing to differentiate cryptocurrencies. Their architecture mainly defines the level of decentralization they have. The cryptocurrency can have a high level of decentralization if it lies on the blockchain technology. However, what is usually misunderstood is that all cryptos don't necessarily rely on blockchain and are therefore not always decentralized. Some of them are also supported by a centralized network, meaning that they are controlled by one single entity, whether it's a financial institution or a private company. The figure 1 above illustrates how the information is stored in a centralized network and in a decentralized network. (Mitchell, 2018) The centralized network has its information stored and maintained centrally by a responsible counterparty. The central entity can decide to share the information or not. The decentralized system has additional nodes where information is stored and can be sent from one party to another without the intervention of the central entity.

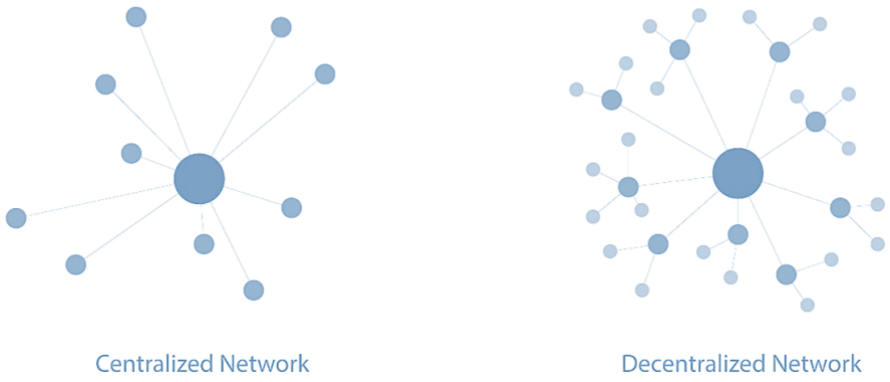


Figure 1: Difference between a centralized and a decentralized network

Underlying technology

The second important factor that allows to classify the different types of cryptocurrencies is according to their underlying technology. Their underlying technology will typically depend on three differentiating features; the level of permission, the level of privacy and their protocol.

The first differentiating feature of the underlying technology is to know if the crypto is permissionless or permissioned. In other words, that means defining if the crypto is respectively public or private. Typically, a cryptocurrency will be permissionless when anyone is allowed to keep a replica of the transaction record (known as "ledger") and is allowed to add new data to the record. On the other hand, it will be permissioned or private if only authorized stakeholders are allowed to maintain the ledger and add new transactions to it. Those stakeholders could be any party owning the system or involved in its functioning, such as illustrated on Figure 2 below. (BIS, 2018) However, it is important to mention that it's not because a crypto is permissioned that it necessarily can't be traded on exchange. The ability to be traded is actually an important condition that allows to define cryptocurrencies as a currency.

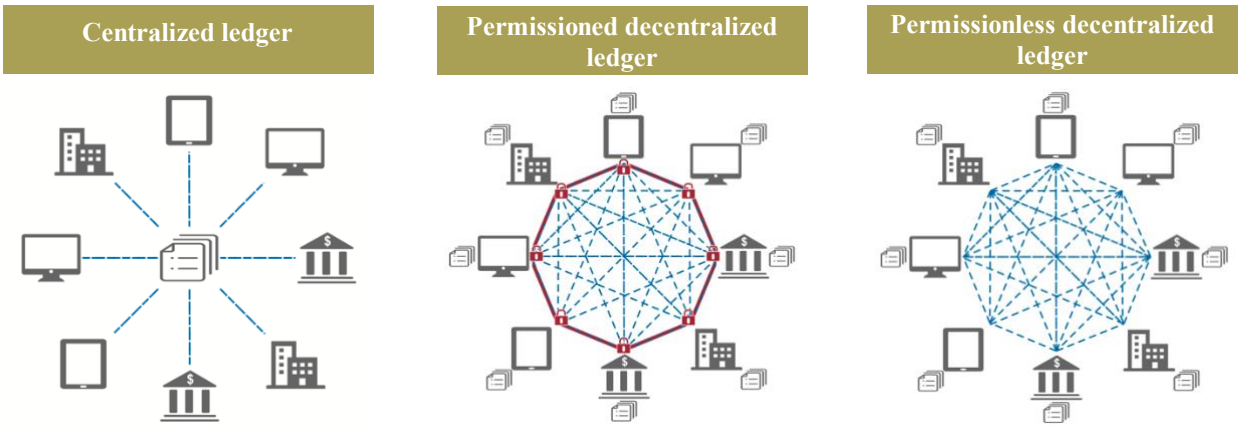


Figure 2: Difference between permissioned and permissionless ledgers in a network

A second differentiating factor of the underlying technology of a crypto is the level of anonymity provided to the users. That is to which level a transaction history can be tracked to the individual user. There are actually multiple ways to ensure the anonymity of users. The most simple and common way is to use pseudonyms to hide one's real identity. This technique is used on nearly all networks to allow users to make transactions in an anonymous way.

Another way to ensure a higher level of privacy will depend on how complex is the underlying cryptography. In other words, how hard it is to trace the details of a transaction.
As an example, the cryptocurrency Monero is known for providing digital cash for transactions in a really secured and untraceable way through a complex cryptographic process. (Monero, 2019)
Finally, cryptocurrencies can also differ in terms of protocol[3] used by their blockchain, in terms of techniques used to encrypt information but also depending on the type on information that is shared.

Specific goals

The last factor that allows to classify the different types of cryptocurrencies is according to the specific goal they seek. Indeed, all cryptos are designed for a specific purpose, while all above characteristics are mainly there to support these goals. Their design aims at tackling a specific problem and can be found in five different categories.

The first and most known one is the whole *digital cash coins* family including for example Bitcoin, Monero, Litecoin or Bitcoin Cash. Those are what most people associate with cryptocurrencies since they represent a digital alternative for cash money and are usually out of the control of financial entities and governments. Their goal is to provide an alternative currency for users to perform transactions in a digital way with focuses on anonymity and execution speed.

The second category are all *payment infrastructure tokens* such as Ripples, Utiliy Settlement Coin or Particl. Those are infrastructures supporting transactions in both cryptocurrencies and traditional currencies. Their key characteristic is to allow real-time and cost-efficient payments and can be profitable to both users and financial institutions. One of the best examples of this category is Ripple, a payment infrastructure using blockchain technology to provide real-time and cost-efficient transactions. The core principle of this infrastructure is based on the so-called IOU (I owe you) concept. In practice, when a buyer A executes a transaction on the platform, the amount of money sent (whatever the currency) is automatically transformed into the equivalent of the platform's native cryptocurrency XRP, named "ripples". The seller B will receive the XRP amount in his wallet and can decide to have it transformed into whatever

[3] A protocol is the foundation code that defines how a specific blockchain network will work. Cryptocurrencies using blockchain all have a specific and unique protocol defining their rules of functioning.

currency he/she wants for the equivalent amount. The platform's native cryptocurrency plays the role of an intermediary allowing to execute transactions with lower costs and improved speed compared to conventional financial infrastructures. (Halaburda & Sarvary, 2016)

The third category are *utility tokens* such as Golem, Timicoin or Brickblock. They account for a unit of value providing the access to distinct goods or services proposed by an entity. As an example, Golem is a decentralized peer-to-peer network regrouping computers with unused computing power. The platform's native tokens GNT (Golem Network Tokens) allow users to buy or sell unused computing power on the network in a reliable, cheap and fast way. (Golem, 2019) Another example of utility token are the ones used by Timicoin, a decentralized network allowing to share healthcare information of patients in a safe and efficient way. Timicoin uses blockchain technology to create a safe and open-sourced ledger of patients' health data to which authorized users can contribute. The platform's utility tokens TMC will be used by permissioned users to request for health data on the decentralized network. (Timicoin, 2018) Utility tokens are also heavily involved in ICO's activities in order for businesses to "tokenize" part of their equity for capital raising. An ICO (Initial Coin Offering) is a digital way for companies to raise funds through the issuing of digital assets. Typically, companies willing to raise money will issue tokens representing the value of a good or service they provide. Those tokens can then be sold as a unit of account for a future good or service providing. ICO's are often compared to IPO's (Initial Public Offering) with the main difference that tokens issued doesn't account for any shares of the issuing company.

The fourth category are *securities tokens* such as RMG or Maecenas. Those are tokens representing a unit of value of a physical asset and supporting users in various trade activities. The difference between utility tokens and securities tokens is quite thin but is important to be made since securities are subject to specific regulations and requirements. The difference will be made with the "Howey Test" that will define a token as a securities token if "a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party". (Prisco, 2019) One very interesting example of securities tokens are the ones traded on Maecenas. The latter is a Fine Art platform using blockchain technology to allow investors, collectors and galleries to finance their art investments via a network of permissioned investors. A piece of art will account for a certain amount of the Maecenas's native tokens "ART", therefore providing the art piece with a digital financial value. On one hand, users willing to raise money will put some of their art pieces as a collateral on the

platform, while on the second hand, investors will be able to diversify their portfolio by investing in stakes from different artworks – represented by ART tokens. This decentralized marketplace allows to bypass traditional intermediaries and therefore be more cost-efficient. (Maecenas, 2019)

The last category are the *general platform tokens* used on platforms such as Ethereum or NEO. Those platforms allow the creation of decentralized applications (also called "dapps") through the settlement of smart contracts between peers. Smart contracts represent a new way of performing peer-to-peer transactions in a totally decentralized and automated manner. They are made of protocols on a blockchain network that will set conditions for the contract to be validated. It's only when all conditions are met that the contract will be automatically executed after validation of the network. That is exactly how the Ethereum platform works. A user could for example set a request for the development of a decentralized application for its business. A smart contract will be set with another user of the network with app development skills. The requesting user will set all the conditions for the completion of the smart contract, which will be executed only if all these conditions are met by the developer. When all conditions are met and validated by the network, the smart contract will automatically execute, the "dapp" will be sent to the user and the developer will be paid with the platform's native tokens ETH (also called "Ether"). The scope of these "dapps" using smart contracts can go way deeper and allow for example to pay your insurances, perform instant payments for any service and even borrow, land or trade digital assets in a totally decentralized, safe and anonymous way. (Elliott, de Lima, & Singel, 2018)

Now that we have a clear view on all types of cryptocurrencies and their applications, let's have a brief technical parenthesis in order to better understand how a transaction with cryptos really works.

Chapter 2. How it works

Most cryptocurrencies working on a decentralized basis usually use blockchain as underlying technology. However, it is important to mention that not all cryptocurrencies use blockchain since they are not all based on decentralized networks. What is also important to remember is that all cryptos using this technology have their own individual blockchain network.

Blockchain is actually one form of what we call *Distributed Ledger Technology* (DLT), a protected online ledger that can be shared simultaneously by all users of the network. Blockchain technology is a specific way of implementing DLT, in which data is stored in a series or chain of blocks (hence "block-chain"). All blocks are linked to the next ones via a cryptographic key that provides them with a high level of security and reliability. Cryptography is a technology allowing to encrypt information through a complex series of codes and that only allows permissioned users to read and understand the information. The blockchain is run and maintained by a network of users called "miners" who validate each new transaction. They are typically syndicate of specialized computers with huge computing power who will be compensated for their work. They represent the nodes of the network and play the role of the trusted counterparty to ensures security and reliability.

In order to understand easily how a transaction with cryptocurrencies works, we'll take the example of a transaction with the most famous cryptocurrency; Bitcoin. Let's consider a user who wants to send a given number of bitcoins to another one and therefore requests a transaction on the network. The transaction is encrypted and directly broadcasted to all available nodes. Each node (or miner) collects new transactions and groups them into what we call a "block". The block will then be broadcasted again to all nodes in order for them to solve a complex "proof-of-work" that will serve as validation for the block. The proof-of-work is an elaborated cryptographic puzzle that miners have to solve in order to validate the block's underlying data. The first miner who succeeds on solving the puzzle "wins" and is compensated by newly created bitcoins. The reason why they are called "miners" is actually because of the fact that they create (or "mine") new bitcoins through the validation process. To ensure the reliability of new blocks, all nodes of the network will need to validate the solved proof-of-work. We say that nodes have reached a consensus when at least 50% of nodes agree to say that the proof-of-work is correct. Once a consensus is found, the verified block will be added to the chain and will usually contain the transactions data, a timestamp and a hash pointer (the link to the previous block). The hash will be timestamped and made publicly visible for all users of the network in order to see what the latest version of the chain is. The succession of all timestamps in the chain makes the transactions irreversible and permanent, meaning that the information can't be modified once broadcasted on the blockchain. (Nakamoto, 2008)

Chapter 3. Conditions for being a currency

Among the huge amount of questions aroused around cryptocurrencies, the most frequently asked would probably be: Are cryptocurrencies real currencies? The question is totally legitimate since meeting the conditions of currencies as we know them today is important to be able to consider a possible development of this new way of transacting. One of the best ways to evaluate the usefulness and relevance of new transaction methods is probably to see what history taught us over the years. Today's means of exchange are just a consequence of a series of evolutions and improvements since approximatively twelve thousand years. Transaction methods have evolved across societies to answer new technological challenges and new economic needs. Let's see how it happened and what historical heritage did it bring to our modern way of transacting.

3.1. History of money

If trust represents one of the biggest issues people are facing nowadays when transacting, it was not such a problem twelve thousand years ago. Indeed, as of we know, the earliest way of exchanging goods was based on trust. There was no money, or anything related to transaction value at that time. People could simply receive a good or service and repay it later with another good or service. The only way to keep track of who gave what to who relied on the community's memory. However, once communities started to expend, it became too complicated to remember all transactions. Communities had to find a solution and started to exchange on an instant basis. That's how barter appeared around 9000 BC. People typically exchanged their surplus of foodstuffs or cattle for the goods they needed. Barter worked for a moment, but issues quickly appeared. Indeed, it was already quite hard to find the person that had the good you wanted but it was even harder to find the person willing to take what you had to offer in exchange.

Around 3000 BC, societies started using for the first-time foodstuffs as medium of exchange. People used for example cacao beans, barley or salt as a uniform value to trade goods. This allowed to solve availability and perishability issues. Overtime, people then started using non-food goods as currencies such as Cowrie shells in order to overpass seasonality and storage issues. Currency at that time started to gain a more symbolic value compared to consumption goods.

As time passed, societies started replacing shells with metal tokens, but new issues raised. Indeed, metal pieces were usually of different size, metal types and purity. The lack of uniformity in the currency initiated the development of metal-based coins stamped with the type of metal, the weight and the purity of each coin. The coins lasted from 600 BC until the Renaissance but it's interesting to mention that the concept is more or less the same as we use nowadays with coins. The 8th century marked the introduction of paper money, first as a promissory note for metal. Paper was way easier to store and to carry than metal pieces, therefore providing better security during transport of money. Paper money was then issued by banks as a promise to exchange gold. Around 1970, gold was no longer a standard and money became "fiat", meaning that it would not be convertible into another value anymore. (Halaburda & Sarvary, 2016)

Of course, all these changes were not easily accepted and it took time to reach full adoption. Paper money was first very bad received by people, considered as less trustworthy than metal. Trust in the currency was not well established until governments started to guarantee its value. It then gained legitimacy and got widely adopted as a mean of payment.

Trust was and will always stay an important component to manage during the development of new transacting methods. Cryptocurrencies are indeed facing huge trust issues for lot of reasons that we will cover in the next section. The history of money is moving to a new era, characterized by a significant change in paradigm. Until today, electronic money such as debit and credit cards have always been backed by fiat money as a physical counterpart. People know that they can exchange their electronic money for tangible notes whose value is stable and guaranteed by central banks, themselves backed by governments. The whole digital currencies family, including cryptocurrencies, only exist virtually. They are not tangible, there is no way to print Bitcoins or have them in our hands. This lack of tangibility has a huge impact on how people have trust in the value of a currency and therefore not consider it as a sustainable medium of payment.

In order to see if cryptocurrencies are real currencies, let's analyse if they have what it takes on a theoretical point of view. In the economic literature, money is usually defined according to the role it plays for individuals. Let's define these roles and see to what extent cryptocurrencies can fulfil them.

3.2. Roles of money

Money as we know it today fulfils three important roles; act as a unit of account, a medium of exchange and a store of value. These roles are the reasons, or even maybe the conditions, required for us to use a currency. (Cartsens, 2019)

Acting as a *unit of account* means that money has to be a globally accepted measure of value. This measure of value will facilitate the comparison of prices for goods and services we buy in the economy by acting as a common denominator. This denominator will allow to evaluate goods and services according to their relative prices. In order to be qualified as unit of account, money needs to be uniform and comparable. As shown earlier, these attributes allowed money to evolve overtime and be widely used to value goods and services.

Being a *medium of exchange* requires the currency to be globally accepted as a mean of payment for the seller. With this characteristic, money is able to answer the economic needs of both buyers and sellers of a transaction. To work as an efficient medium of exchange, a currency needs to have five important attributes; be divisible, uniform, easy to carry, trustworthy and scarce.

The last role of money is to act as a *store of value*, meaning that its value should be stable and reliable enough to be used in the future. In other words, acting as a store of value allows to transfer one's purchasing power overtime. To do so, the currency should be durable, easy to store securely and somewhat, scarce to avoid it being depreciated.

