Ca' Foscari
University
of Venice

Master's Degree
in Finance

Final Thesis

The Payment Services Directive 2 in the era of cryptocurrencies: analysis of their relation in the payments landscape

Supervisor
Ch. Prof. Andrea Minto

Graduand
Miriam Munaro
Matriculation Number 862437

Academic Year
2020 / 2021

CONTENTS

Introduction 1

CHAPTER I: Payments digitalization and oversight in the European Union 5

1.1 The rise of FinTech 5

1.2 The payments landscape in the EU 7

1.2.1 Electronic money payments.. 11

1.2.2 Platforms and third party providers 13

1.3 Overview of the payment systems 16

1.3.1 The regulatory framework for payment services 20

CHAPTER II: The advent of the Payment Services Directive 2 (PSD2).......................... 23

2.1. Access to accounts and Third-party payment service providers 25

2.2 The Open Banking.. 30

2.2.1 Transparency in the PSD2 32

2.3. The payment process... 33

2.4 The payment user authorization and the SCA 36

***2*.5 Bodies of law in accordance with PSD2** 41

2.5.1 The General Data Protection Regulation... 41

2.5.2 The Anti-money Laundering Directive 46

CHAPTER III: Cryptocurrencies and the role of PSD2 in their legal framework........... 53

3.1 An overview on cryptocurrencies 53

3.1.1 The idea of blockchain as a trustless mechanism and "The Code" 56

3.2 Cryptocurrencies as a means of payment... 61

3.2.1 Crypto payment gateways.. 65

3.3 Crypto payment gateways classification under the EU legal regime 67

3.3.1 "SpicePay" payment gateway 69

3.4 The application of the Payment Services Directive 2 to cryptocurrencies........ 73

3.4.1 Stablecoins.. 76

CHAPTER IV: Regulatory evidence for cryptocurrencies in the EU 79

4.1 The digital financial package 79

4.1.1 The "Retail Payment Strategy" and the review of the PSD2 79

4.1.2 The MiCAR Proposal 81

4.2 The regulatory framework in some countries 84

4.2.1 Italy 84

4.2.2 Malta 86

4.2.3 Switzerland 88

4.2.4 Estonia 89

Conclusion 91

Bibliography 101

Sitography 114

Introduction

The financial world is rapidly transforming thanks to the innovations brought by technology. In particular, it is possible to addressed FinTech, which has gained major interest from individuals. It is digitalizing the way of performing transactions, and has introduced new entities, as the cryptocurrencies. Within this landscape, the European Union intends to provide legal certainty and safeguard to customers. This dissertation analyses the evolution in the payments landscape, where the execution of exchanges in non-cash forms is becoming increasingly widespread, especially for what concerns electronic money. Within this context, is provided a throughout analysis of the Payment Services Directive 2, the fundamental piece of law that has established and regulated new ways of performing payments. However, technology has introduced also virtual currencies in such environment, entities highly discussed for their risks and also for the huge interest towards them from individuals. Apparently, between the PSD2 and cryptocurrencies there is not a relation, but the existence of crypto payment gateways could change such view. These entities are now beginning to be increasingly widespread, and their functioning will be deepened.

Chapter 1 introduces the phenomenon of FinTech, describing three different waves of its existence. Subsequently, it is provided an overview on the current situation for payments, highlighting their digitalization and the introduction of third parties which perform online transactions. This paper focuses mainly on retail payments, which define high volume transactions of quite low value. They mainly represent non-SIPs which are executed in the SEPA area and are under the Eurosystem's oversight. Currently, people prefer tailor-made and fast services, thus they do not resort to the use of cash, rather they utilize electronic-money or cards. Under these circumstances, the EU has introduced rules in order to provide safety and harmonize the payments landscape.

Chapter 2 illustrates the advent of the Payment Services Directive 2, describing its innovative legislative framework. It has defined the Open Banking, which allows entities outside financial institutions, i.e. Fintechs, to have access to people's data that are kept by banks, thanks to the Application Programming Interface (API). In particular, it has introduced the Third Party Payment Service Providers, namely the Payment Initiation Service Provider (PISP) and the Account Information Service Provider (AISP) which, respectively, arrange the payment transaction between the payer and the payee, and provide the general financial situation of the user. Such innovations have to abide to specific requirements in order to carry out their activities, not only those defined by the PSD2, but also those of the AMLD and the GDPR, which are essential for the contrast of illicit behaviours and for the protection of data.