The applicability of these roles for cryptocurrencies can be discussed. Considering a cryptocurrency as a unit of account can be seen in two different ways. The first one would be to say that on a theoretical point of view, cryptos can be units of account since they represent units of value in a specific environment. That means that on a specific platform using only e.g. Litecoin, we would be able to use the cryptocurrency to compare different goods or services. Two goods could be worth a given number of LTC[4] and it would therefore be possible to extract a relative price from these two goods. If we now look at the question on a more practical point of view, we quickly realise that our first view is not totally applicable. Being in an open environment with lot of different currencies is not an issue since this is exactly what we

[4] Acronym of the Litecoin tokens.

encounter in the current economy. The issue stands in the fact that cryptocurrencies are not trusted and spread enough to be used as a unit of value. Up to now, we mostly express crypto's value according to conventional currencies. They are mainly considered as a rate such as BTC/EUR or BTC/USD if we take the example of Bitcoin. Even though some countries like South Korea are early adopters of Bitcoins for daily transactions, it is still very rare to see products in a shop expressed as a certain number of Bitcoins. As a matter of fact, only 0.3% of shops in America allow payments with Bitcoin. (Landau, 2018) In addition, transaction costs remain really high since retails hedge against volatility by applying big margins to prices expressed in Bitcoin.

Telling if cryptocurrencies can play the role of medium of exchange also involves a contrasted answer. As we just saw, they can only be defined as a unit of account to a limited extent because of the low level of adoption. This weak adoption rate will of course influence the fact that cryptos can hardly be globally accepted as a mean of payment. One of the biggest barriers to adoption is the fact that cryptos are mainly held for investment purpose. A survey run in the United States of America showed that only 8% of Americans who bought bitcoin did it for transactions purpose. Cryptos indeed represent a great way for investors to make fast profit because of the high price volatility. This phenomenon is reinforced by the fact that there is no financial entities or governments to regulate their use. Because of that, the level of transactions using cryptos stays really low compared to traditional currencies. If we take again Bitcoin as an example[5], we'll see that the level of Bitcoin transactions in the Euro zone account for only 0.2% of all transactions (excluding speculative transactions).

If we stick to the definition, as of today, cryptocurrencies can't play the role of a generally accepted medium of exchange. However, this definition might face limits that cryptos would be able to solve in a near future. Indeed, the current role of money to act as a medium of exchange is limited to specific geographic areas and is therefore not universal. There are e.g. very few places in Europe where you'll be able to pay in Yen. Of course, all these currencies enable easier trading activities but are usually only accepted as a mean of payment in a limited area. This is where cryptocurrencies go far beyond the concept of payment as we know it as of today. Cryptocurrencies allow to perform transactions wherever we're located, in whatever

[5] Since Bitcoin is the most known and used cryptocurrency, most surveys and calculations are based on this crypto. As other digital cash coins represent an extremely low portion of transactions, we consider Bitcoin's figures to be relevant enough for our analysis.

crypto we want and in a nearly instant way. The fact that cryptocurrencies are not currently globally accepted as a mean of exchange doesn't mean that we should exclude them from the definition. This technology represents a heavy change in the payment paradigm and deserves to be considered to its full extent.

The last role, being a store of value, also represents an important factor for the adoption of a new currency on a market. Obviously, the high price volatility makes it impossible for cryptocurrencies to be considered as a store of value, at least in the long term. It has been reported that cryptocurrencies are approximatively 25 times more volatile than American stocks, 5 times more than commodities and 12 times more than the Japanese Yen. (Landau, 2018) If people can't be sure they'll be able to exchange their money in the future for approximatively the same value, they won't consider a currency as trustworthy. A point that is worth mentioning is that the definition considers of course a currency to be a store of value only if it allows to transfer one's purchasing power in the long term. However, the first well-functioning cryptocurrency (Bitcoin) was created only 10 years ago. It is therefore too early to say if their value could (or not) be stable in the long run.

At the end, one could question the applicability of the "Three roles of money" on cryptocurrencies for the simple reason that the way we see money is evolving and switching to a brand-new dimension. The three roles we analysed actually determine how things should work at equilibrium in a specific paradigm, the one we know today. But what if this paradigm was changing? In order to answer that question, let's see to what extent cryptocurrencies represent (or not) an innovation in our way of transacting with each other.

Chapter 4. A technical innovation

Cryptocurrencies are an ingenious combination of technological innovations and monetary innovations. They leverage on state-of-the-art technologies to provide a totally disruptive way of performing transactions on the market. In order to better understand where the innovation stands, let's have a more detailed view on all components of these technical and monetary innovations. We'll use the Figure 3, "The Money Flower" developed by the Bank for International Settlements (BIS) to support our analysis. (BIS, 2018) The schema proposes a

clear and visual representation of a taxonomy of money including cryptocurrencies and central banks digital currencies (which we will cover in the second part of this report).

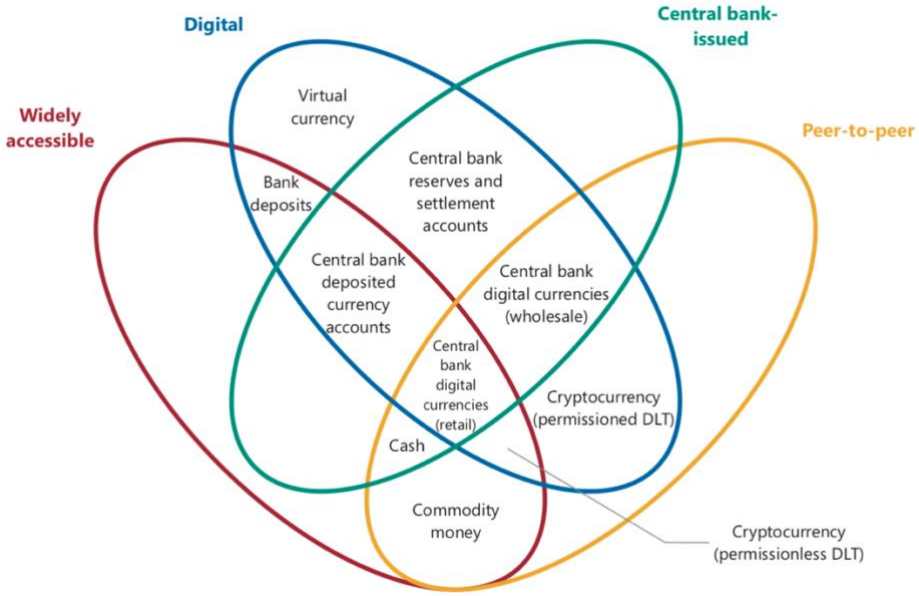


Figure 3. The Money Flower - Taxonomy of money

The first thing we see when looking at the Money Flower is that innovation doesn't stand in the fact that cryptocurrencies are digital. Except cash and commodity money, all other currencies are represented or used in a digital form. Tangible money is doomed to disappear in the next decades due to the growing influence of digitalization in payments. Where the innovation stands is in technology but not individually. What represents the biggest innovation of cryptocurrencies is actually the intelligent combination of multiple technologies such as distributed ledgers, cryptography and electronic signatures. As a matter of fact, those innovations taken individually are not so new as their concept existed since a long time ago. The development of technology simply enabled them to evolve in a more convenient and effective way. Those three technologies are linked to each other to provide the so-called blockchain technology. Even though all cryptos don't necessarily use blockchain, it is still a huge component of what constitutes cryptocurrencies and deserves strong attention.

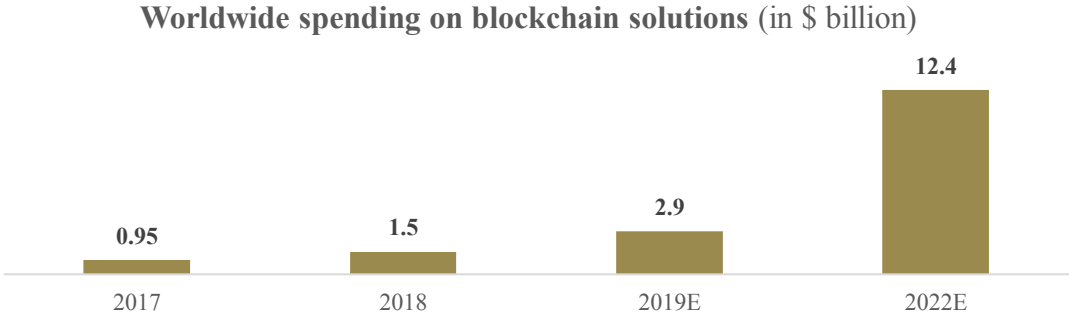
4.1. Blockchain outlook

Blockchain technology was mainly discovered after Bitcoin's media attention but actually goes far beyond just cryptocurrencies. It is every day more and more adopted by companies all around the world in many different sectors, going from public services, to healthcare or

financial services. It represents a new way of exchanging and storing information, with a strong focus on security and anonymity.

> Today, blockchain is to trust what the web was to communication: a profoundly disruptive technology that transforms not only business but the way humans transact and engage. (Deloitte, 2019)

Companies are heavily investing in blockchain technology in order to be provided with strong first-movers advantages in the coming years. As a matter of fact, global spending on blockchain solutions are expected to increase from 2017 to 2022 with a Compound Annual Growth Rate (CAGR) of 74,16%. (IDC, 2019)



Graph 1: Worldwide spending on blockchain solutions

Blockchain is able to provide support to a wide range of activities, both for public sector, private companies or individuals. It could e.g. help private or public companies to exchange digital assets, distribute information safely or share digital contracts. Individuals on their side could use blockchain to manage their financial information, their health records or their legal documents. The technology could potentially take over the role of any trusted intermediary such as banks or credit agencies. (Deloitte, 2018) In terms of market shares, blockchain is mainly used in the financial industry (60.5% of market shares), followed by the manufacturing sector (17.6%), the distribution & services sector (14.6%), the public sector (4.2%) and infrastructure (3.1%). (IDC, 2018)

Few examples of near-future implementations of blockchain could be in voting systems, identity verification and of course, cryptocurrencies. Voting systems could leverage blockchain technology in some developing countries where elections are usually manipulated or hacked. It could also be of a great help to support the management and verification of identities by

providing a global and reliable shared source of information. Finally, one use case of permissionless cryptocurrencies would be e.g. in countries with hyperinflation, where cryptos could represent a viable alternative to the current payment system. Gartner actually forecasts a considerable increase in the use of blockchain technology in these three specific topics in the next 4 to 6 years. (Gartner, 2018)

Chapter 5. A monetary innovation

Besides being a technical innovation, cryptocurrencies also represent a monetary innovation in the way we experience payments. Overtime, money has evolved either through improvements of how the payment system works or through changes in the nature of money. Today, cryptocurrencies mark a new era in the payment ecosystem by working on both components at the same time. In order to better understand this evolution, let's go through the most popular means of payment in place as of today and see what their key advantages and disadvantages are. We'll then go through the economic characteristics of cryptocurrencies to have a better idea of the level of innovation provided by this new mean of payment. This chapter actually represents a sort of continuum of the section 3.1 about the history of money but focusing on the current payment mediums.

5.1. Cash money

Cash constitutes the pillars of our contemporary payment system, nearly everything is backed with cash. It is usually described as a set of key characteristics also associated with their core advantages. The first and most obvious characteristic is the instant dimension of cash. Payments in cash happen on an instant basis and therefore settle instantly the underlying obligation. This instant feature implies the absence of credit risk during cash transactions and implies the change of ownership at the moment when the transaction is settled. Its second important feature is that cash is the liability of the central bank that issued it. This characteristic makes it more trustworthy for people than deposits, debit or credit cards that are the liability of a private bank. In theory, central banks should indeed be less prone to default risk than private banks. Another feature of cash is the level of privacy it provides to its users. Cash settlements are totally anonymous and therefore prevents any malicious party to collect and store any personal information or transaction history. One last but very important characteristic is that cash money

doesn't require any intermediary for a transaction to be settled. They are peer-to-peer transactions as they happen on an instant basis between a buyer and a seller, without any financial institution acting as a third party.

5.2. Credit and debit cards

Credit and debit cards are the most widely accepted means of payments worldwide. On a local perspective, a study (PostNord, 2018) showed that 59% of Belgians prefer using their credit or debit card to make purchases online. This number is growing over the years while other payment methods are declining, such as direct electronic payments or cash on delivery. Credit cards offer lot of advantages to both customers and retails. Customers benefit from delayed and deferred payment of their bills, as well as rewards for the money spent and protections against theft or scams. Businesses, on their side, benefit from assurance of payment in case of troubles and from network effects inducing customers to pay more with their credit card and more often. (Beach & Hagiu, 2014)

Unfortunately, this widely accepted payment method also has its drawbacks. Providing customers and retails with so many protections against theft and fraud necessarily imply the fact that such things can happen quite often. Risks of theft and data misuses considerably increased with the growth of contactless cards being progressively adopted by individuals. Indeed, studies (ING, 2016) showed that European consumers are feeling more and more confident about using contactless payments, even though nearly half of them are still concerned about their security. Another strong limit to credit and debit card use is the low speed of transactions. A settlement will usually take between two or three days to be settled, therefore creating a potential credit risk for users. This transaction time maybe seemed standard a few years ago but the need for globalisation and speed pushes this standard to be revised every day. A third shortcoming is more credit cards-specific since it's the fact that such services are usually costly for users, through various fees or interest's payment. Finally, even though it seemed obvious, credit and debit cards require users to have an account in a financial institution. This means that users have to provide a bunch of information making them identifiable. Their transactions can then be tracked and regulated easily.

5.3. E-transfers

E-transfers are bank transfers linked to an individual or an entity's bank account and usually performed online. E-transfers have more or less the same drawbacks as credit and debit cards with the main difference that e-transfers are limited to certain types of payments, usually recurring payments or small amount settlements. For the rest, bank transfers can also be costly depending on the method used to perform the transactions. Online or mobile payments are usually costless while payments in branches will induce transaction fees. E-transfers will also usually take time to settle depending on the geographic area and the chosen financial institution of both users. They are bank account-based, meaning that they are not anonymous, can be tracked and that banks act as an intermediary in transactions.

5.4. Online payment platforms

The last type of payments we'll consider are payments performed via an online platform, independent from private banks. These platforms allow users to settle electronic transactions by either depositing money on the platform or by linking users' credit or debit cards on their account on the platform. A worldwide reference of online payment platform is PayPal, referred as the second preferred online payment method worldwide, with a global annual amount of transaction of 9.9 billion transactions for a total annual amount of 578 billion U.S. dollars as of 2018. (PayPal, 2019)

This kind of platforms have no choice but to benefit from network effects in order to be widely adopted. Since users need to create a customer account on the platform in order for them to perform transactions, it makes it impossible to transact with individuals who are not registered on the platform. They are also considered as more secure than other electronic payment methods since users don't need to provide a wide bunch of financial information in order to use the platform. Users are usually authenticated through their email address and have their linked bank account information encrypted and protected. These platforms allow peer-to-peer payments in the sense that the only intermediary is the platform that supports the transaction of electronic value. This feature allows them to provide payments in a fast and costless way. The only potential shortcoming of this feature is that money deposited on the platform is the liability of the latter and therefore exposes users to potential credit and default risks. (Athanassiou, 2017, pp. 5-9)

This allows us to summarize each above payment method characteristics in the below table;

	Cash	Debit & credit cards	E-transfers	Online payment platforms
Processing time	Instantly	Few days	Few days	Almost instantly
Liability of …	Central banks	Private banks	Private banks	Platform
Privacy	Anonymous	Limited	Limited	Good
Intermediary	None (P2P[6])	Private banks	Private banks	Platform (P2P)
Risk of fraud	Very low	Medium	Medium	Low
Costs	Costless	Fees & interests	Fees	Almost costless
Credit & default risk	Extremely low	Medium	Medium	Medium

Table 1: Characteristics of current payment methods

Now that we have a clearer view on these different characteristics, let's see to what extent cryptocurrencies differ from the latter.

5.5. Cryptocurrencies' added value

We'll use the below figure (Landau, 2018) to position cryptocurrencies in the payment ecosystem and underline their key differences.

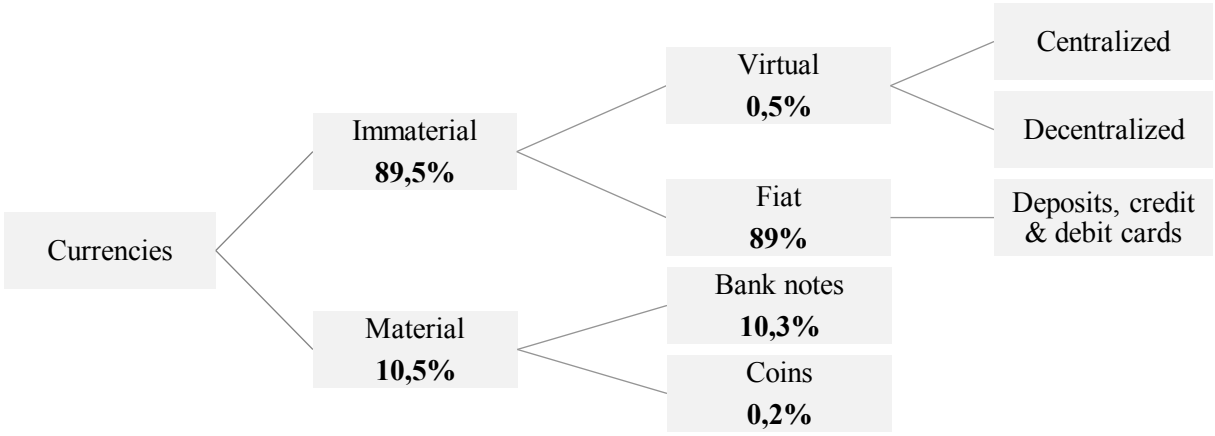


Figure 4: The money ecosystem

One of the very first distinction to make is between fiat currencies and virtual currencies. As we saw in chapter 1, cryptocurrencies are a type of virtual currencies, meaning that they are totally *dematerialized* and can't be converted into physical money. It is important to avoid the confusion between electronic money, such as the one used e.g. for mobile payments, and virtual

[6] Peer-to-peer

money. Virtual currencies only exist in a virtual way, whereas electronic money is simply the result of digitalization and improvements of user experience. This is already one crucial innovation pattern in the sense that it represents a true upset in the nature of money. Money is no longer seen as fiat and is switching to a fully digital form devoid from any physical counterpart.

Another considerable innovation pattern is the fact that cryptocurrencies are traded *independently from financial institutions* and central banks. The latter have no control on the issuing or circulation of tokens. The first implication of this characteristic is that cryptos aren't the liability of anyone compared to other payment methods that usually represent a claim on either commercial banks or central banks. They are peer-to-peer and don't need any financial institutions as intermediary to complete transactions. The platform or the network act as a unique intermediary to exchange value in a virtual form. (Landau, 2018, p. 7) The economic implications of this lack of financial institutions as counterparty will be discussed in the last part of the report.

A key added value of cryptocurrencies is the *speed of transactions*. Indeed, as we just saw, alternatives such as credit cards or bank transfers can take between two and three days to have a transaction settled and can be even longer depending on the geographic location of users. Crypto payments process much faster and could take in the worst-case scenario a couple dozen of minutes to be settled, whatever users' geographic location. The time needed for a transaction to be settled will mainly depend on how complex is the underlying protocol, how big are the blocks and how busy are the nodes. In other words, the main driver of speed in cryptocurrencies transactions is the time required by miners to verify each block. Depending on their architecture, some can be faster than others. For example, Dash coin uses speed of transaction as a differentiating factor by pledging a transaction speed of one second. (Dash, n.a.) In addition to the underlying architecture, improved transaction speed also comes from the absence of financial institutions as intermediary, allowing transactions to travel solely through one single and global platform.

One of the most claimed added value of cryptocurrencies is also the *level of privacy* it provides to users. Indeed, through the lack of regulatory institutions, cryptos are able to provide fully anonymous transactions to users compared to electronic payment methods seen above. Of

course, the question of full anonymity raises lot of debates that will need to be cleared-up at some point. We'll discuss this question more broadly in chapter 2 of our last part.

The last strong argument of cryptocurrencies is their *low transaction costs*. Indeed, cryptos users are able to perform transactions at a cost close to zero compared to e.g. credit cards that request fees for enrolment and international payments. However, even though transactions seem costless for consumers, they are not necessarily for retails that undergo the whole volatility of the exchange cryptocurrency. In order to protect themselves, retails therefore apply considerable margins on goods and services as a kind of hedging instrument. This margin can be considered as a transaction cost supported at the end by consumers that will have to pay more for a product if they decide to buy them e.g. in Bitcoin rather than with their debit card. These transaction costs apply when considering only buyers and sellers, but if we look beyond that, we can also easily consider "mining" costs as strong transaction costs. Mining costs are not directly visible for end users but are an important part of debates around cryptocurrencies. We'll discuss more broadly this issue in section 2.4 of our last part.

At the end, all these improvements put together can change our perspective on how to exchanges goods and services. The innovation actually stands in the way we experience the use of a new type of money. Fast, cheap and seamless transactions aim at improving our experience in a way we never encountered. Indeed, the types of currencies have changed a lot over history but there has always been one or more of the following characteristics: (Landau, 2018, p. 7)

- A support from governments and central banks;
- A physical counterpart as back-up;
- An intrinsic value.

Today, cryptocurrencies represent a truly disruptive innovation upsetting all the standards we have set over the years. They are a new way to perform payments in a paradigm we barely discover.

Actually, the last point deserves to be considered with more attention. In the economic literature, the shortcut is usually taken to say that cryptocurrencies don't have any intrinsic value since they only exist virtually. The question needs to be considered with nuances depending on how we value cryptocurrencies.

DO CRYPTOCURRENCIES HAVE AN INTRINSIC VALUE?

In order to answer that question, we'll need to go deeper into details and use a microeconomic perspective focusing on marginal production costs. According to the theory, the value of a good would be equal to the sum of all its marginal costs of production.

The biggest indicator of cryptocurrencies' costs of production are the mining costs that can take huge proportions in some cases. Mining a cryptocurrency is the process of validating a new block through the resolution of a complex cryptographic puzzle called "Proof-of-Work" (PoW). During this process, miners will compete in order to be the first to solve the PoW and get remunerated.

The most controversial cost component is the amount of electricity required to solve such complex puzzles. Indeed, one single transaction of bitcoins requires around 635 KWh[7] to be settled from end-to-end. (Digiconomist, 2019) On a larger scale, the global energy consumption of Bitcoin is approximatively equivalent to the energy consumption of countries like Czech Republic. (Digiconomist, 2019) This huge electricity consumption is mainly the result of competition between miners in solving the Proof-of-Work, resulting in spoiled energy consumption for the ones who didn't succeed on solving the puzzle. In addition, the more competition there is, the more complex is the PoW and the bigger the energy consumption will be. What also comes to reinforce this phenomenon is the network effect generated by an increase in adoption. Indeed, the more people use cryptocurrencies, the more technology will improve and people will consider it as socially acceptable as a mean of payment. This will result in higher volumes of transactions and greater complexity of technology to provide better security. Mining costs will therefore increase quite significantly. (Sia Partners, 2019)

Saying that cryptocurrencies don't have any intrinsic value is hence a too easy shortcut considering their inner cost structure.

[7] Kilowatt hour is a metric used to measure energy consumption. It represents the number of Kilowatt consumed during an hour in a closed system.

PART II. DEVELOPMENT OF CRYPTOCURRENCIES

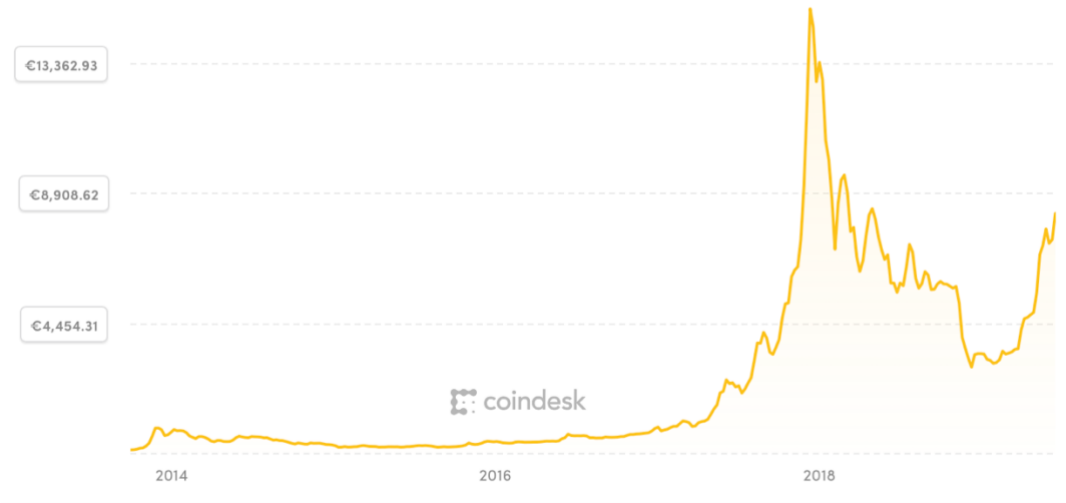
Now that we have an in-depth view of what are cryptocurrencies, let's see more into details their current development and adoption. We'll go through the current state of adoption by determining the drivers of demand & supply and by going through some examples of adoption around the world. This will allow us to have a greater idea on how promising and trusted cryptocurrencies could be. We'll also put the emphasis on the changing environment in the financial sector by going through key emerging trends such as digitalisation, FinTech and the introduction of the GAFA in the financial industry. The last chapter of this section will be dedicated to a use case analysing the possible development of central bank-issued cryptocurrencies.

Chapter 1. Current state of development

1.1. Drivers of demand

Same as any other currencies, the value of cryptos is influenced by its underlying demand and supply. Demand for cryptocurrencies is determined by 5 key drivers that are direct indicators of the level of adoption of the latter.

The first and most popular driver of demand is *speculation*. It represents people who are only buying cryptocurrencies with the expectation to extract profit from their investment in the short term. They are the greatest number of users but actually represent a barrier to the use of cryptos as a mean of payment. In order to invest in cryptocurrencies, users will need to open an account on an exchange platform such as Coinbase or BitStamp. These are platforms that allow users to buy and sell cryptos amongst a large choice. More advanced investors will also use cryptocurrency derivatives exchanges allowing to speculate or hedge against cryptos volatility. The main issue with speculation is its unpredictable pattern. Exchanges are based on the future, representing the opposition of buyers' and sellers' expectations. Buyers typically have a positive opinion about the future while sellers have a pessimistic view on the future, believing that the value will decline. Volatility therefore arises when expectations about the future are changing. The best example we can take is the price index of Bitcoin that heavily fluctuated during the last two years. The graph 2 below (Coindesk, 2019) illustrates the overall price of BTC, resulting in strong changes in buyers' and sellers' expectations overtime.



Graph 2: Overall Bitcoin Price Index (EUR)

A second driver is the users holding cryptocurrencies for *investment* purpose. It is kind of the same as the previous one but with on focus on long-term profits. They believe cryptos' value will increase in the future and therefore buy them either for profit purpose or as a way to hedge against the risk of some current currencies. These are actually the exact same reasons why people buy commodities or other conventional currencies. Cryptocurrencies represent a new asset class that is not yet totally accepted but that is more and more spread over investment portfolios. They typically provide investors with improved returns due to the higher risks generated by their volatility. These users will also usually use cryptocurrency exchanges to perform their investments.

The third key driver of demand is the use of cryptos as *alternative currency* to the conventional ones. Users typically believe the crypto could allow them to purchase goods or act as a store of value. They usually have faith in such currencies for their core characteristics being the lack of control by governments, the high level of security and the anonymity. In order to use cryptos as a mean of payment, users will need a crypto-wallet, which is a software platform allowing them to store and transact cryptos. On their side, retails will of course need to accept cryptos as a mean of payment. To do so, they will need to equip themselves with crypto-payment processors. These are IT infrastructures allowing retails to accept cryptos for payment by converting received cryptos into the currency they want. (Elliott, de Lima, & Singel, 2018)

What can be seen as a fourth driver is the use of cryptocurrencies for *technological purposes*. This is typically the case of platform tokens (cfr. Types of cryptocurrencies) that support a

specific task by acting as an enabler in the network. Demand for such tokens will depend on how widely a platform is used. The more people use the platform, the higher will be the demand for platform tokens.

The last driver of demand represents users acting as *market makers*. They account for a very small part of demand for cryptocurrencies and could be assimilated on some points to speculators. What they typically do is to go from exchange platforms to exchange platforms in order to benefit from differences in prices. Demand for cryptocurrencies in this purpose is likely to remain quite low but stable considering the fact that exchange platforms will always offer slightly different prices depending on their adjustment mechanisms. (Elliott, de Lima, & Singel, 2018)

On a business perspective, we can therefore generalize cryptocurrencies holders into three categories:

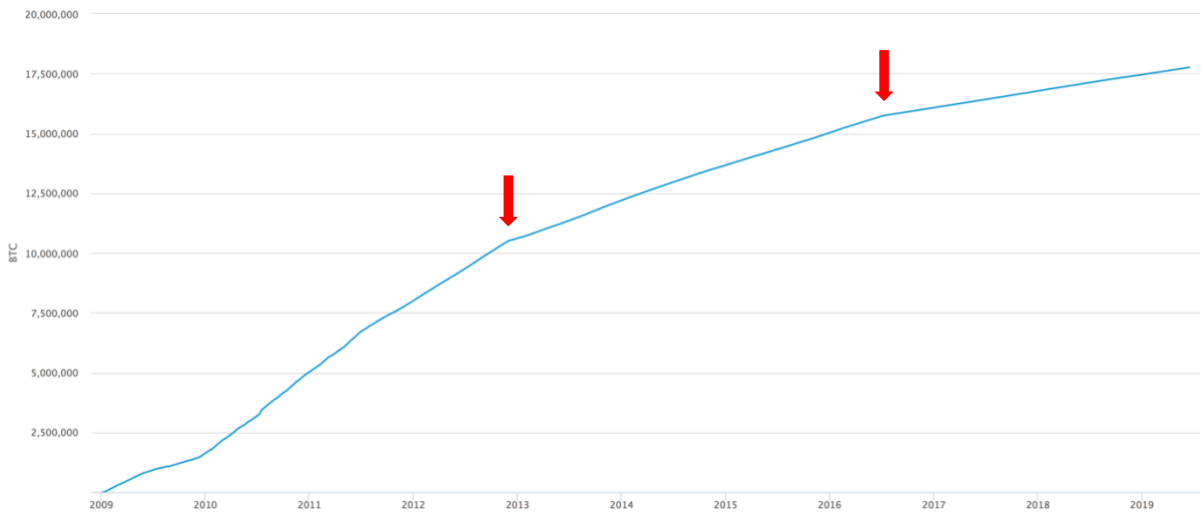
- Speculators, who hold cryptocurrencies with the expectation to make profit but don't intend to use them for transactions;
- Technologists, who hold cryptocurrencies because they believe in the disruptive pattern of the technology and want to support it;
- Rebels, who hold cryptocurrencies for their anonymity and deregulated features and typically use them for illegal purchases or to stay away from the control of a central entity.

1.2. Drivers of supply

Same as any other currency, cryptocurrencies are issued by an entity with the goal of regulating the value of money put on the market. The only difference with conventional money is that cryptos are issued by the private entity that created it. They are the only ones with the right to issue new tokens. However, all cryptocurrencies are not issued at the same rhythm and quantity.

A first method used by cryptocurrency founders is to cap the number of tokens issued to a final amount such as this is the case for Bitcoin. The number of BTC is hence limited to a maximum of 21 million BTC, among those, around 17.7 million are already circulating. New bitcoins are then created through the mining process and are distributed to miners. Bitcoins are created every time a new block is validated, which happens approximatively every 10 minutes. However, in

order to avoid their value to decrease due to over-issuance, the level of rewards will be cut by half roughly every 4 years. This controlled increase and final amount of BTC allows Bitcoin to benefit from a very stable monetary issuance model. The graph 3 below (Blockchain, 2019) shows the number of BTC in circulation over time. If we look closely, we can see the two first rewards reduction that happened in November 2012 and July 2016, represented by small flattening's of the curve.



Graph 3: Number of Bitcoins in circulation overtime since 2009 until 2019

A second way to manage the supply of a cryptocurrency is by defining an initial number of tokens set aside and that will serve as reserve for the future. This is how Ripple recently (2017) improved its issuance model. What they did is that they set aside 55 billion XRP in Escrow out of the 100 billion initially created. The escrow is then divided into 55 contracts of one billion XRP. Each month, a contract will expire and the billion XRP will be made available for Ripple to sell them to users of the network. The XRP remaining will be put back at the end of the Escrow in order to be used in the future. The key difference of Ripple compared to the previous case is that XRP do not require any mining activity since they are all "pre-mined" by the founding company. The only way to enter new XRP in the network is therefore to sell them to clients, being either banks or payment providers. The main reason why they developed this issuance model is to allow people to evaluate and forecast with precision the total supply of XRP overtime. (Ripple, 2017)

The last type of issuance model is the one used by the decentralized platform Ethereum. Their ETH supply mechanism is more or less the same as the one of Bitcoin in the sense that they both issue new tokens through the mining process. The only difference with Ethereum is that the number of ETH distributed is not a fixed number but is based on a percentage of the total pre-sale purchases of ETH tokens. Miners will therefore be remunerated of a few ETH to reward them for the validation work of new blocks. Reward level is also intended to decrease in order to avoid hyperinflation of the currency. (EthHub, n.a.) However, it's important to note that Ethereum will very soon change its issuance policy to go for a more efficient one that will grant higher rewards to miners. This new policy is called Proof-of-Stake and will replace the current Proof-of-Work. We'll see to what extent this new model differentiates itself from the current one in section 2.4 of our last part dedicated to the impacts of cryptocurrencies.

Now that we have a theoretical background regarding demand and supply of cryptocurrencies, let's deep dive into real life examples of companies and governments that adopted this technology in their day-to-day life or activities. Such use cases show how relevant cryptocurrencies can be in different situations and give them a more realistic image on the market.

1.3. Companies as early adopters

When digging a bit amongst cryptos' adopters, one quickly realises that digital cash coins are not just a geek tool invented to make money. Going through the list of early adopters will allow to have an idea on how global the adoption of such currencies is. It will also be interesting to see that not all types of cryptos are used by the same players and in the same industries.

Adoption of cryptos is already spread around different sectors, going from delivery to holidays bookings. The biggest example of adoption is the online food delivery platform Takeaway.com that is now accepting Bitcoin payments through BitPay, a cryptocurrency payment provider. Customers from nearly all European countries can buy their food in a few clicks. The good point is that Takeway.com is not applying any fees on such transactions in order to give customers the incentive to use such payment methods. In order to know what exchange rate will be applied for the payment, customers have to refer to the rates proposed by the payment provider BitPay. (Takeaway, 2019) Another strong player of the market who also adopted Bitcoin as payment method is Dominos Pizzas. Dominos on their side have put a strong focus

on the US market of food delivery in order to be early adopters of Bitcoin payments. One of the latest adopters in the food sector is Starbucks since May 2019. They will now allow their customers to buy their favorite drinks with Bitcoins. Bitcoin has also been well adopted in other industries such as travels with Expedia or online retails such as Rukuten, the biggest Japanese online retailer who will soon allow payments with its native crypto and accept cryptocurrencies exchanges.