When payment transactions are performed, it is mandatory the application of the Strong Customer Authentication, which requires the authentication of the user, based on two or more factors. Moreover, when a merchant intends to sell online his/her goods or services, it is possible to identify the four-party model, where payment gateways fulfil a fundamental role, as they securely transmit the information and decide whether to accept the exchange. As will be illustrated, in such operations are involved multiple entities.

Chapter 3 continues the analysis of the evolution within the payments field. Thus, it introduces the phenomenon of cryptocurrencies, describing their characteristics. In particular, this dissemination focuses on decentralized virtual currencies, as the well-renowned Bitcoin. They function through the blockchain, a technology based on nodes' validation, which does not need trust. However, such paradigm will be contested, as the statement 'In code we trust' has not solid foundations. Cryptocurrencies are mainly used for investment purposes, nonetheless, their use as a means of payment is increasing, however, they do not represent a legal tender. In this chapter will be tackled the main question of this paper: is there a relation between the PSD2 and cryptocurrencies? The answer is to be found in the evaluation of crypto payment gateways, entities arranging payment transactions using virtual currencies, thus, acting as 'payment institutions'. For such purpose, will be considered Spicepay, whose website provides detailed information.

Chapter 4 addresses the new regulatory initiatives of the EU in the field of technology, hence, will be considered the ‘Digital Financial Package’, a decisive step towards harmonization in the context of FinTech and innovation. It intends to define a revision of the PSD2 and, for the first time, provide a taxonomy of crypto assets in the MiCAR proposal. Moreover, some countries of the EU will be examined, to understand how the PSD2 has been transposed and what are the rules for what concerns crypto assets.

CHAPTER I: Payments digitalization and oversight in the European Union

1.1 The rise of FinTech

Technological innovation has been changing the financial sector for decades, and it is possible to outline this progress as *FinTech*; the term itself is the simple combination of the words 'finance' and 'technology', and its first appearance can be dated back to the early 1990s. It was used for a project pertaining to "Citicorp" (today Citigroup[1]), titled "Financial Services Technology Consortium" which aimed to facilitate the bank cooperation with technology[2]. However, the first real definition was provided by the Financial Stability Board, which addressed FinTech as:

> "*Technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services[3]".*

This interpretation was presented in 2017, nevertheless FinTech is not a new phenomenon, and it is possible to define three distinct waves in history. *FinTech 1.0* (1838 – 1957) is identified with the invention of the telegraph and the creation of the transatlantic cable, which represent the starting point of the financial globalization. The first ATM (Automated Teller Machine) installation, by Barclays in the UK, commenced *Fintech 2.0* (1967 – 2008). It was the first time a digital transformation of cash was performed and rose the possibility of owning payment cards. In 1973 was founded SWIFT (Society for Worldwide Interbank Financial Telecommunications) which established a code system that still represents a landmark for financial institutions, as it assigns a numerical code to banks in order to identify the characteristics of the

[1] An American multinational investment bank and financial services corporation in NY.

[2] Marc Hochstein: "*Fintech (the Word, That Is) Evolves*", AMERICAN BANKER (Oct. 5, 2015), available at: *http://www.americanbanker.com/bankthink/fintech-the-word-that-is-evolves-1077098-1.html.*

[3] Available at: *http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-fintech/.*

transactions performed. Furthermore, in the 1970s was created VISA and its first debit card and, in the same period, the original electronic securities market Nasdaq was established. During this era, financial institutions started using the IT (Information Technology) in their operations, and with the spread of the World Wild Web, transactions began to be regularly performed online.

Nevertheless, it is only in the last five years that FinTech has gained global attention[4], and what we know today can be defined as *Fintech 3.0* (2008 – current). It was initiated by the 2008 global financial crisis, a "once-in-a century credit tsunami"[5] that dramatically changed the financial landscape. Since this moment, people began to be interested in Fintech, as it provides faster e tailored services. It operates in three main areas[6]: transactions executions, funds management and insurance, but it can be referred to a broader range of innovations, made possible by the new technologies.

One of the crisis' direct consequences has been the loss of confidence in the strength of key financial institutions and markets[7], and what has emerged as a consequence is *data economy*, a reality composed by actors with no financial qualification, where the crucial matter is, indeed, data. Therefore, the financial world is not dominated solely by traditional incumbents, but there are many new players such as tech start-ups, disruptors and a wide use of blockchain and cryptocurrencies, which will be examined in the following chapters.

Under these circumstances, banks have lost their influence and their monopoly. As art. 4 (1) of Regulation (EU) 575/2013 states, a bank is *"an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account".* Thus, one of its primary objectives is to provide liquidity to

[4] See *https://trends.google.it/trends/explore?date=all&q=fintech.*

[5] Testimony of Alan Greenspan: "*The financial crisis and the role of federal regulators: Hearing before the House Committee on Oversight and Government Reform"*, 110th Cong. 2008.

[6]Giorgio Barba Navaretti, Giacomo Calzolari, Alberto Franco Pozzolo: "*FinTech and Banks: Friends or Foes?"*, page 12.

[7] Bernanke BS.: "*Stabilizing the financial markets and the economy",* Speech Presentation at the Economic Club of New York. New York, 2008, October 15.

customers, as it gives access to notes and coins. The collection of funds still is a prerogative of banks, as in order to do that, the banking license is required. Therefore, they still perform their tasks, but the technological innovation has forced the adaptation to the new digital world, changing the way of performing clients' requests.

FinTech has triggered the financial digitalization already during its second wave, but it is only since the global financial crisis that there are non-traditional players who exploit customers data, instead of protecting them. Big data companies have blurred the line between what is personal information and what is not, and what before represented a liability for banks, has now become an asset. This has generated competition among financial institutions, which have responded in different ways[8]: with a 'closed' approach, by defining agreements with the new players about specific technologies and restricting access to their data, others have provided access to information under certain regulations, and some banks have denied the access permission because of safety concerns. Nevertheless, they are moving towards a cooperation, as FinTech is becoming an integrated part of the financial world and digitalization is essential for customers.

1.2 The payments landscape in the EU

A payment transaction can be described as "*a transfer of funds which discharges an obligation on the part of a payer vis-à-vis a payee*[9]", thus it is possible to identify a payer, who decides to initiate the operation, and a payee, who receives the funds. The payment system involves three main elements: the chosen payment instrument (including the approval and the submission of the transfer), the processing of the payment (also, clearing), and eventually the settlement. According to the kind of actors engaged in the transaction, it is possible to list two main types of payment: large-value (or wholesale) and retail. With respect to the former, both parts involved are financial institutions and denote large-value operations. In the latter form, instead, at least one

[8] Governor Lael Brainard: "*Where Do Banks Fit in the Fintech Stack?",* April 28, 2017. At the North-western Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice.
Available at: https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm.

[9] ECB: "*The payment system"*, 2010.

of the participants is a non-financial institution (it might be a consumer, a business or a government), there are high numbers of these low-value transactions daily, and this form is the one mainly considered in this paper.

In retail payments cash represents the most widespread way to discharge obligations. In particular, across the European Union the official currency is the euro, introduced on 1 January 1999, with banknotes and coins launched on 1 January 2002. According to article 128 (1) TFEU, the euro represents a legal tender henceforth its acceptance is mandatory. Money have three important features: they are a 'medium of exchange' because they are accepted as means of payment, they represent a 'unit of account' since they can be expressed in a common unit, and they are also 'store of value' because money entails an intrinsic value; all these features provide trust in their practise.

Nevertheless, the new technology mentioned in *paragraph 1.1,* has prompted the evolution of payments, making them possible also in cashless forms. This digital transformation can be dated back to the 1870s, when the first electronic fund transfer (ETF) was created by Wester Union. The idea was to allow a long-distance exchange of funds between people, among the cities of New York, Chicago and Boston. It was later defined as "*a funds transfer initiated through an electronic terminal, telephone, computer (including on-line banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account*[10]*".* This description represents the fundamentals of cashless payments, which, according to the ECB[11], involve the authorization of the payer to his/her bank, to perform a transfer of funds to the payee's bank.

Moreover, the world wide web appearance has accelerated these transactions introducing several ways to perform them, and banks are not the only player, as stated earlier, since the advent of *Fintech 3.0,* and at the present time also tech giants such as Facebook, Google play a key role in the financial world. As a consequence, the use of

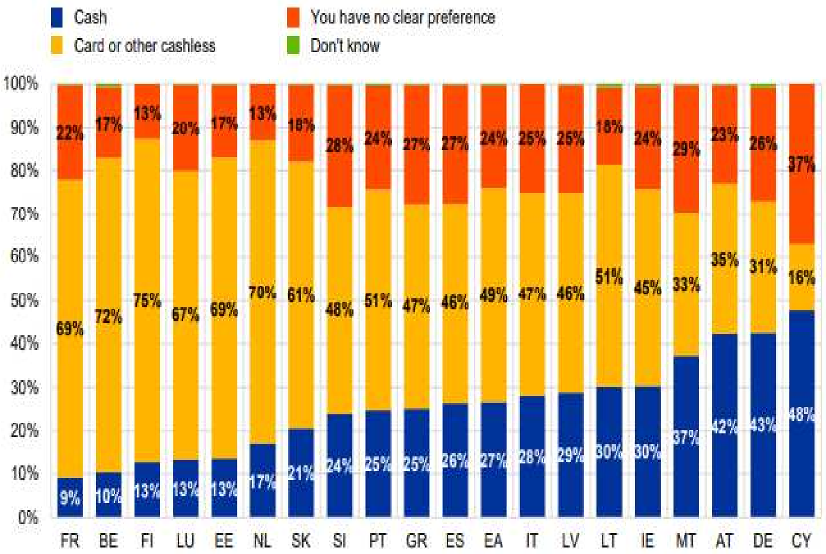
[10] *Electronic Transfer act*, Federal Reserve board, (15 USC 1693 et seq.)