Besides private companies, Bitcoin is also heavily accepted by non-profit organizations such as Wikipedia or WikiLeaks[8]. They typically accept payment not for transaction purpose but as an alternative way to find funding. WikiLeaks e.g. benefits from Bitcoin's anonymity feature to receive donations from people who support their activity all around the world. This alternative funding method got even more important for them since global service providers such as Visa and Mastercard banned WikiLeaks from their client list for the controversial aspect of their activity.

Even more surprising, some real estate agencies such as Bitcoin Real Estate (Bitcoin Real Estate, n.a.) are today specialized in selling properties in cryptocurrencies. You could e.g. buy a house on the beach or even an hotel with Bitcoin, Ethereum or Litecoin. Properties are usually sold on a conventional currency basis and will be converted into the equivalent amount of cryptocurrency at the time of the sale. Landlords selling their house in cryptocurrency typically have low risk aversion profiles considering the current volatility of such cryptos. Buyers and sellers could potentially make money from a capital gain resulting in an increase or decrease of the cryptocurrency exchange rate.

1.4. Financial institutions as early adopters

When we talk about cryptocurrency adoption, we usually talk about people using Bitcoins for investment purpose or companies slowly starting to accept cryptos. People usually criticize cryptos for stealing power from banks but what if banks were actually following the hype and started adopting cryptocurrencies? In fact, many banks are currently assessing the impact of a potential development of such new technologies. Even though cryptos will still need some time to have their place in the banking ecosystem, it is not the case of blockchain that is getting more

[8] WikiLeaks is a non-profit organization founded by Julian Assange, where anonymous people can publish classified, censored or highly confidential documents on a platform in order to make them public.

and more attention from financial entities. Leading financial institutions have indeed stepped in to integrate the power of blockchain technology into specific financial activities. Amongst them, we can find JP Morgan, Santander, Barclays, Credit Suisse, HSBC and the U.S. payment provider American Express.

The most interesting step is probably the one made by Santander and American Express through their partnership with Ripple. The English bank and the American payment provider have indeed started collaborating with the FinTech company to improve their cross-border payments, especially between U.K. and the United States. Using Ripple's powerful blockchain, they are now able to exchange value between participating banks in Euros, U.S. Dollars and English Pounds. International interbank transactions hence happen on a real-time basis, at no costs and in a smooth and seamless way. The Ripple network is easily scalable and already includes Merrill Lynch, the Royal Bank of Canada, Standard Chartered and other important financial institutions. Of course, the technology and the development will improve if more financial institutions join the network, hence creating a network effect. In the current state, cryptocurrencies don't have a consequent utility but might be used in the future as an intermediary to support transactions in the network. (Browne, 2017)

Other leading banks are also working hard to discover how blockchain could revolutionize their core business. Credit Suisse e.g. has partnered with FundsDLT, a distributed ledger network, in order to perform assets investments in different currencies and at low costs. On their side, HSBC is using blockchain technology to reduce their foreign exchange transactions costs in trade finance. Barclays is also investigating on how to offer to their client the option to trade cryptocurrencies. Another powerful bank putting its trust into blockchain technology is the Suisse bank UBS, currently investigating to see how customers and businesses could benefit from blockchain through a totally new and unique financial experience.

Amongst all these leading banks, the one that is probably doing the biggest step into the unknown is JP Morgan with the introduction of their own digital coin, JPM Coin. The American bank is currently in a testing phase of a blockchain-enabled digital coin that will allow their institutional customers (banks and businesses) to perform real-time transactions between members of the network. The JPM Coin will act as an intermediary in transactions, representing virtual versions of U.S. dollars and convertible on a one to one basis.

The announcement of the introduction of JPM Coins by the American bank raised lot of critics regarding the characteristics that cryptocurrencies should take in order to be considered as so. On its website (J.P. Morgan, 2019), JP Morgan explains the key differences of its digital coin compared to "traditional" cryptocurrencies, mostly digital cash coins such as Bitcoin. The first thing is that JPM Coins are virtual representations of money owned by clients on their JP Morgan Chase account, therefore excluding any other non-client to participate and exchange money. In a more crypto-specific term, we can say that the network is hence permissioned or private. The value of one JPM Coin actually represents one U.S. Dollar of the customer's account, which means that the coins are backed by the money available on the client's account. The coins are hence backed by the bank's liquidity resources. Another difference raised is the fact that most cryptocurrencies have target users being retails and individuals, while JPM Coins is mainly business-to-business.

If we now take a more critical perspective, it's quite obvious to see that JPM Coins can't really be compared to traditional cryptocurrencies for the simple reason that they don't belong to the same category of cryptos. Bitcoin and Litecoin e.g. belong to the digital cash coin family and therefore have specific attributes and a specific purpose. On the other side, JP Morgan coins could be rather associated with cryptocurrencies such as Ripple that uses its tokens as an intermediary for transactions. However, it is still worth mentioning that JPM Coins have a unique benefit in terms of regulation compared to other cryptos. Indeed, since users are actually clients from the bank, regulatory requirements such as KYC[9] and AML[10] checks have already been run at the beginning of their relationship with the bank and are updated regularly.

On a general perspective, the growing consideration for cryptocurrencies from financial institutions is a strong sign that the technology is considered as potentially disruptive and needs to be understood as soon as possible. Banks are rushing to explore the full power of blockchain and intensively investigate to understand how this technology could improve customer experience through seamless processes, real-time transactions and low costs structures. The decentralized nature of the technology could allow the creation of a huge financial ecosystem where people could exchange virtual value instantly in a much more convenient way.

[9] Know Your Customer is a compliance requirement for banks to collect relevant information on their clients with the objective to avoid fraudulent activities and money laundering.
[10] Anti-Money Laundering is a regulatory check allowing to avoid money laundering.

1.5. Governments as early adopters

While some governments like Morocco or Bolivia simply decided to ban cryptocurrencies, some actually believed in the potential of the technology and decided to adopt them for specific uses. This is the case of Argentina that now allows its citizens of 37 cities to pay for public transport with Bitcoin. (Janus, 2019) They want to leverage on the new technology to improve the country's financial inclusion through day-to-day use of Bitcoin.

An even more surprising adoption is the case of a trade deal recently concluded between Paraguay and Argentina using Bitcoin. Indeed, Paraguay recently bought a set of chemical products and paid for them in Bitcoin. (Berman, 2019) Although the amount was only worth $7 100, it is still impressive to see how such governments can trust a cryptocurrency to settle their export deals. The transaction served as a test for both countries in order to conclude such transactions faster, more securely and without the consequent usual underlying fees. It also represents a solution for them to palliate to high inflation rate of their national currency.

Another interesting case is the one of Philippines' central bank who just allowed Union Bank to launch their first Bitcoin ATMs. (Young, 2019) Citizens will now be able to convert their paper money into Bitcoins (and vis versa) in order to use them for their day-to-day transactions. Such initiatives represent a huge opportunity to improve the very low level of financial inclusion in the country. As a matter of fact, only 34.5% of the population in Philippines in 2017 actually owned an account in a financial institution. (World Bank, n.d.)

Globally, it is often observed that adoption is significantly higher in unstable countries like Brazil, Colombia and Argentina. Such Latin America countries are currently facing series of political events resulting in low trust in governments and in a growing instability of the national currency. The Figure 5 below (Buchholz, 2019) also shows Turkey and South Africa as big adopters of cryptocurrencies. Unbanked population, high inflation rates and constant political conflicts are key factors in the adoption of alternative payment methods.

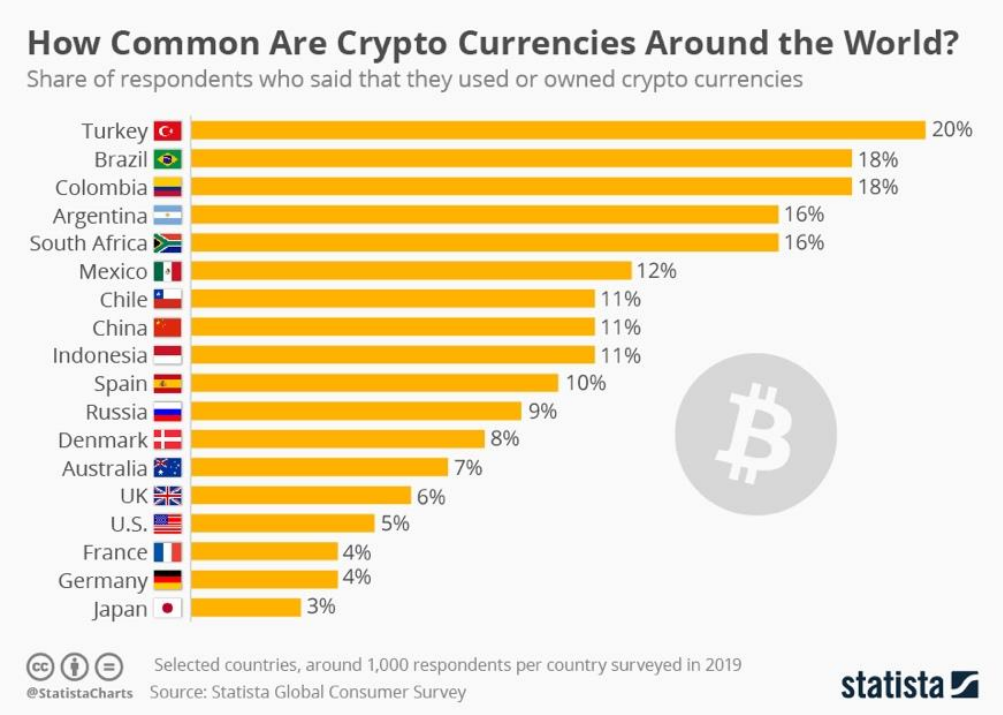


Figure 5: How common are cryptocurrencies around the world?

Of course, the adoption shown on the figure above do not only depend on high inflation and low financial inclusion. There are most certainly lot of other reasons to explain why e.g. Turkey is the first country on that list while Germany sits at the bottom.

These examples of adoption across players and industries clearly show how imminent is the cryptocurrency phenomenon. Actually, more than a phenomenon, cryptos are becoming a reality in lot of industries and capturing the attention of more and more institutions. What is also important to understand is that this development is not a standalone innovation. It is anchored in a broader upheaval of environment, characterized by new customer needs and powered by disruptive technologies.

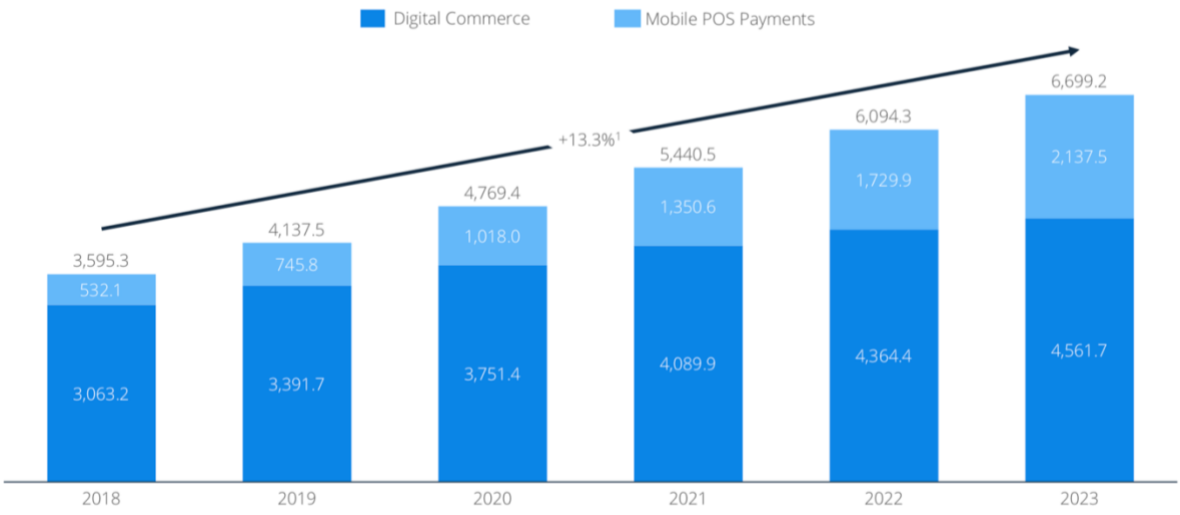
Chapter 2. A changing environment

The world is changing, that's a reality. It's now our role to understand it and integrate these changes in order to be part of the revolution. This upset comes from different sides but is mainly reflected in three ways:

- Transformation of financial institutions' core business;
- changes in customers' needs and profiles;
- arrival of new players in the market.

2.1. New value proposition

Money has constantly evolved overtime, going from tokens to cash and fiat money. Customers' needs and technology have acted as key enablers in providing us with new ways to exchange money. New payment methods are now emerging in our day-to-day life. Amongst them, mobile wallets, contactless payments and virtual currencies are taking an increasing share of the digital payment market. According to Statista (Statista, 2019, p. 25), digital payments are growing considerably and are still expected to grow at a Compound Annual Growth Rate of 13,3% from 2018 to 2023. What is interesting to note is that even though mobile POS[11] payments will keep on increasing, digital commerce will remain the largest segment for digital payments.



Graph 4: Global transaction value forecast in billion US$

[11] Point-of-sale. Mobile POS payments refer to all payments performed in-store using mobile or wearables.

One of the strongest drivers of this development will rely on the ability of banks and payment providers to reorient their business model into mobile-centric business models. Indeed, what comes out of Deloitte's 2018 banking industry outlook (Deloitte, 2018) is that mobile enablement is becoming an increasingly important feature for customer experience. While mobile solutions where previously considered as one of many channels, it will tomorrow be in the middle of banks' business models. This hype for mobile payment solutions is reinforced by factors such as high-speed connectivity and technologies like face recognition that have direct impacts on how users experience their day-to-day payments.

Mobile payments allow to deliver value to customer way beyond the transaction itself. They aim at providing users with additional underlying services and data sharing solutions through user friendly infrastructures. People are more and more looking for aggregated apps allowing them to have a full view on all their accounts and transactions, whether provided by their bank or by other external payment providers. They want to be able to create budgets and manage their money more efficiently. As a matter of fact, an Accenture study (Accenture, 2017) showed that 64% of customers are considering the use of a mobile wallet as of 2020, with the objective to manage their financial information and spend their money in a more convenient way.

This change in banks' and payment providers' value proposition reinforces the digitalization and dematerialization of money. Paper money is slowly fading from the payment ecosystem, leaving the room to all new types of payments using digital money. Cryptocurrencies are therefore enrolled in a continuum of this digitalization phenomenon, where money is no longer going from hand to hand but circulating from crypto-wallet to crypto-wallet.

The place of mobile solutions for financial services is for sure a huge part of the evolution but is of course not the only reason.

2.2. New types of customers

Another huge driver of the changing environment is the emergence of new types of customers as Millennials[12] are getting replaced by Generation Z[13]. These individuals are future customers who were raised in a fully digital environment. They are looking for more and more personalized experiences and want to be able to manage their money where and when they want. They are fully connected and live through their social media platforms. They hence come to reinforce the mobile-centric hype by using their smart phone for any occasion. The Accenture survey (Accenture, 2017) mentioned above also showed that 69% of these individuals use their mobile banking app every day or weekly, compared to a low 17% for baby-boomers (people born from 1946 to 1964).

Generation Z represents tomorrow's workforce. They will thus give more and more power to new digital payment methods by adopting them in their day-to-day life. They will most probably give legitimacy to payment methods that were today feared or misunderstood. Gen Z individuals are deeply anchored in the digitalisation era we are facing and will act as key enablers of this phenomenon in the coming decades.

2.3. Emergence of FinTech

A huge component of the current changing environment is the development of companies leveraging on financial technologies, also called FinTech companies. These companies typically try to answer new customers' needs by providing them with external solutions to perform payments and manage their money. Such highly innovative companies are disrupting the financial sector in its core and represent a real challenge for banks. They are willing to take over the financial industry, with or without traditional players. If banks are not looking for partnerships with FinTech companies, they are likely to face strong losses in market shares. (Accenture, 2017)

FinTech companies have the power to evolve with their environment and thus create new markets never explored as of today. They typically have a strong focus on users, are agile and heavily data-driven. They leverage on technologies such as artificial intelligence, blockchain,

[12] Millennials are all individuals born from 1980 to 1999.
[13] Generation Z are all individuals born from 2000 to 2019. In the same way as Millennials, Gen Z represent a share of the population with specific behaviors and unique attributes representing their part of a century.

machine learning and automated robo-advisors to bring a strong added value for customers. They have the ability to combine state-of-the-art technologies through seamless integrations to deliver convenient end-to-end processes. (Statista, 2019, p. 8)

FinTech companies are now part of the financial ecosystem and should be considered as a strong driving force of the changing environment we are facing today. However, FinTech firms might not be the only new entrants of the financial market…

2.4. GAFA entering the game

Indeed, GAFA[14] are also entering the financial market with the willingness to take their part of the cake. If Google and Amazon have been really quiet on the financial market, it is not the case of Apple and Facebook. They both decided to take the step and become financial services providers, not at the same level though.

Apple

The giant American hardware producer Apple will launch this summer its first credit card called Apple Card. They promise to offer a new generation of credit card coming along with convenient services. They define their Apple Card as being simple to use, transparent and with a strong focus on privacy. Indeed, Apple promises that they will not have any access to their client's financial information. They will have one aggregated app where customers will be able to manage their money and have a full view on their spending's, classified by categories such as already provided by independent financial services providers such as the English Revolut or the German N26.