[11] Tom Kokkola: "*The payment system*", ECB 2010, EDITOR

cash has diminished throughout the years, all over the world. Nowadays, it is shrinking also for safety purposes: the ECB has stopped the production of the 500 Euros banknote for traceability reasons, and Covid-19 has fostered electronic payments because of health concerns.

It is important to remind that the widest used mean of payment still is cash (banknotes and coins), especially for low amount expenses. However, as can be noticed in *Chart 1*, people in the Euro zone have declared a significant preference for non-cash payment in 2019, as expressed in 'SPACE[12]' the study conducted by the ECB. The coronavirus pandemic has accelerated this trend, and the main reason provided for such choice was not because people were afraid of the virus on banknotes (38%), but mostly because digital payments result more convenient (45%). The predilection for these instruments is given by people's need for fast and easy transactions, and they require personalized experiences.

Chart 1: Preferred payment instrument by country

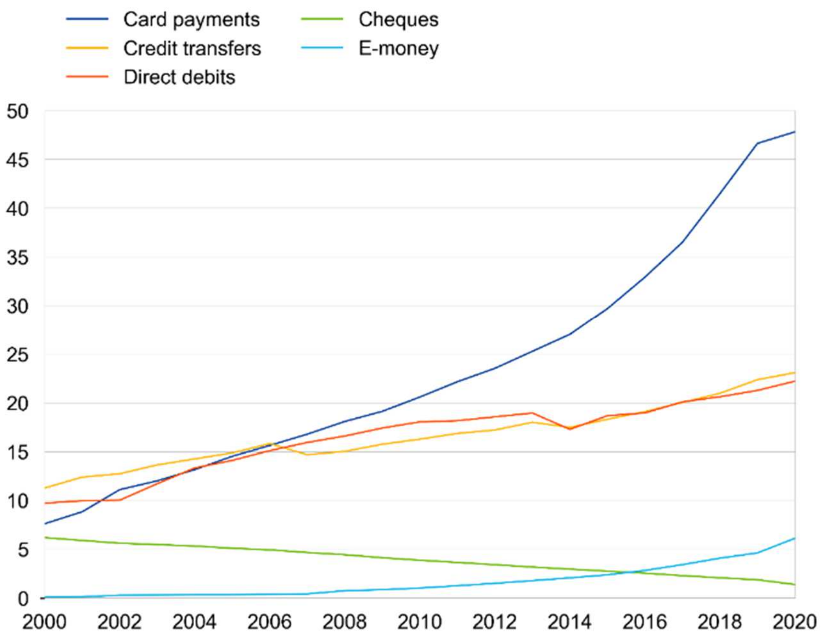


Source: ECB (2019), De Nederlandsche Bank and the Dutch Payments Association (2019) and Deutsche Bundesbank (2019).

[12] *"Study on the payment attitudes of consumers in the euro area",* it has considered the retail payment system.

ECB's *Chart 2*[13] shows that, during the year 2020, there was an increase in non-cash payments in the euro area of 3.7%, which reached a value of 101.6 billion. Precisely, the 47% of all transactions were performed using card payments, the 23% via credit transfer and the remaining 22% through direct debits.

Chart 2: Use of the main payment services in the euro area



Source: ECB (2020)

As listed in the previous charts, it is possible to describe several types of non-cash payment instruments. The least used one is *cheques*, a paper-based form that involves a written request of funds transfer, from the payer bank account to the payee one. It defines the most expensive way and entails the issue of the drawer's creditworthiness; indeed, its usage shows a downward trend. People are inclined to

[13] ECB: "*Payment statistics: 2020*", 23/07/2021.

prefer electronic payments where transactions are arranged through a so-called payment service provider, namely a third party arranging the exchange. The reasons for such choice are given by the speediness of the operation and the possibility to pay whenever the person wants to, which is a fundamental feature as online purchases have become a daily activity.

Card payments represent the widest used method. They are in a plastic form and issued by an authorized intermediary; they can be used to withdraw money from the ATM, to pay at POS terminals (Point at sale) or to conclude a purchase on the internet. In order to perform the transaction a PIN in required. There are three kinds: credit cards, which are linked to a bank account, and enable the user to delay the effective charge (usually it is charged monthly); debit cards, which are also related to a bank account, and whose purchase operations are effective immediately or within few days, but they present a limit on the amount that can be used daily and monthly; prepaid cards, which work similarly to debit ones, but the holder does not need to have a bank account, hence they have their own IBAN and they can be reloaded.

Credit transfers are payment orders performed by the payer to his/her bank account, to arrange a transfer of funds to another person. *Direct debits*, instead, represent an authorization from the payer to her/his debtor, to independently collect an amount of money from the bank account (usually this happens for regular payments). Eventually, exists another way to perform transactions, namely e-*money* payments which represent the most innovative method, enabled by the last technology advancements, and require a detailed description.

1.2.1 Electronic money payments

This particular method is revolutionizing the payments landscape, also thanks to the so-defined “disruptors” which entered into the financial world, alongside banks. There are several manners to perform electronic money payments. *E-wallets,* as the name declares, are digital wallets which can store various type of information, such as the identity card, the driver license, but they are predominantly used as substitute for the physical debit or credit card. Hence, they are utilized to perform payment transactions; in order to function, the individual simply has to create an account and insert a password of his/her choice. Purchases can be made online or at the store, thus we are referring to internet-based and device-based wallets. The first type is the most widespread, used for e-commerce acquisitions, and a typical example is PayPal which allows online payments, since 1998. The latter one typically involves the NFC (Near Field Communication) technology, and the transaction takes place in a contactless manner, by approaching the device to the payment reader, like Apple pay, WeChat pay. The use of this payment method grew globally by 7% in 2020[14].

It is more accurate to define the last method as *mobile wallet*. Nowadays, in the European Union almost every individual possesses a mobile phone, and during the year 2019, the 22% of purchases made in stores were settled using smartphones[15]. This trend is weakening the existence of payment cards in the physical form, encouraging the contactless way to pay, but also to withdraw cash from ATMs. As stated before, the technology used is the NFC which transfers the information from the phone to the terminal; exists also the QR code, which simply needs to be scanned in order to perform the payment. Moreover, these technologies can be used through smart objects, facilitated by the IoT (Internet of Things), which make the payment even more invisible and immediate. Based on the instrument employed, it is possible to talk about smart speaker payment, smart car payment and smart appliance payment. Also, it is possible to use wearables, such as smartwatches.

Another novelty is represented by the *"Peer-to-Peer"* (P2P) lending. The term itself came up from the internet environment during the 2000s, addressing the approach used to share files directly to another person, without the need of an intermediary server. Currently, it can be identified in the financial world too, and its origin can be dated back to the creation of the firms "Zopa" in 2005, in the UK, and "Prosper" in 2006, based in the USA[16]. They presented to their clients the possibility to overcome banks

[14] PWC: "*Payments 2025 & beyond Navigating the payments matrix Charting a course amid evolution and revolution*".

[15] *Worldpay from FIS 2020 Global Payments Report.*

[16] Milne and Paul Parboteeah: "*The Business Models and Economics of Peer-to-Peer Lending* Alistair", May 2016.

and lend directly to each other using a marketplace. This represents the beginning of P2P platforms' growth, which today are creating a lot of competition between giant tech firms. The "peers" can virtually exchange funds through the network, thus it is possible to identify a payer and a payee. It is easy, instant, fast and it is possible to use the mobile phone to perform the exchanges, the user only has to create an account and choose a PIN. This operation can be feasible by using a digital wallet connected to the person's bank account or card payment, as it works for PayPal and Satispay. However, there are also other platforms which do not require the recipient of the transfer to possess a bank account, and others employing the so-called cryptocurrencies (as Bitcoin).

1.2.2 Platforms and third party providers

The incessant technological innovation has introduced new players in the payment transactions, namely the "third-parties", entities that arrange the transfer of information and funds. Nowadays, in the financial world are used digital platforms which, according to the EBA[17], can be addressed as "a technical infrastructure that enables at least one financial institution directly (or indirectly using a regulated or unregulated intermediary) to market to customers, and/or conclude with customers' contracts for financial products and services[18]". Their utilization is increasing, and the 97% of the credit institutions that took part on the EBA questionnaire[19], asserted that uses platform-based means, and a great part of them holds it for payment service purposes. The platforms identified by the EBA are five, labelled according to the participants involved, the services provided and the intent of their use. "*Comparators*" provide access to the financial institution's website, in order to allow the customer to compare the products offered from several financial institutions; "*Financial institutions +*" allow third parties to distribute services to the customers, also intermediating the

[17] EBA: "Report on the use of digital platforms in the EU banking and payments sector", September 2021, EBA/REP/2021/26.