Apple claims to offer its credit card without any fees and with very low interests that will be estimated in real time before each transaction, depending on your balance and the amount of the transaction. Clients will also get a cash-back equivalent for a percentage of every transaction they do. This cash amount will be stored on an Apple cash account, where users will be able to use, send or collect that money. They will leverage on their existing security mechanisms such as Touch ID or Face ID to allow people to perform transactions in a really effortless and highly secured manner. To improve even more the level of security they promised, the physical version

[14] Acronym referring to the four internet giants: Google, Apple, Facebook and Amazon.

of their credit card is empty of any financial information. There is no card number nor CVV written on the card, preventing users from unhappy missuses of their card. (Apple, n.a.)

Although Apple uses its independence from financial institutions as a differentiating factor, it is still worth mentioning that the American investment bank Goldman Sachs will be Apple's main partner in this project. Goldman Sachs will therefore issue and back-up the credit cards. Amongst the consequent amount of questions raised by this partnership, the previous statement about data privacy is now a bit unclear. Indeed, although Apple promises not to capture its client's financial information, Goldman Sachs will.

Facebook

One of the most promising steps in the financial industry is the one made by the internet giant Facebook with its very recent announcement to launch its private cryptocurrency as of next year. Facebook will shortly introduce Libra, an open sourced blockchain-based infrastructure coming along with an underlying native digital currency of the same name. Their ambition is to provide their two billion users with a solution to buy online and transfer money worldwide at no costs. With this new payment method, Facebook aims at targeting the 1.7 billion unbanked people all around the world to enable them to purchase whatever they want online and exchange money freely. (Kharif, 2019) Customers will be able to buy and pay with Libras in one click at all Facebook's partners such as Uber, Booking.com, Spotify, Vodafone, eBay, etc. They will also be able to exchange Libras between WhatsApp or Messenger users all around the world and at any time, such as this is already the case in Asia with WeChat.

Facebook wants to create a digital currency "that brings together the attributes of the world's best currencies: stability, low inflation, wide global acceptance and fungibility." (Libra Association Members, n.a.) To do so, the Libra Coin will be backed by a bunch of bank deposits and trustworthy central banks securities. Libra will be part of a new but very audacious category of cryptos called stable coins, which are indexed on popular conventional currencies such as US Dollars, Euros or Yen. They will therefore be more stable than cryptocurrencies as we know them today. This feature provides a solution for the question of coexistence between cryptos and conventional currencies, and actually shows that Dollars or Euros can act as enablers of a more efficient and digital version of themselves. We can have the same observation when it comes to the place of central banks in the cryptocurrency ecosystem. Libra doesn't intend to

replace central banks' money but acts as a complement to provide a more efficient, global and free way for people to exchange and transact.

A key difference with Libra compared to other cryptocurrencies is that anonymity is not one of the core principles. Indeed, in order to make money, Libra will keep an eye on users' spending's' and sell this information to its partners. Imagine a user paying for his/her holidays on Booking.com with Libra, the information will then be sold to Uber e.g., which will be able to offer you a driver for your ride to the airport. Facebook promises that it will not collect any financial information itself since Libra's data will be managed by a subsidiary called Calibra. Even though it claims that both entities will have independent databases and will not share information, one might be doubtfully about this statement considering the recent privacy troubles Facebook went through.

Besides its privacy concerns, Libra actually has really interesting technical characteristics. The first promising characteristic is that its blockchain is open sourced and uses kind of customizable smart contracts. In other words, any developer can build apps or platforms with specific features using the Libra blockchain in order to answer a designated financial need. We could e.g. see the development of apps allowing students or young entrepreneurs to manage their money and transact in Libra. The options are unlimited and could potentially lead to a huge financial ecosystem of users with Libra as core unit of value. According to Joe Weisenthal, executive editor for digital news at Bloomberg, if Libra becomes successful and widely adopted, it would actually be much more than a simple cryptocurrency. It would become a worldwide financial ecosystem allowing to process fiat currency-equivalent tokens. (Weisenthal, 2019) On top of its flexible feature, Libra blockchain also has for ambition to be scalable in order to face heavy adoption and worldwide use in the future. It is of course also provided with high level security to protect users' financial information.

The only blurred point in the Libra project is about the blockchain governance. At the beginning, the network will be permissioned and managed by a group of partner companies, NGO's and financial entities. They will be grouped in what will be called the Libra Association, already regrouping e.g. Mastercard, Paypal, Visa, Uber, Booking, Spotify and a bunch of venture capital firms. Libra's objective would be to have around a hundred partners at the launching of the project by 2020. However, in the future, Libra wishes to make its blockchain become permissionless to allow anyone to participate in the validation and development of the

network. It is still unclear how this transition will take place but Facebook should soon clarify this point.

Although the project seems really promising, regulatory authorities already stepped in and promised to come soon with an appropriate regulatory framework that could potentially threaten the project. On top of the common privacy issues, regulatory authorities might also step in to address the fact that financial institutions will get less and less power if Libra starts to be used as a global financial ecosystem. This would then leave room for money laundering and illicit activities. Another big concerns from governments will probably be the fact that they will hardly be able to collect taxes on services and goods that were exchanged on a private network. It is indeed hard to imagine that any government will support the project if they know it will result in low tax revenues. The macroeconomic implications of such developments will be discussed more into details in the last part of the report.

Chapter 3. Use case: Central Bank cryptocurrencies

We talked a lot about the use of cryptocurrencies in a retail and corporate perspective, but what if we could go beyond that? What if central banks could issue their own cryptocurrency that would be used on a global basis to perform real-time, cost efficient and secured payment all around the world? The concept is actually hardly investigated by central banks worldwide in what would take the form of a "Central Bank Digital Currency", also called CBDC.

Central banks play a key role in today's economy by supervising and ensuring a smooth money flow and by supporting banks in their activities. They have the task of controlling the money supply and allowed us to benefit from trustworthy payment systems. Central banks have been involved in the evolution of money overtime and now have the duty to continue doing so by investigating on new types of currencies. As a matter of fact, a study conducted by the Bank for International Settlements (Cartsens, 2019, p. 8) showed that 70% of central banks interrogated were actually investigating in order to understand how CBDC could improve the current monetary system. Half of them even tested the concept to see how it could potentially work and be implemented in a near future.

Central banks quickly identified three key factors that would gradually lead to key changes in the financial ecosystem. The first factor is that demand for cash is slowly decreasing with the

development of contactless and cashless payments such as cards and mobile payments. Technology aims at constantly improving customer experience, leading to lower need for cash movements. However, it is worth mentioning that cashless payments are not evolving at the same rhythm in all countries. While some remain strongly attached to their cash, others like Sweden are moving towards zero cash use and sometimes don't even accept cash anymore. (Cartsens, 2019) A second important factor is of course the development of distributed ledgers technologies that have a heavy potential to transform the way we exchange and store information. Finally, what central banks are keeping in mind is that they are responsible for establishing monetary policies and therefore have to consider the development of a new type of currency that could have an impact on how money is used all around the world. (Coeuré, 2018)

CBDC could take lot of different forms but what comes out the most is to have a digital coin that would be the virtual representation of conventional fiat currencies and that could be exchanged on a one to one basis (same as the JPM Coin seen before). These coins would come in addition of what central banks already provide; cash for individuals and reserves for banks. (Kiel Institute for the World Economy, 2018) They would then be virtual money owned by individuals on central bank accounts, where the latter would act as the trustworthy counterparty that people are missing with current cryptocurrencies. We would most probably have two types of CBDC, the ones used between banks for wholesales transactions for specific purposes and the ones used by individuals for retail purposes. (Cartsens, 2019) If digital coins were owned directly at central bank accounts, they would also probably come along with negative interests that would serve as fees for owning the account.

Even though the concept sounds interesting, it might actually have quite negative impact on the financial system. Indeed, the reasoning is that if people start using more CBDC, this means that deposits at the banks will become less important. CBDC could potentially erase banks from the ecosystem, already pushed out by new innovative entrants. Since banks deposits represent their main source of liquidity, this might have a huge impact on bank's business models that would therefore need to find alternative ways of funding. In the current state, if such scenarios happened, central banks would need to step in to provide them some capital. (Kiel Institute for the World Economy, 2018)

As of today, central bank digital currencies would have a hard time integrating in the current monetary system. Even though they could have a great potential to improve the payment experience, their implementation involves huge changes in the environment and are really not likely to happen soon. Current market infrastructures will hardly be transformed for the only objective to introduce cryptocurrencies. What is more likely to happen is that crypto founders or financial institutions find a way for cryptocurrencies to integrate smoothly in the current ecosystem, causing the less troubles as possible and providing a new and unique experience to customers.

PART III. IMPLICATIONS

Cryptocurrencies are for sure a very challenging innovation representing deep changes in the way we spend money. Such disruptive innovations often come with a bunch of consequences that will need to be handled in order to allow the innovation to settle in the current framework. In this last part, we'll go through a series of questions raised around the impacts of cryptocurrencies. We will first analyse the most important macroeconomic implications that cryptocurrencies could have if their development became wider. This includes some questions raised about the impact of cryptos on the economic efficiency, the financial stability and on the policies set by policymakers. We will then go through some general challenges faced when we talk about the development and use of cryptocurrencies. The chapter will analyse the current state of regulation and go through the different options for regulatory authorities. It will then be followed by an analysis on a key question around the anonymity feature of cryptos and the underlying risk for illicit activities. The chapter will eventually discuss about the high volatility of cryptocurrencies, still representing important concerns for most people. Finally, this last part will end up with the analysis of the technical issues raised by cryptocurrencies. The chapter focuses around the scalability issues of some cryptocurrencies. Huge electricity consumption and network overload are common concerns that represent an important part of the technical challenges currently faced. We will eventually go through the cyber risks of cryptos, which are still representing a considerable unknown and source of fear for most people.

Chapter 1. Macroeconomics effects

Besides some independent implications, it is important to analyse the implications of the development of cryptocurrencies on the global economy. We'll analyse the impact of the development of cryptocurrencies on three key aspects of the economy; the economic efficiency, the financial stability and the fiscal policies. By doing so, we can then have a better understanding on how cryptos could disrupt (or not) the way our economy works. We'll raise different questions to see if the current system can sustain with the implementation of such new technologies and see how the different actors can find it acceptable. For clarity matter, the chapter will keep a global view on the three points and not go too much into details.

1.1. Economic efficiency

The key objective of cryptocurrencies is to improve user experience during payments through more efficient processes. Technology allows to perform cost-efficient, real-time, transparent and highly secured payments. This innovation comes as a response to current processes, which are anchored in an old infrastructure resulting in slow and costly transactions. The introduction of convenient peer-to-peer transactions, without the need for any counterparty, allows to bypass these drawbacks in an innovative way. Improved speed and reliability at lower costs represents a true solution to improve payment services compared to what is offered today. It represents a change in paradigm that will hence have the power to provide a greater economic efficiency.

However, it is still important to remember about the high volatility of cryptocurrencies and about transaction costs, which are still quite unstable and can vary a lot from time to time. Transaction costs of Bitcoin once even overpassed the transaction costs of the current payment system. They represent one of the biggest challenges for scalability of cryptocurrencies. Scalability is an important requirement for the development of a new type of currency and it's essential to understand to which extent cryptocurrencies will reach such requirements. The scalability aspect of cryptos will be covered in the last chapter. Nevertheless, what is already observed is that if transaction costs succeed to be lowered or at least stabilized to a low level, cryptocurrencies could be used as an easier way to perform international money transfers. They would then be huge competitors for traditional players such as Western Union. (Elliott, de Lima, & Singel, 2018) This is actually the same goal that Facebook is seeking with the development of its Libra. One of their main objectives is to be used as a way to send money abroad easily to anyone owning a Facebook account. Such initiatives will have a huge impact on financial inclusion of developing countries and will allow millions of people to benefit from worldwide and costless settlements. Improving the global financial inclusion will increase the number of people participating in economic activities, which will then have a great impact on the economic growth. (Quoistiaux, 2019)

If we look beyond just cryptocurrencies, it is noticeable that blockchain also has the power to significantly improve the economic efficiency of current processes in multiple sectors like identity management, healthcare or public processes such as voting systems. With the use of tokens, blockchain could allow closed environments to work in a much more efficient way. Users of a private system would then use tokens as a unit of value to exchange goods and

services, with the same principle as the Ethereum network. Such cases could be found e.g. in the agricultural sector, where actors of the network would use their unique tokens to exchange goods and services much faster, cheaper and without any intermediaries. The network would then be able to work more efficiently and deliver value more easily to its surrounding environments. Using a cryptocurrency in a single industry could help revitalizing the system by providing it with a new way to value and exchange work. Such improvements come from the fact that a system works much faster and cheaper if the number of intermediaries is kept low. Few intermediaries working efficiently would allow much lower transaction costs and high speed, resulting in more efficient working systems as a whole. (Gailly, 2015)

Technology is improving every day and the scope of usability is huge. Experts are still experimenting to see where it would be best used. It is clear that problems currently faced will be solved in the coming years and if not, the technology will adapt to suit our needs in the best way possible. We still don't know where cryptocurrencies will take us but it will most probably remain under high surveillance for the next decades. Cryptocurrencies may not necessarily be the key domain of innovation in the current system, maybe the economy itself will adapt to enable cryptos as a more convenient way to transact… the future of cryptocurrencies is not clear enough to predict what is going to happen. We know that cryptocurrencies have the power to improve efficiency of payment systems, resulting in greater financial efficiency and growth. The only thing is that big changes in a global environment rarely happen without contestations. People are usually scared by change, especially when it comes to their money. The development of cryptos and the impacts on economic efficiency are at the end of the day a matter of adaptation. The key question is to know who will adapt first; will the economy adapt to cryptocurrencies or will cryptocurrencies adapt to the economy? Both sides have their own interests and the future will probably tell us more about it.

1.2. Financial stability

Besides the fact that the economy needs to work efficiently, it is also of a high importance to make sure that the system remains stable and sustainable. Introducing a new type of currency might threaten the whole financial stability of the monetary system if not well managed.

In order to understand to what extent the financial stability might be threatened, let's first have a definition of what is a financially stable system according to The World Bank.

> A stable financial system is capable of efficiently allocating resources, assessing and managing financial risks, maintaining employment levels close to the economy's natural rate, and eliminating relative price movements of real or financial assets that will affect monetary stability or employment levels." (World Bank Group, n.a.)

In fact, some of the characteristics of this definition might be affected if some current issues related to cryptocurrencies are not solved. In the current state, a sharp growth in cryptos could have a big impact on the financial stability for different reasons. The factors that might impact the financial stability are the volatile level of prices, the low level of protection of users and investors and the low adoption level. (Elliott, de Lima, & Singel, 2018)

The price volatility of cryptocurrencies is one of the most common criticism made to this new type of currency. If cryptocurrencies were developed more widely and if volatility remained an issue, leverage could go up and down at a rate that would threaten the financial stability in its core. However, it is still worth mentioning that this scenario is a hypothetic scenario where volatility issues are not treated. In reality, cryptocurrencies and their underlying technologies are constantly adapting and improving to solve arising issues. As a matter of fact, volatility is nowadays nearly fixed with the development of *stable coins* being indexed on strong conventional currencies. Most problems will often come with a solution, it's just a matter of time to know when they will be made public.

The second factors impacting financial stability is the low level of protection for users and investors due to the lack of regulatory entities for the use of cryptocurrencies. In fact, institutional investors currently have a low level of involvement in the development of cryptocurrencies as a mean of payment due to important counterparty risks, security risks and operational risks. Even though the high transaction speed of transactions with cryptocurrencies reduces the systemic and credit risks, they are still subject to other issues. Cryptocurrencies being independent from financial institutions therefore heavily depend on the companies issuing the tokens and might be facing cyber-attacks or technical issues. These last two points will be analysed more into details in the next chapters. Improvements in investor protections would be beneficial to the development of cryptocurrencies at a larger scale, coming along with a higher adoption of the technology.

Besides the investors side, user adoption is also important to be followed closely in order to ensure the sustainability of the development projects. The low level of adoption usually comes from the fact that people have a hard time trusting a system that is not backed up by any governments or financial institutions. In addition, the complex technology underneath cryptocurrencies is another source of misunderstanding and fear for most people. Although adoption from people is important in terms of development, it is even more important to monitor the relationship that financial and regulatory entities will have with cryptocurrencies. Indeed, if adoption gets more important and financial entities don't act to include them in the environment, financial stability could be really threatened and potentially lead to multiple parallel financial ecosystems. Such scenarios would be dramatic for the overall financial stability, leading to the erosion of the payment system as we know it. The opposite scenario in which authorities step in to integrate cryptocurrencies in their processes is much more friendly and would be less dramatic for the overall financial stability.

What will act as a determinant for financial stability is the role financial institutions will play in the development of cryptocurrencies. Banks can either ignore this new type of currency or integrate them in their processes to ensure a stable development. Even if some cryptocurrencies work without banks as intermediary, that's not the case for all of them. In contrary to what most people think, the development of cryptocurrencies doesn't necessary means that banks will be excluded from the framework. Some cryptocurrencies such as Ripple work with financial institutions as clients to provide them with a new way to perform interbank transactions. Banks can have a role to play in the development of cryptocurrencies. It will be their duty to understand and evaluate how can cryptos improve their processes. If banks and regulators fail to adapt to the technology, financial systems will be distorted and potentially lead to the destruction of the role of banks for payment services. Banks could easily be replaced by more convenient and innovative competitors entering the market with strong technologies in their hands.