[18] Are excluded in this definition: mobile banking apps or online banking tools used by a financial institution to offer regulated financial services in a fully digitalised way displacing the need for customers to enter a physical branch or use a telephone service and without changing the nature of how financial institutions operate and deliver value (i.e. pure financial institution operated digital distribution channels); platforms used only by (and for) 'crowdfunding service providers' within the scope of Regulation (EU) 2020/1503; platforms used only by (and for) P2P lending.

[19] EBA's Spring 2021 RAQ.

exchange of funds; "*Platforms with banking/payments as a side service*" which are wrought by a business that is not a financial institution, offer to clients the access to "banking and payment services offered by third-party financial institutions and non-financial services or products offered by other third-party firms[20]"; "*Ecosystems*" define marketplaces where firms and financial institutions can deliver their services/goods. The last category of platforms is "*Enablers*", governed by a technological company which offers an interface between the customer, the bank and a third party. In this case, it facilitates the payments, and the user has a contractual relationship with the bank (i.e. a bank account).

When referring to third parties, it is possible to define two main approaches: front-end[21] providers and end-to-end providers. With respect to the first ones, there is a platform allowing an interaction between the customer and the seller and also with the bank, which processes the transaction, including clearing and settlement. Are involved into this kind, mobile wallets and e-money institutions. Essentially, the payer initiates the transaction through the bank which organises the transfer, and the funds are received from the payer, as can be noted in *Image 1.* Such platform acts as a "third party payment service provider", whose peculiarities will be discussed in *Chapter 2*.

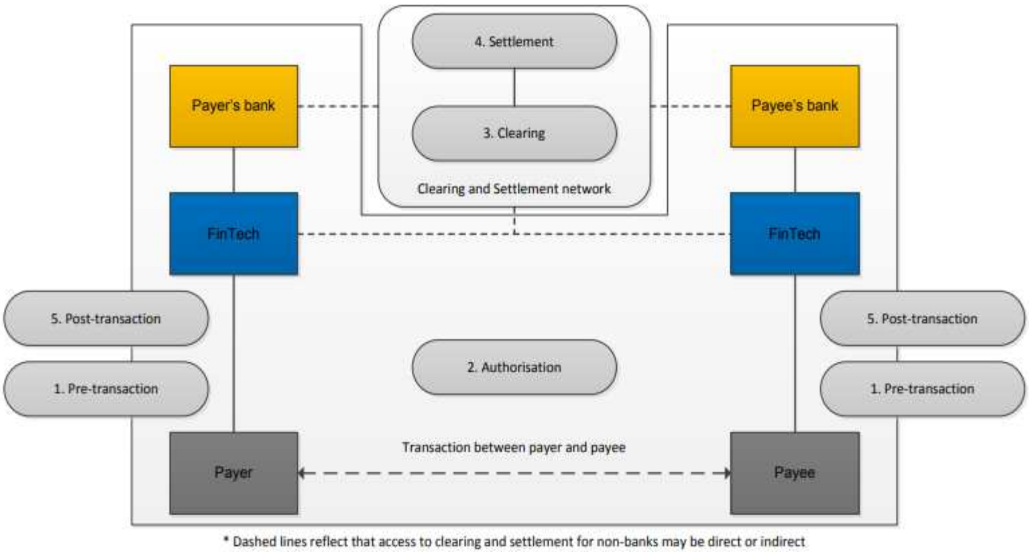
The latter form, instead, does not require the presence of a financial institution to perform the payment. The actors involved execute their actions on a FinTech platform, what they need in order to participate is only their e-mail. This is typically used for virtual currencies exchanges. Currently, it is possible to identify two new entries in the payments landscape: cryptocurrencies and stablecoins. The former term identifies "digital representations of value" which can act like coins but do not represent a legal currency, moreover, they are decentralized and not backed by an asset (such as Bitcoin). Stablecoins, instead, define their value basing on another fiat currency or commodity, they are becoming an interesting subject, not only for firms (as Facebook's Diem) but

[20] EBA: "Report on the use of digital platforms in the EU banking and payments sector", September 2021, EBA/REP/2021/26, page 23.

[21] It is possible to include within this category the Payment Initiation Service providers (PISPs) and the Account Information Service providers (AISPs), thus defined in PSD2, Directive (EU) 2015/2366 that will be explored later in this Chapter.

also for Central Banks, thus we refer to CBDC (Central Bank Digital Currency). These topics will be further discussed in *Chapter 3.*

Image 1: Parties involved in a transaction with a front-end provider


4. Settlement
Payer's bank
3. Clearing
Payee's bank
Clearing and Settlement network
FinTech
FinTech
5. Post-transaction
5. Post-transaction
2. Authorisation
1. Pre-transaction
1. Pre-transaction
Transaction between payer and payee
Payer
Payee
* Dashed lines reflect that access to clearing and settlement for non-banks may be direct or indirect

Source: The Netherlands Authority for Consumers & Markets Fintechs in the payment system, 2017

It is clear that exist new ways of performing payments, for example arranged using payment services providers, as a consequence many questions related to the way of their functioning and their security may arise. First and foremost, what is necessary to define is regulation, to draw the line between what is good and what is not. Specifically, because there are entities outside traditional incumbents which have access to personal information, arising crucial risks. During the years, the European Union has regulated and defined infrastructures for the payments landscape, also analysing the new phenomenon and outlining several rules. Nonetheless, when dealing with technology, labelling the new phenomenon is a complex task, thus arises the "boundary problem": what should be under the regulatory environment and what should not?

1.3 Overview of the payment systems

The payment system can be described as "*a formal arrangement between three or more participants, not counting possible settlement banks, central counterparties, clearing houses or indirect participants, with common rules and standardised arrangements for the execution of transfer orders between the participants*[22]". Within the EU, the single monetary policy is ruled out by the Treaty on the Functioning of the European Union and the Statute of the European System of Central Banks and of the European Central Bank[23]. In 1998 was conceived the European System of Central Banks, which comprises the European Central Bank and the National Central Banks of all Member States, whether they have adopted the euro or not, and co-exists with the Eurosystem[24], the monetary authority. These entities (ESCB, ECB and NCBs) are essential for the payment systems' oversight, supervision and regulation. The article 127 of TFEU provides the legal basis for the ESCB activity, and besides the primary objective of maintaining the price stability, identifies in paragraph 2 the tasks, which include "*the promotion of the smooth functioning of the payment systems*". Additionally, according to the Article 22 of the Statute: "*the ECB and the national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payments systems within the Union and with other countries*". Upon these provisions, they oversee the Financial Market infrastructures, whose correct functioning is fundamental for stability purposes, and since the introduction of the euro (1999), the Eurosystem has contributed for their redesigning. FMIs permit the relation between financial institutions and financial markets, and the clear and settlement of transactions[25].

Considering large-value payment systems, it is possible to define two main infrastructures: TARGET2 and EURO1. The first one (TS2), represents a channel originally

[22] Regulation of Central Bank 795/2014 on oversight requirements for systemically important payment systems of 3 July 2014, ECB/2014/28), Art 1 (3).

[23] Available at: https://www.ecb.europa.eu/ecb/orga/escb/html/index.en.html.

[24] which instead includes only those EU Member States which use the euro as legal currency, and the ECB.

[25] ECB: "*Eurosystem oversight policy framework Revised version*". July 2016.

implemented in 1999, named “Trans-European Automated Real-time Gross settlement Express”. It is operationally managed by the Bank of Italy, the Deutsche Bundesbank and the Banque de France, and it was created to provide real-time gross payment transactions among banks. Its objectives were the enhancement of the safety of payments, efficiency of cross-border ones and integration within the European money market. In November 2007 it was transformed into TS2 which is based on a single shared platform, but still structured as a multiplicity of national payment systems under their NCB scope. EURO1 was also settled in 1999, but it is a private system handled by EBA Clearing, it provides transactions on a net-multilateral basis which are settled through TARGET2 at the end-of-the day. Moreover, in November 2018, was introduced TARGET instant Payment Settlement (TIPS), which accounts for the digitalization in the payments landscape. It represents a step-forward as it embraces innovation, permitting the immediate execution of bank transfers. This platform can handle over 43 million transactions daily and allows individuals to perform exchanges within the Europe in real time, every day and every second. As a consequence, this novelty has blurred the line between wholesale and retail payments since the service is provided for both type of operations.