However, if banks lose their role as payment providers, this would have dramatic impacts on financial stability as a whole. Since deposits represent the main source of liquidity for banks, it would be very problematic if other players came to replace them as payments services providers. On top of that, in a world where cryptocurrencies have a more important place, the supply mechanism of money would have to be revised. Indeed, as of today, banks create money by granting loans to individuals to help them in their projects. As we saw earlier in this report, supply for cryptocurrencies are set by the companies issuing them and can have different forms,

either fixed or variable. The question is then to know how it will be possible for banks to lend money and keep a stable money supply at the same time, knowing that most cryptos are created through a mining process. Another question is to know how to decide when banks and individuals would need to use conventional currencies and when would they use cryptocurrencies. It will then be required to define how it is possible to ensure a stable level of money, whether conventional or cryptocurrencies. (Gailly, 2015)

These are so many questions that are still left without any answers but will probably need to be tackled in the future. What is for sure is that whoever will be answering such questions will have a huge impact on the global financial stability. These people will have into their hands a very powerful innovation that can either be an amazing way to revolutionize payments, or either threaten the whole financial system.

1.3. Fiscal policies

One of great fear of governments nowadays regarding cryptocurrencies is to know if they will threaten their ways of collecting money through taxation. When cryptocurrencies started to get attention and generated profits for investors, governments' first reaction was to find a way to categorize them in order to collect taxes. The only issue is that cryptocurrencies can be obtained from different manners, either from mining, when exchanging them for goods & services or when bought for investment purposes. Finding a way to tax cryptocurrencies would then require three different frameworks, which would be quite hard to set. The most common options would be to set different policies with taxes on sales, taxes on transactions and taxes on profits. These are current policies that could more or less fit what cryptocurrencies do. However, some drawbacks make it hard to collect most of these taxes. Authorities around the world are moving towards policies defining cryptocurrencies as a capital asset, implying taxes on capital gains.

The biggest issue faced by tax authorities is about the different existing types of cryptocurrencies and their underlying technologies. In fact, applying taxes on individuals of a private network is easy since people can usually be identified. But what if we're facing a permissionless cryptocurrencies where users are only identified through their pseudonyms and cryptographic address? It's therefore much more complicated to identify the revenues made by each people and associate them with an individual legally speaking. Finding policies for such cryptocurrencies is quite tricky but some solutions exist. One solution would be to lose the

anonymity feature of cryptocurrencies by making the link between cryptographic wallets and real-life individuals. Tax authorities would then be able to see the revenues made by each person and collect taxes on them. However, even though the solution seems to be the best for tax authorities, it is quite unlikely that such changes happen since anonymity is one of the key aspects of cryptos. The fact of being anonymous provides them with a real added value for people wanting to avoid government's control. Still, it is clear that revenues made through investments in cryptocurrencies should be classified and taxed appropriately. There is no reason why this type of profits shouldn't be regulated for the only matter to maintain anonymity of its users.

The other solution relies on trust in investors and implies the help of cryptocurrencies exchanges. Such platforms could help tax authorities by providing their client's ID and revenues in order to be legally taxed. The only thing is that regulations protecting clients' data will hardly allow such agreements. What is already done today by some exchange platforms is to help users by providing them with tax reports through automatically generated forms including their capital gains coming from trading activities. It then relies on peoples' sincerity to send these forms to tax authorities. (Elliott, de Lima, & Singel, 2018)
Fiscal policies regarding cryptocurrencies are still very unclear and will need to be fixed in order to ensure a trusted and legit development. We need ways to have an equal and safe way to tax the different types of cryptocurrencies. Distinctions should of course be made between investment uses and transaction uses but whatever the purpose, differences in technology remain a quite problematic drawback.

Another issue is the worldwide dimension of cryptocurrencies that is hardly matching the different fiscal regimes across each country. Cryptos are global and not related to one country or another. If people are not identifiable, how should we define which fiscal policy to apply for which individuals? Tax authorities around the world should coordinate in order to set global or in-lined fiscal policies for cryptocurrencies.

Chapter 2. Challenges

Cryptocurrencies totally disrupt the way we perceive money. Technology is enabling to perform transactions in a new way, therefore considerably transforming the paradigm we all know. Whatever the advantages and drawbacks of the technology, its development necessarily implies some important challenges and risks that need to be addressed. This chapter will focus on four of the most discussed challenges when it comes to cryptocurrencies development; the state of regulation, the underlying illicit activities enabled by the anonymity, the user privacy in such an open-sourced environment and the extreme volatility level of prices.

2.1. Regulation

The question of regulating cryptocurrencies is probably the most discussed one. In the current state, legislation is blurred because current laws are hardly applicable to this new technology. This blurred legislation led to misuses from malicious individuals and hence tainting cryptocurrencies with a bad image.

Governments around the world are trying to better understand this new type of currencies in their multiple aspects. Taxation, money laundering, money tracking and illicit activities are all concerns governments are trying to address in order to prevent all fraudulent actions. However, regulatory entities are having a hard time coming up with solution because cryptos go against all regulatory standards we have today. Control and security are things that governments can't control with this type of technology. They are asked to go against all their core principles by providing countries with a framework for such currencies.

Governments are testing laws that would be able to regulate the use of cryptocurrencies, each at their own pace. Some countries have hard opinions on the technology and decided to ban cryptocurrencies from the country. On the other hand, some have more friendly opinions and either authorize or warn their population about the risks associated with them. Each government then has its own regulation of cryptocurrencies according to their interpretation. As an example, the United States gave full power to its States to set independently the legislation they find the most appropriate. Since there are no standards or best practices, some states decided to apply some restrictions, some decided to impose licenses and some simply warned their population about the risks associated with using cryptocurrencies. (Girasa, 2018)

The thing is that having multiple laws and interpretations don't match with the worldwide and anonymous features of cryptocurrencies. Since tokens can travel from a continent to another in a few seconds, they require a global and worldwide framework in order to avoid any misuses, whether coming from cyber criminals or from countries themselves. As a matter of fact, North Korea has been investing in mining machines in order to make money to finance their nuclear missiles. They accumulated around $670 million worth of Bitcoin by confiscating cryptos illegally owned by their citizens and by heavily mining cryptos. (Cuthbertson, 2019) Such cases are examples that show that a global regulation is required in order to avoid any threats, whether coming from individuals or hostile countries.

As of today, there are no perfect solutions for regulating cryptocurrencies. Regulatory authorities might have different options, depending on the types of cryptocurrencies they want to regulate and who they want to involve in the process. The outcome could then lead to either extreme measure or more friendly scenarios. Players from all around the world have proposed recommendations or path of answers to this tricky question.

The consulting company Oliver Wyman has imagined three scenarios of possible actions policymakers could take in the future. (Elliott, de Lima, & Singel, 2018) In the first scenario, policymakers would ensure an efficient operation of the markets by ensuring stability of prices, liquidity resources and fair distribution of wealth between all players in order to avoid bigger players to take over the market. This approach focuses on ensuing a stable workload to both current players and new players entering the market. It has the objective to ensure stability of the system and focuses on the global aspect of cryptocurrencies. The second scenario is a scenario in which policymakers would provide a full customer protection through standards regulating the scope of action of service providers. Some examples would be to set price regulations and privacy protection mechanisms. The most important parts would probably be the day-to-day transactions in a world where cryptocurrencies would be much more developed as an alternative mean of payment. Such service providers would have to work actively with policymakers to provide enough protection to users in order to encourage them to participate more and more in the market. An increased user protection would allow people to better trust the system, hence improving the level of adoption. The last scenario is more about the task of policymakers to follow closely how the current monetary system evolves and to be able to position themselves in the cryptocurrencies ecosystem. They will have to make sure to

perpetuate the role central banks and financial institutions play today by ensuring financial stability and efficiency of the system. Regulatory authorities will need to monitor closely how the relationship between the current system and a potential new system will evolve. It is however hard to say if we need to take preventive actions to impose the cohabitation or if it's better to wait and see how the two systems will adapt by themselves. If the choice was made to take preventive actions, it would be a great responsibility for policymakers to decide about the optimal solution to take.

However, what policymakers can already do is to set regulations and limits to current market players in order to avoid common illicit activities and opportunistic behaviours. Even though anonymity makes it hard to identify users' transactions, exchange platforms e.g. could be involved in the process and communicate all suspicious transactions operated on their platforms. On a global perspective, if a relevant regulatory framework can be set, this would allow to reinforce trust from users and market participants. The level of adoption would then significantly increase and cryptocurrencies could eventually be considered as a legit alternative for payments. The main drawback coming with imposing regulations is that it would probably increase the costs for market players to participate and possibly limit the innovation. It's not a surprise to say that regulated environments usually have a lower room for innovation and that's actually exactly why cryptocurrencies were born. Bitcoin, the first cryptocurrency, was created by Satoshi Nakamoto with a level of innovation totally unknown in the payment ecosystem. The key reason for this innovation is that not any regulators never ever imagined such things could exist. There was therefore free room to create whatever was possible. In a regulated environment, innovation could hence be limited.

2.2. Illicit activities

Amongst the multiple challenges' cryptocurrencies have to face, one of them is that fact that the technology enables a series of illicit activities. In fact, the anonymity feature of cryptocurrencies has two-ways consequences. While some might find it beneficial to act anonymously in order to avoid being tracked and controlled by banks and governments, some saw in the technology a way to perform illegal activities. The sad reality is that Bitcoin was first known and heavily criticized because it was used by cyber criminals to purchase drugs, bypass tax payments, finance terrorism, enable money laundering and buy any other illegal products or services on the so-called "dark-net". As a matter of fact, it has been proved that

Bitcoin was used by Islamic terrorists such as the ISIS[15] organisation to collect money from their supporters in a totally anonymous way. (Girasa, 2018) Even though terrorists might be restricted by their country's regulation restricting the use of exchange platforms, it still represents a way for them to receive and use funds in a different and anonymous way.

Such activities are getting more and more easy to perform with the development of distributed ledgers allowing individuals to transact anonymously. Even though cash money allows to perform the same activities, regulatory frameworks have been set to all counterparties in order to avoid such things to happen. For example, banks are now required to respect some compliance checks such as KYC[16] and AML[17] in order to avoid any suspicious or fraudulent activities. The thing is that cryptocurrencies are provided with an additional technological complexity, making it harder to identify fraudulent individuals. We therefore need to set some new frameworks and control mechanisms adapted to the underlying technological complexity. (Elliott, de Lima, & Singel, 2018)

In some cases, cryptocurrencies even made anonymity one of their key characteristics in order to differentiate themselves. Anonymity can be nearly total in some permissionless cryptocurrencies networks. They only thing related to the users are their cryptographic address, which is a long series of letters and figures. Besides that, people are only using pseudonyms to represent themselves during transactions. The only way to track down a user is through a complex manipulation allowing to trace back the IP address of the individual. Such thing is quite hard to do but can be easily performed by well trained hackers. In fact, some governments are already working with private companies in order to bypass the anonymity and track every movements of money. It is then possible to find back the identify of some users by tracking the transactions made with their cryptographic address.

The issue with anonymity is that it creates some doubts on how useful is a currency that is mainly used by criminals in order to buy illicit products on the dark-net. It gives a false image of what cryptocurrencies really allow to do and hides the real potential they have to considerably improve efficiency of payments. What needs to be taken into account is that the

[15] Islamist State of Iraq and Syria
[16] Know Your Customer is a compliance requirement for banks to collect relevant information on their clients with the objective to avoid fraudulent activities and money laundering.
[17] Anti-Money Laundering is a regulatory check allowing to avoid money laundering.

primary purpose of cryptocurrencies is not to perform illegal purchases online. It is true that cryptos facilitate to perform illicit activities but such things were actually already possible before. Technology simply made it more easily accessible because of the lack of regulation.

Whatever its form, the development of cryptocurrencies might improve with an increasing regulation and involvement of all market participants. People would then probably see them as a legit way to exchange goods and services with greater privacy. However, some cryptocurrencies might be adopted more easily depending on their underlying architecture. One of the easiest ways to avoid anonymity issues is with permissioned cryptocurrencies, where the governing entities would be able to track and regulate the use of cryptocurrencies in their network. Permissionless networks are trickier to regulate since there's no bank equivalent for AML and KYC checks.

On a general perspective, illicit activities could be treated in the future but it might take some time and not be total. In order to reach such situations, it would first be important to fully understand the technology and find manners to bypass technological complexity in order to stop fraudulent individuals or entities. Priorities should then be set in order to tackle the most threatening activities such as terrorism financing or drugs dealing. Finally, the most important point would be to involve private companies and any counterparty interacting with cryptocurrencies in order to set compliance and regulatory checks. Solutions could e.g. be to involve exchange platforms or crypto wallets by requiring them to ask for the clients' ID when creating an account. (Elliott, de Lima, & Singel, 2018) They would then be able to report to regulatory entities any suspicious funds movements. The only checks required afterward would be for people wanting to exchange conventional currencies into cryptocurrencies in order to avoid money laundering. Real transactions using cryptocurrencies wouldn't need to be controlled, except for abnormal amounts. It will also be necessary to make the distinction between users using cryptos for investment or speculation purpose and people using cryptos for transaction purpose. Again, we would need to set a global framework defining the responsibilities of each market participant in the process in order to avoid any other illicit activities to be performed.

2.3. User privacy and protection

Nowadays, data is getting more and more important for businesses who are willing to collect extra revenues and engage more customers. Whether it's for regulation purpose or for business purpose, financial institutions are collecting their clients' financial data. This allows them to have a good view on their customers and better understand their needs. In addition, what happens today is that PSD2 regulation forces banks to provide their customers' data to big companies if the client agrees to do so. Huge firms such as the GAFA can then have full access to your preferences and hence provide you with better offers and services in order to extract better revenues. (Claerhout, 2019)

In a world where data is getting more and more important, one could then ask if such situation would get even worst if cryptocurrencies came in addition in the framework. Will it become mandatory to share our data with big companies like GAFA? What if people don't want to have their financial information spread for business purposes? The question is worth to be asked if we take e.g. the cryptocurrency that Facebook is creating. Transactions performed in Libra will indeed be sold to other private companies in order to increase their revenues and offer more appropriate content to their customers. However, data privacy is really unclear and it hasn't been stated if customers will have the right to refuse having their data shared with Facebook's partners. Since there are still no regulatory framework applicable to cryptocurrencies, it is hard to tell if customers' data privacy will be respected or not. Still, from what we know today, the sales of clients' data to its partners will be the main source of revenues for the Libra Association. It is hence hard to believe that the Association will take the risk of granting the right to their clients to choose if they want or not to have their financial information shared.

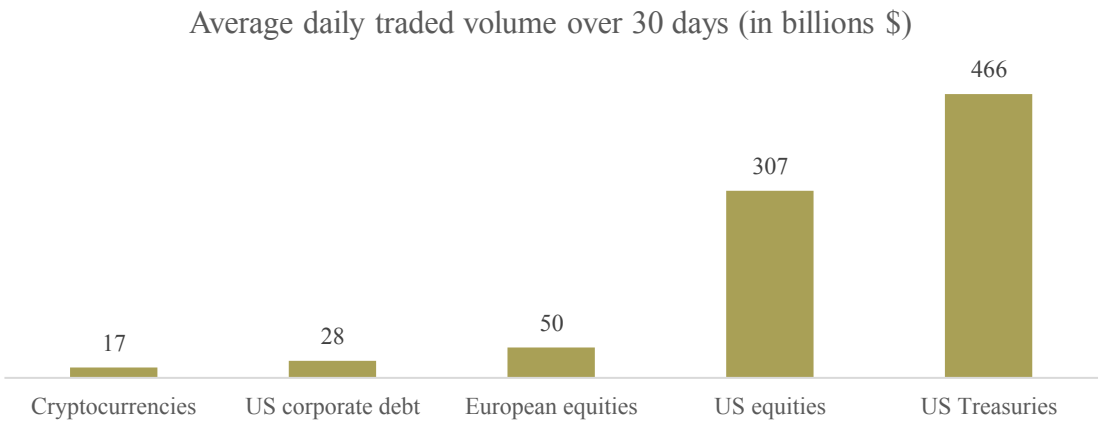
The other side of the problem is the very low level of protection provided to users in case of problems. If a crypto-wallet or an exchange platform gets hacked, clients' financial information and money could be lost or used for illicit activities, without any ways to avoid it. Users don't have anything to do if such things happen. There are not any insurances or bank obligations to restore the stolen money because no regulatory entity is there to cover the risks. Whether it's for inheritance or litigations, data management with cryptocurrencies is really hard to handle because of the high level of security and complexity. As an example, it would be nearly impossible for the family of a dead individual to recover the cryptocurrencies the person had in its cryptographic wallet. If the person didn't communicate its cryptographic key and passwords

with its family, the cryptos are then lost on the platform without anyone being able to retrieve them. It is still hard to tell if cryptocurrencies users will be able to benefit from same protection mechanisms as the ones we have today, considering the high level of complexity. There is the strong need for control coming from regulatory entities or any other player willing to enter the market with such solutions. (Elliott, de Lima, & Singel, 2018)

2.4. Volatility

Since their beginnings, cryptocurrencies are facing extreme changes in value, with an average volatility 12 times higher than the Yen. (Landau, 2018) They are much more volatile than any other conventional currency or investment product such as commodities or the US stocks. Of course, the level of volatility depends on the type of cryptocurrency we're talking about and on its underlying architecture. However, what is common to all of them is the fact once introduced, it immediately becomes the target of investors willing to extract easy money through speculation. Their volatility indeed provides them with great changes in value, representing potential higher profits but also higher risks when investing in such products.

This high volatility can be explained by the very low value of traded volumes compared to other most traditional markets. Liquidity is hence much more limited, which makes them even more sensible to any changes in demand. Since the demand for cryptocurrencies is changing a lot, this results in prices moving at the same rhythm. Another factor impacting the volatility is the fact that cryptos are often really interconnected. In other words, nearly all of them can be bought with another currency, without the need for a fiat currency equivalent. Some of them don't even have a fiat currency equivalent and are only dependent on other's value. The result is that in order to buy a specific crypto, one would then need to first buy e.g. bitcoins in order to make the transaction, hence impacting the demand for bitcoin. One last reason is that the cryptocurrency market is still quite young and benefits from lot of enthusiasm from investors willing to make profits. It is however still not predictable if speculation will keep on going and if their value might potentially stabilize at some point. (Kiel Institute for the World Economy, 2018)



Graph 5: Cryptocurrencies' average daily traded volume over 30 days compared with major traditional segments

Source: Sanford C. Bernstein note citing CoinMarketCap, CBOE, Coindance, SIFMA

What can still be noted is that there's an increasing link between cryptocurrencies and fiat currency exchange. Investors and financial institutions are more and more willing to exchange cryptos into conventional currencies, which actually shows a kind of confidence from their side. The only risks related to such investments is if banks start using cryptocurrencies derivatives or to back up their assets with cryptocurrencies. The value of these assets would then become much more volatile and banks would need to set aside a greater part of equity as security. Risk management with such products would then become much trickier.

This move from financial institutions also comes with a general trend implying lower speculation and leaving more room to experiment the real objectives of cryptos. Players of the market are evaluating the potential functional use cases cryptocurrencies could provide in order to fulfil their key role that is to act as an alternative to traditional payment systems. Technology is adapting and new types of cryptocurrencies are created in reaction to current problems. This is how more and more new cryptos are considered stable coins and are indexed on conventional currencies in order to avoid the usual extreme volatility. Solutions are coming from everywhere, whether from market participants or from new entrants such as GAFA or even countries themselves.

Cases mentioned earlier in this report are perfect examples of reactions from current or new players to provide a more stable and convenient way to perform payments. Facebook's Libra will typically be indexed on a bucket of four of the most popular fiat currencies in order to keep

a stable value and hence represent a viable medium of exchange and unit of value. The JP Morgan coin is another example where the coins is worth exactly the value of one US dollar. Users can then benefit from all the benefits of decentralized currencies while keeping a value that allows them to transact without worrying about volatility. Such cryptocurrencies hence become a more credible alternative for day to day payment, a thing that is hardly reliable with the current volatility. Another even more impressive example is the case of Venezuela who created their own crypto called Petro with a value being indexed on the price of a barrel of petrol in Venezuela. (Pollock, 2019)

All these examples show that solutions can be found to tackle such problems. The evolution of the technology and the involvement of market participants in finding alternatives will tell us if the future of cryptocurrencies will be bright or not. We'll probably have to wait another few years in order to tell if some solutions are credible enough in order to represent more efficient and convenient alternatives to the current payment system.

Chapter 3. Technical limits

Besides the regulatory challenges, cryptocurrencies also suffer from strong technical limits that have an impact on their level of adoption. Electricity consumption, infrastructures saturation and cyber risks are three of the most discussed and challenging of them. These are technical limits that can have a real impact in case of a potential development of cryptocurrencies.

3.1. Electricity consumption

Amongst the different critics made to cryptocurrencies, the huge electricity consumption is probably the most controversial. In a world where people are focusing more and more on the ecology, it seems totally insane to spend a huge amount of electricity to create a currency that is barely used for real transactions. Indeed, cryptocurrencies using blockchain and that require to perform a validation process through Proof-of-Work are consuming a considerable amount of electricity, sometimes equivalent to the annual electricity consumption of countries like Austria or Venezuela. (Halaburda & Sarvary, 2016) As a comparison, the Bitcoin's energy consumption could e.g. power 22.1% of the global energy used in the United Kingdom or 63.7% of the Netherlands (see graph below). (Digiconomist, 2019)

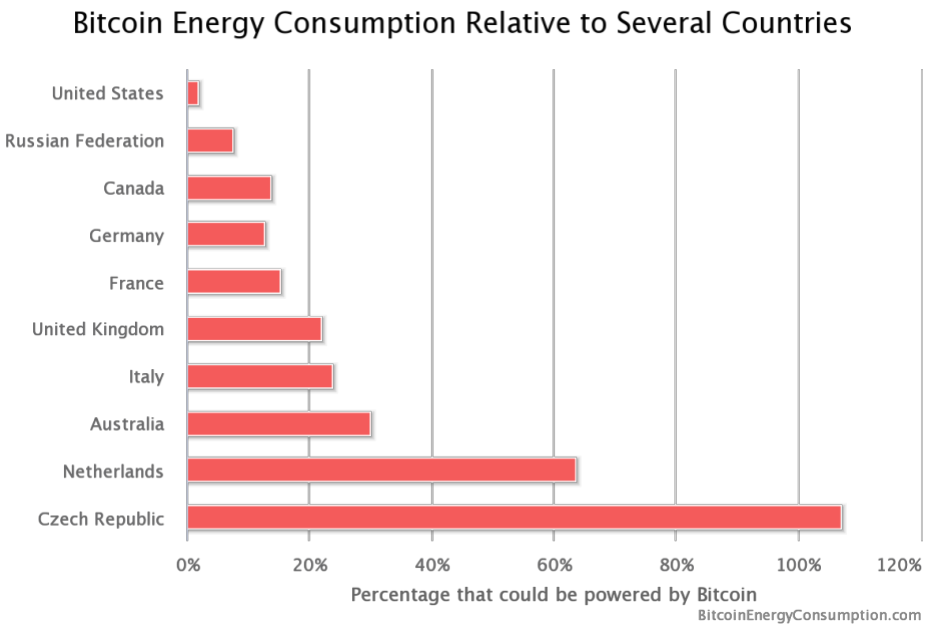


Figure 6: Bitcoin energy consumption relative to several countries (%)

This gigantic energy usage is explained by the fact that solving Proof-of-Work puzzles requires super-computers with huge computational power. These computers are extremely energy voracious and hence implies an energy footprint of around 635 kWh for every transaction performed in the network. As an example, the estimated annual electricity consumption of Bitcoin is currently worth the deplorable amount of 73.12 TWh (approx. 73 120 000 000 kWh). The huge energy consumption comes from the fact that miners are competing in order to be first to solve the cryptographic puzzle and hence receive newly created Bitcoins. In order to update the ledger with a new transaction, all miners have to validate every single transaction of the ledger. (BIS, 2018) The most shocking thing in the process is that only one miner "wins" the puzzle, which means that all the efforts and electricity consumed by the others were useless. The quantity of electricity wasted during the Proof-of-Work represents one of the most important technical impact faced by cryptocurrencies.

Mining cryptocurrencies therefore creates considerable negative externalities, mostly on the environment. As a matter of fact, when translated into carbon footprint equivalent, we can see that each new transaction with cryptocurrencies generates on average 301.4 kg of CO2. (Digiconomist, 2019) The electricity production needed to run the super-computers has a direct impact on our planet and its ecosystem.

If cryptocurrencies were more widely adopted and developed on a global basis to serve as an alternative to current payment systems, it is for sure that our planet would suffer from severe externalities. This huge electricity consumption isn't sustainable and hence represents a barrier to a more global adoption. It is very unlikely that governments and regulatory authorities allow the development of a technology producing such amount of CO2 without any sufficient reasons. However, technological problems are usually very quickly tackled by experts who then provide better solutions to keep on using cryptocurrencies without using that much electricity. This solution is called the Proof-of-Stake and will be discussed in the next section.

3.2. Infrastructures overload

In addition of being very energy voracious, the technology behind cryptocurrencies might also be facing some limits in terms of scalability. The first thing pointed out is the potential network saturation that might happen due to an increasing size of the different blockchains. The Bitcoin blockchain e.g. is getting bigger and heavier every quarter, now reaching around 227 000 megabytes such as shown on the below graph. (Blockchain, 2019)

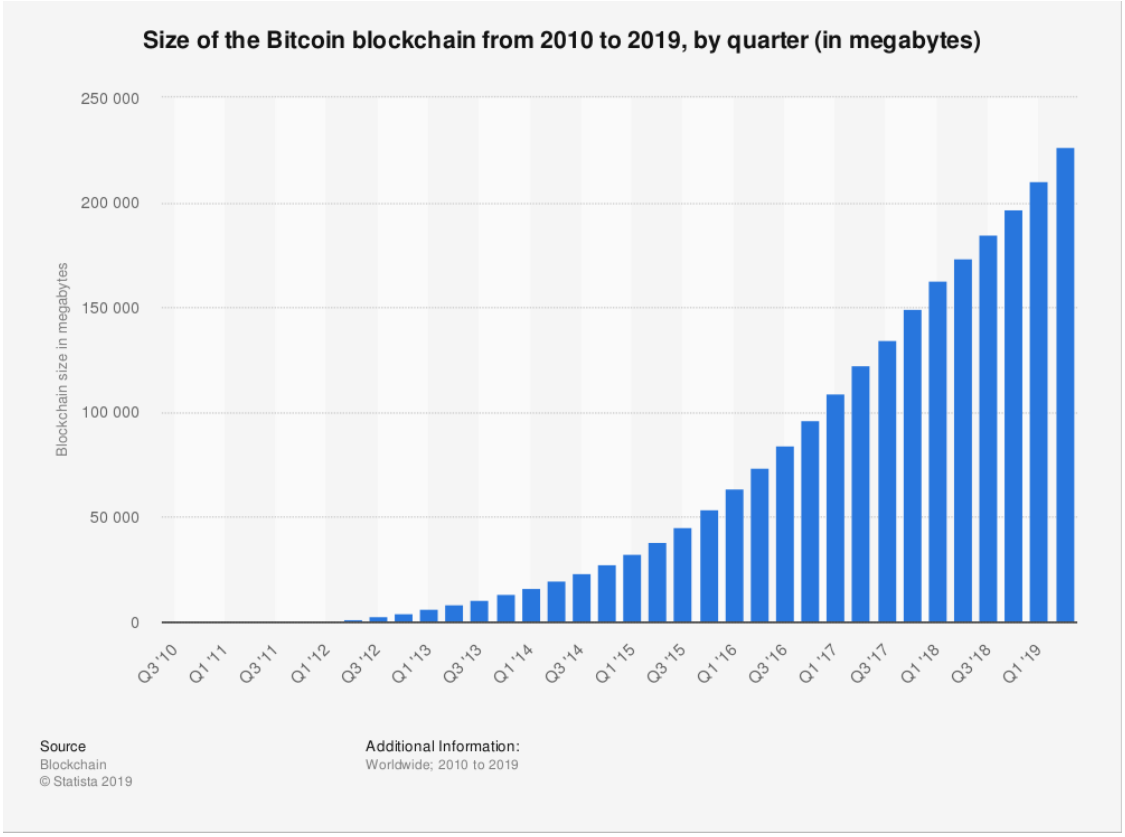


Figure 7: Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes)

This increasing blockchain comes from the fact that the Proof-of-Work process is having a hard time handling high volumes in order to validate all transactions. Every transaction weighs the network with a few more hundred bytes, making the ledger more and more heavy to be supported. As a result, the validation time of transaction will be increasing overtime and weakening the previous advantages of cryptos. The explanation of this longer validation time is that in order to validate a transaction, miners have to go through the whole history of the ledger and verify every single transaction already performed until they reach the last one. (Landau, 2018)

The current technology seems hardly scalable and might be quite weakened if the number of transactions came to increase overtime. A broader development of cryptocurrencies would have an impact on their ability to be used for day to day transactions, hence characterized by slower transactions. The investments required to run the ledger would also considerably increase with the growth of the required processing capacity. Indeed, a heavier ledger involves the need for stronger and more powerful computers to validate transactions. Consequent investments in really complex computers would then be essential in order to stay competitive, hence increasing the transaction costs of cryptocurrencies transactions. (BIS, 2018) Another technical challenge related to scalability and that might increase the transaction costs is the supply regime of some cryptocurrencies. Bitcoin rewards will decrease overtime in order to reach a fix total amount of bitcoins. This means that at some point, miners will not receive new bitcoins from mining and will then ask for additional fees, which will increase again the transaction costs.

What comes out of these technical challenges is that if cryptocurrencies were developed more widely, it is really likely that transaction costs and time will increase. The more adoption will increase, the less the technology will be efficient. It might not be impossible that cryptocurrencies using Proof-of-Work become less efficient that traditional payment systems. If such things happened, we would probably see this technology disappear for a more appropriate one. In fact, cryptos specialists have already been working on a new type of validation process that might solve most problems described earlier. This solution, the Proof-of-Stake, might have an increasing place in newly created cryptocurrencies and represent a more efficient alternative to verify transactions.

THE PROOF-OF-STAKE AS A VIABLE ALTERNATIVE

Proof-of-Stake (PoS) is a new validation process that has the potential to replace the current Proof-of-Work (PoW) process, characterized as too expensive, too slow and too energy consuming.

While PoW relies on competition between miners in order to be the first to solve the cryptographic puzzle, PoS relies on an algorithm that choses the creator of a block according to the stakes the user has in the cryptocurrency. This first distinction already creates a huge difference in terms of energy consumption. Since miners don't have to compete anymore, there is no huge amount of electricity spent and wasted in the competition. The only energy used will come from the computer of the user who was granted the right to add a new block on the ledger.

The second key distinction is the underlying reward structure of the PoS validation process. In this process, users are not rewarded with newly created cryptos but rather receive fees on the transactions they validate. Such structure can have a huge impact on the supply policies of cryptocurrencies and could allow to define new ways to control the supply of a specific crypto. New mechanisms could be put in place in order to better manage the quantity of cryptos in circulation and therefore better control volatility.

Finally, the fact of using an algorithm granting the block to a user according to its shares also has great impact on security. With such mechanism, it is very unlikely that a fraudulent actor takes control of the ledger. The reason is because in order to do so, the hacker would need to own more than 50% of the total amount of cryptocurrency in circulation. Such scenario is of course very unlikely to happen and hence provides the cryptocurrency with a greater security. (Rosic, 2017)

3.3. Cyber risks

The last considerable technical limit of cryptocurrencies is the cyber threats they may be facing. Indeed, even though blockchain technology allows to solve current risks and improve the efficiency of business processes, they also create new underlying risks. These are risks related to the underlying technology or more precisely to third parties willing to disrupt the system, whether to steal money or important financial information. Market participants now have to find new ways to protect against risks that were usually managed by regulatory entities. (Deloitte, 2018)

The risk of cyber-attacks is really important to take into consideration when talking about the development of cryptocurrencies. It has a direct impact on the trust granted by people and hence on the level of adoption. This increasing fear for cyber-attacks is totally legit since it questions the reliability of a technology supposed to secure people's money. Such threats are getting more serious day after day since cyber criminals are getting more and more sophisticated to perform such attacks. Their technology is evolving at the same rhythm as the one used to run a cryptocurrency network. At some point, cyber criminals are even considered as national security threats since they have the power to steal massive data amounts or steal money that could serve to finance terrorism. Attacks are a reality but the level of attacks will depend on how important the cyber criminals want the attack to be. The Defense Science Board of the US Department of Defense classified cyber opponents in six tiers depending on the level of threat they represent. (Defense Science Board, 2013)

Tier I and II are cyber criminals using easily accessible techniques. One of their most popular attack is the so-called 51% attack which consists in taking over the mining power of a ledger. This attack is usually done by the two first tiers but might require the help of higher tiers in order to be more effective. The 51% attack, also called the Goldfinger attack, threatens the trust process underlying cryptocurrencies. Indeed, in order to validate transactions, miners have to go through the Proof-of-Work and reach a consensus of more than 50%. Once a consensus is reached, a new block can be added to the ledger. What happens during a Goldfinger attack is that a group of miners or hackers succeed to have enough computing power to take over more than 50% during a Proof-of-Work process. These individuals hence control the majority of the ledger and have the power to decide which transaction should be added to the network. They might then add some fraudulent transactions in the ledger or block some specific transactions.

Such attacks can be performed by cyber criminals who heavily invested in computers better performing than the average computational power of the market. They have hence enough mining power to win the Proof-of-work and have a majority during the consensus process. Another way to conduct the 51% attack would be to hack other mining pools and take over the mining power. (Baron, O'Mahony, Manheim, & Dion-Schwartz, 2015) We're talking about mining pools when few individual miners decide to regroup in order to leverage their computational power and have more chances to win the Proof-of-Work process. If a mining pool gets big enough, it might have a chance to reach more than 51% during the consensus process, even without any malicious intentions. That's what actually happened with the Ghash.io group who briefly reached the majority but immediately stopped and apologized. (Halaburda & Sarvary, 2016)

Tier III and IV are opponents performing attacks with self-made hacks, mainly focusing on breaches and weaknesses of a network. Such attacks are called zero-day exploits, which means that they succeed to find a vulnerability of the network that is unknown by the owner of the system. (Baron, O'Mahony, Manheim, & Dion-Schwartz, 2015) They can then e.g. modify the rules used to validate transactions or to grant cryptos to miners as rewards for mining. They potentially have the power to attack exchange platforms or mobile apps using cryptocurrencies with the intention to steal funds.

The last two tiers are the most powerful cyber criminals, capable of creating some weaknesses themselves in the network in order to attack with a greater level of sophistication and often using HUMINT[18]. Such hackers have the power to perform all kind of attacks and have the power to considerably modify some key standards of a cryptocurrency. However, such cyber criminals are usually acting low-profile since they might be easily identified considering the high level of sophistication they are able to deliver. Not all hackers are capable of performing such disruptive attacks, which hence makes them identifiable by specialized agencies.

In a general perspective, cyber risks represented in the form of such attacks is nearly impossible to counteract. The cyber risk is a reality of the cryptocurrency world which heavily threatens the fundamental principle of security. If a system can't be considered enough secured, it will hardly be trusted by users and hence be very poorly used as a medium of payment. However,

[18] Abbreviation for Human Intelligence. HUMINT is the gathering of political or military intelligence through secret agents. (Dictionary.com, n.d.)

even though cyber risks are well present in the crypto world, it doesn't necessarily mean that such attacks will happen often. Hackers will have to evaluate if all the required investments are worth the reward they'll be getting from hacking a blockchain network. It is then worth asking if the development of cryptocurrencies will necessarily have an impact on the number of cyber-attacks performed in this payment system. Considering that such risks are already well present in the current system, why would this risk increase in a world where cryptocurrencies act as an alternative to settle transactions? Overall, it would cost more to hackers to perform attacks on a cryptocurrency infrastructure than on the current one. In order to be relevant and effective enough, hackers willing to threaten a crypto blockchain would need to invest in really expensive and specialized machines with an extremely high computational power. The cost-benefit ratio of such operations might then not be high enough to run cyber-attacks on a network. The only reason why cyber criminals would ignore the cost-benefit ratio would be in the case of an attack with the objective to take a participant out of the market, whatever the reasons.

Even though cyber risks still represent an important part of the technical limits that cryptocurrencies have to face, they might not represent the biggest issue in case of an increased adoption of cryptocurrencies as a medium of payment.

CONCLUSION

Cryptocurrencies have the power to disrupt the whole payment system with their technology allowing peer-to-peer transactions. They promised to act as an alternative to the current payment system by providing near-instant payments at no costs and with a high level of security and reliability. Their development is being monitored by players all around the world and early adopters are stepping in to start testing the new payment method. Famous companies and NGO's are getting involved in order to be the first to accept cryptocurrencies payments. Even governments and financial institutions are taking the step into the crypto world, whether by testing new payments infrastructures or by creating their own cryptocurrencies such as the JPM coin created by JP Morgan.

This early development shows how worldwide market players and financial institutions see cryptocurrencies as an innovation with the power to change the current paradigm of payments into a more efficient and convenient one. The development of this new technology is anchored in a changing environment characterized by strong driving forces. Banks' operating models are moving towards more mobile-centric solutions, incarnating changes in customers' needs and expectations. Millennials and Generation Z individuals are putting their trust into new technologies, while constantly looking for better customer experiences. This new environment is characterized by the entrance of new players on the markets such as fintech companies or GAFA, willing to have their piece of the cake. Companies like Facebook have the ability to become really powerful players in the financial industry by providing their own cryptocurrencies to billions of users and allowing them to perform easy and costless payments all around the world.

All along this thesis, we were able to understand to what extent cryptocurrencies represent an innovation in the way we transact. They are an ingenious combination of technical innovations and monetary innovations. They leverage on distributed ledgers technology to provide a highly secured and reliable storage of financial information. On top of that, they represent an improvement in the operating model of payments and a total upset in the nature of money by switching to fully virtual currencies. What makes it even more innovative is its total disconnection with the current payment system. Cryptocurrencies go against all standards of trust that we created overtime by being totally independent from financial institutions.

The innovative patterns of cryptocurrencies make no doubts. On the other side, the disruptive pattern of this technology will stand in the manner it affects our ways of transacting with this new type of money. All the underlying implications of cryptocurrencies are interconnected with a series of challenges and limits having a direct impact on their development.

Overall, cryptocurrencies have the power to improve the global economic efficiency through the improvement of our payment processes. Their technology allows to benefit from more efficient processes either globally or locally. Improving the economic efficiency of multiple specific sectors through the development of payment infrastructures will have a great impact on the overall efficiency. The improvement of the financial inclusion all around the world will also considerably improve the economic efficiency. Providing an easier access to the economic activities with the use of cryptocurrencies will allow to involve much more people in the economy and thus have a considerable impact on the economic growth.

However, this improvement in efficiency might be limited by some key challenges faced by cryptocurrencies. Their anonymity feature still remains a controversial point, acting as an enabler of illicit activities. Anonymity questions the trust people can have in such currencies and make them less credible for day-to-day transactions. On top of that, we saw that most cryptocurrencies were hardly scalable in case their development became broader. They are currently facing strong technical limits due to the very high level of electricity consumption and the potential infrastructure overload. These limits are representing an important barrier to adoption and make their development as an alternative payment method less credible.

The low level of adoption is reinforced by the high price volatility of the cryptocurrency market. The low traded volumes of cryptocurrencies make them even more sensitive to speculation, leading to extreme changes in value overtime. These two factors would then have a negative impact on the financial stability if cryptocurrencies were developed in the current state. In addition, the risks of cyber-attack and the lack of regulations regarding cryptocurrencies could weaken even more the overall financial stability.

What is for sure is that lot of questions still need to be answered in order to see a real development of cryptocurrencies as an alternative mean of payment. Financial institutions and regulatory entities will have to step in to provide a framework for the crypto ecosystem to work efficiently and peacefully. The analysis performed during this thesis shows how essential it would be to have a global regulatory framework set by policymakers all around the world. Banks and central banks will also have to better understand this new technology and decide on which role they want to play in this new environment. If regulations are not set to clarify the current situation, this might lead to the creation of two hermetic financial ecosystems, which would have considerable impacts on our economy.

Even though cryptocurrencies are facing a lot of drawbacks and unanswered questions, cryptos specialists usually come up quite quickly with new solutions. Some typologies of cryptocurrencies might be best suited for a global acceptance, such as payment infrastructures tokens or general platform tokens. On top of that, the development of stable coins might be really interesting to follow as they represent a great way to bypass the current volatility and act as a reliable option for day-to-day uses. Facebook's cryptocurrency Libra is the best example of such innovations, with the potential to disrupt the payment system by providing a more convenient, costless and global payment method to its users.

Technology is able to adapt easily to the current challenges faced by cryptocurrencies. What will now be interesting to monitor will be the way policymakers and financial institutions position themselves in this changing environment. Cryptocurrencies are now a reality and the next question to be asked is: Who will be the firsts to adapt to this new technology and how will it affect our ways of using money? Will the economy adapt to cryptocurrencies or will cryptocurrencies adapt to the economy? The reaction of authorities all around the world will for sure have a huge impact on their development and on the global economy. We will probably have to wait a few decades to see how our future payment system will look like. The future will tell us.

REFERENCES

Accenture. (2017). *Driving the Future of Payments. 10 Mega Trends.* Retrieved from Accenture website: https://www.accenture.com/us-en/insight-banking-future-payments-ten-trends

Apple. (n.a.). *Apple card*. Retrived from: https://www.apple.com/apple-card/

Athanassiou, P. (2017). Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks. *ECB Legal Working Papers, 16*, 5-11. Retrived from: https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e

Baron, J., O'Mahony, A., Manheim, D., & Dion-Schwartz, C. (2015). *National Security Implications of Virtual Currencies.* Santa Monica, CA: Rand Corporation. doi:10.7249/RR1231

Beach, N., & Hagiu, A. (2014). *Bitcoin: The Future of Digital Payments?* Harvard Business School. Retrieved from The Case Center website: https://www.thecasecentre.org/main/products/view?id=124014

Berman, A. (2019). *Argentina settles export deal with Paraguay using Bitcoin*. Retrieved from CoinTelegraph website: https://cointelegraph.com/news/argentina-settles-export-deal-with-paraguay-using-bitcoin

Bank for International Settlements. (2018). BIS a*nnual economic report 2018*. Retrieved from: https://www.bis.org/publ/arpdf/ar2018e.pdf

Bitcoin Real Estate. (n.a.). *Home page*. Retrieved June 21, 2019, from: https://bitcoin-realestate.com

Blockchain. (2019). *Bitcoins in circulation*. Retrieved June 18, 2019, from: https://www.blockchain.com/charts/total-bitcoins?timespan=all,

Blockchain. (2019). *Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes)*. Retrieved July 3, 2019, from Statista website: https://0-www-statista-com.lib.unibocconi.it/statistics/647523/worldwide-bitcoin-blockchain-size/

Browne, R. (2017). *American Express, Santander team up with Ripple for cross-border payments via blockchain*. Retrieved June 24, 2019, from the CNBC website: https://www.cnbc.com/2017/11/16/american-express-santander-team-up-with-ripple-on-blockchain-platform.html

Buchholz, K. (2019). *How Common is Crypto?* Retrieved June 21, 2019, from Statista website: https://0-www-statista-com.lib.unibocconi.it/chart/18345/crypto-currency-adoption/

Cartsens, A. (2019). *The future of money and payments*. Speech from the 2019 Whitaker Lecture. Central Bank of Ireland, Dublin. Retrieved from Bank for International Settlements website: https://www.bis.org/speeches/sp190322.htm

Claerhout, P. (2019). Le secteur bancaire à la veille d'importants changements. *Trends tendance, 44(26-27)*, 64-67.

Coeuré, B. (2018). *The future of central bank money*. Retrieved from the European Central Bank website: https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514_4.en.html

Coindesk. (2019). *Bitcoin Price Index*. Retrieved June 18, 2019, from: https://www.coindesk.com/price/bitcoin

Cuthbertson, A. (2019). *North Korea using cryptocurrency to fund nuclear weapons development, report warns*. Retrieved from the Independent website: https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-bitcoin-cryptocurrency-nuclear-weapons-sanctions-rusi-a8872056.html

Dash. (n.d.). *Home page*. Retrieved June 11, 2019, from: https://www.dash.org

Defense Science Board. (2013). *Resilient Military Systems and Advanced Cyber Threat.* Task Force Report, Department of Defense of the United States of America, Washington. Retrieved from: https://apps.dtic.mil/docs/citations/ADA569975

Deloitte. (2018). *2018 Banking Outlook.* Retrieved from: https://www2.deloitte.com/be/en/pages/financial-services/articles/gx-banking-industry-outlook.html

Deloitte. (2018). Blockchain to blockchains. In *Tech Trends 2018 - The symphonic entreprise* (pp. 95-97).

Deloitte. (2019). Macro technology forces at work. In *Tech Trends 2019 - Beyond the digital frontier* (p. 8).

Dictionary.com. (n.d.). *humint*. Retrieved June 29, 2019, from: https://www.dictionary.com/browse/humint

Digiconomist. (2019). *Bitcoin Energy Consumption Index*. Retrieved June 17, 2019, from: https://digiconomist.net/bitcoin-energy-consumption

Elliott, P. J., de lima, L. & Singel, R. (2018). *Cryptocurrencies and Public Policy. Key Questions and Answers.* United States: Oliver Wyman. Retrieved from: https://www.oliverwyman.com/our-expertise/insights/2018/feb/cryptocurrencies-and-public-policy.html

EthHub. (n.d.). *Monetary Policy*. Retrieved June 19, 2019, from: https://docs.ethhub.io/ethereum-basics/monetary-policy/

Futura Tech. (n.d.). *Zero day*. Retrieved from: https://www.futura-sciences.com/tech/definitions/informatique-zero-day-4029/

Gailly, P. (2015). *Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux.* Paris, France: Les éditions des Journaux officiels.

Gartner. (2018). *Predicts 2019: Blockchain technologies.* Retrieved from: https://www.gartner.com/document/3894681?ref=solrAll&refval=227935062&qid=528abc5c4878eb3b96bff1

Girasa, R. (2018). *Regulation of Cryptocurrencies and Blockchain Technologies.* Pleasantville, NY: Palgrave Macmillan. doi:10.1007/978-3-319-78509-7

Golem. (2019). *About Golem*. Retrieved from: https://golem.network/home/

Halaburda, H., & Sarvary, M. (2016). *Beyond Bitcoin. The economics of digital currencies.* Hampshire, UK: Palgrave Macmillan. doi:10.1057/9781137506429

IDC. (2018). *Distribution of Blockchain market value worldwide in 2018, by sector.* Retrieved June 10, 2019, from Statista website: https://0-www-statista-com.lib.unibocconi.it/statistics/804775/worldwide-market-share-of-blockchain-by-sector/

IDC. (2019). *Worldwide spending on blockchain solutions from 2017 to 2019 and in 2022 (in billion U.S. dollars)*. Retrieved from Statista website: https://0-www-statista-com.lib.unibocconi.it/statistics/800426/worldwide-blockchain-solutions-spending/

ING. (2016). *I would feel confident that my money is secure if I used contactless payments**. Retrieved June 11, 2019, from Statista website: https://www.statista.com/statistics/611425/confidence-about-contactless-payment-security-in-the-benelux-by-country/

J.P. Morgan. (2019). *J.P. Morgan Creates Digital Coin for Payments*. Retrieved from: https://www.jpmorgan.com/global/news/digital-coin-payments

Janus, E. (2019). *Argentina: Bitcoin now accepted for public transport in 37 cities*. Retrieved from Bitcoinist website: https://bitcoinist.com/argentina-transport-sube-bitcoin/

Kharif, O. (2019). *Facebook's Libra Crypto Coin: 5 things we know, 5 We Don't*. Retrieved from Bloomberg website: https://www.bloomberg.com/news/articles/2019-06-22/facebook-s-libra-crypto-coin-5-things-we-know-and-5-we-don-t

Kiel Institute for the World Economy. (2018). *Virtual Currencies: Monetary Dialogue July 2018.* Brussels: Policy Department for Economic, Scientific and Quality of Life Policies. Retrieved from: http://www.europarl.europa.eu/committees/en/econ/monetary-dialogue.html?tab=2018

Landau, J.-P. (2018). *Les crypto-monnaies. Rapport au Ministre de l'Economie et des Finances.* Paris: Ministère de l'économie et des finances. Retrieved from: https://www.ladocumentationfrancaise.fr/rapports-publics/184000433/index.shtml

Libra Association Members. (n.a.). *Libra White Paper.* Retrieved June 24, 2019, from Libra website: https://libra.org/en-US/white-paper/

Maecenas. (2019). *How it works*. Retrieved from: https://www.maecenas.co/how-it-works/

Mitchell, S. (2018, October 4). *Bithumb Cryptocurrency Exchange To Launch A Decentralized Exchange.* Retrieved from Best GPU For Mining website: http://bestgpuformining.com/bithumb-cryptocurrency-exchange-launch-decentralized-exchange/

Monero. (2019). *Home page*. Retrieved from: https://www.getmonero.org

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from Bitcoin website: https://bitcoin.org/en/bitcoin-paper

PayPal. (2019). *PayPal's annual payment volume from 2012 to 2018 (in billion U.S. dollars)*. Retrieved June 11, 2019, from Statista website: https://0-www-statista-com.lib.unibocconi.it/statistics/419783/paypals-annual-payment-volume/

Pollock, D. (2019). *Cryptocurrency Volatility: Enemy Or Friend? How Can Digital Assets Be Price-Secure*. Retrieved from Forbes website: https://www.forbes.com/sites/darrynpollock/2019/04/16/cryptocurrency-volatility-enemy-or-friend-how-can-digital-assets-be-price-secure/#70d93466183f

PostNord. (2018). *Which of the following methods do you prefer to use when you pay for a product you have bought online?* Retrieved June 11, 2019, from Statista website: https://www.statista.com/statistics/672168/ranking-of-preferred-payments-methods-in-belgium/

Prisco, G. (2019). *2019: The year of the Security Token Offering (STO)?* Retrieved from Medium website: https://medium.com/chainrift-research/2019-the-year-of-the-security-token-offering-sto-bb52a09d0701

Quoistiaux, G. (2019). Facebook réinvente le bitcoin. *Trends tendances, 44 (26-27)*, 24-29.

Ripple. (2017,). *Ripple Escrows 55 billion XRP for supply predictability*. Retrieved from: https://ripple.com/insights/ripple-escrows-55-billion-xrp-for-supply-predictability/

Rosic, A. (2017). *Proof of Work vs. Proof of Stake: Basic Mining Guide*. Retrieved from Blockgeeks website: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Sia Partners. (2019). *La valeur intrinsèque du Bitcoin : du constat à la théorie*. Retrieved from Finance & Strategy website: http://finance.sia-partners.com/20190226/la-valeur-intrinseque-du-bitcoin-du-constat-la-theorie

Statista. (2019). *FinTech Report 2019.* Retrieved June 21, 2019, from: https://0-www-statista-com.lib.unibocconi.it/study/44525/fintech-report/

Takeaway. (2019). *Customer service - Payments*. Retrieved June 19, 2019, from: https://www.takeaway.com/be-fr/service-clientele-consommateur-sujet-paiement

Timicoin. (2018). *Home page*. Retrieved from: https://www.timicoin.io

Weisenthal, J. (2019). *Facebook's Libra Crypto Coin: 5 Things We Know, and 5 We Don't*. Retrieved from Bloomberg website: https://www.bloomberg.com/news/articles/2019-06-22/facebook-s-libra-crypto-coin-5-things-we-know-and-5-we-don-t

World Bank Group. (n.a.). *Financial stability*. Retrieved June 26, 2019, from World Bank website: https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/financial-stability

World Bank. (n.d.). *Share of population* with an account at a financial institution in Asia-Pacific in 2017, by country.* Retrieved June 24, 2019, from Statista website: https://0-www-statista-com.lib.unibocconi.it/statistics/632834/asia-pacific-population-with-an-account-at-a-financial-institution-by-country/.

Young, J. (2019). *A major philippine bank just launched crypto ATMs and it may fuel massive Bitcoin adoption*. Retrieved from CCN website: https://www.ccn.com/a-major-philippine-bank-just-launched-crypto-atms-and-it-may-fuel-massive-bitcoin-adoption/

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/lsm**