It is crucial to underline that non-cash retail payments are performed under the Single European Payment Area (SEPA), to which assent all the 27 Member States and some countries[26] outside the EU, facilitating today over 43 billion transactions in 36 countries[27]. It aims to provide safer and easier payments across the participating states, establishing a level playing field. The role of SEPA was described in the 2005 “Lisbon Programme Proposal”: *“The Commission's objective is to create a Single Payment Market where improved economies of scale and competition would help to reduce the cost of the payment system […] this is complemented by industry's initiative for a Single Euro Payment Area (SEPA), aimed at integrating national payment infrastructures and payment products for the euro-zone[28]”*. It was introduced in the

[26] Andorra, Iceland, Norway, Switzerland, Liechtenstein, Monaco, San Marino, United Kingdom, Vatican City State, Mayotte, Saint-Pierre-et Miquelon, Guernsey, Jersey and Isle of Man.

[27] European Payments Council: "*Introducing the EPC”*

[28] Implementing the Community Lisbon Programme: Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market and Amending

1990s, but its implementation occurred right after the euro adoption, in 2002. In the same year the European Payments Council (EPC) was settled, to regulate and develop the project. It has defined several rules and frameworks for credit card operations, and in particular for SEPA credit transfer (SCT) and SEPA direct debit (SDD) whose transactions, within the European Union, require the IBAN code to identify the bank accounts, and the ISO 20022 XML (for financial institutions interexchange). For these services, SEPA was adopted in 2008 by banks, its features were amended with Regulation (EU) No 260/2012 and on 2014 its implementation resulted achieved, accomplishing what was delineated in the European Commission "*SEPA Roadmap*[29]" in 2009.

Nevertheless, the standards' adaptation to the framework has been challenging. First of all because the critical phase of the project coincided with the global financial crisis, thus the resources to be addressed to innovation were dwindling, secondly because the pre-existing infrastructures remained operational (especially for what concerns bank transfers). A key role for SEPA development was played by a normative source, the European Union Payment Services Directive (2007/64/CE) created in 2007. It comparted the objectives of fostering innovation and competition in payment services, through the provision of a pan-European set of rules, to enhance the efficiency of non-cash transactions. Notably, it provided the Member States with a common legal framework, which will be later discussed in this paper. Moreover, on 19 December 2013 the ECB established the European Retail Payments Board (ERPB), which has been improving retail payments in the SEPA area. It accelerates harmonization ensuring that there is no dissolution, providing standards and recommendations. It seeks to promote innovation, accounting for the several existing payments, especially contactless, instant, P2P mobile. Nowadays, the evolution of SEPA is still ongoing, one novelty is the SEPA RTP (Request To Pay). It is active since June 2021 and allows the payer to perform a digital payment request to his/her debtor, related to the kind of good or service

Directive 97/7/EC, and 2002/65/EC (presented by the Commission) COM (2005) 603 final (Dec. 1, 2005), art. 2.

[29] Commission of the European Communities, Bruxelles. 10.09.2009, COM (2009).

provided; the two actors remotely exchange the transaction's data before its occurring, and after that the payee decides whether to perform it and in which form, partially, totally or deferred.

In compliance with this framework, the retail payment system relies on the Clearing and Settlement Mechanisms (CSM) model. This enables the exchange of funds between two payment service providers, which can choose their CSM and make themselves 'reachable' in order to be able to perform the transaction, in accordance with the SEPA rules. In this way, the operators involved perform clearing and settlement, and for the purpose of being reachable the PSPs can use the following options[30]. "Automated Clearing houses (ACH)" which represent many-sided procedures based on common rules, that comply with SEPA, where the pan-European one is STEP2, created on 2003, that defines the PEACH (Pan-European Automated Clearing House – model). Another way is using "decentralised bi- or multilateral clearing and settlement arrangement" conforming to SEPA, where the activities between the PSPs might be agreed upon a third actor (i.e., bank). Otherwise, an **"**intra-*PSP* and/or intra-group clearing and settlement arrangement" compatible with SEPA, where the two PSPs are affiliates of another PSP and use its accounts.

With regards to oversight, the Eurosystem differentiates into systemically important (SIPs) and non-systemically important (non-SIPs) payment systems. Their classification is evaluated each year and is based on several conditions, such as size and activities. Regulation and its compliance is essential for SIPs, because if they are not safe, they could trigger systemic risks; TARGET2 and EURO1 are included within this group. The ECB oversees them, and in August 2014 used its regulatory powers in this field for the first time with the issuance of the Regulation 795/2014 "*on oversight requirements for systemically important payment system*s". It provides stricter rules for this category, fulfilling and making binding the "Principles for financial market infrastructures" (PFMIs). They were delineated in April 2012 by the CPSS-IOSCO[31], and represent the

[30] Available at: https://www.europeanpaymentscouncil.eu/what-we-do/sepa-payment-scheme-management/clearing-and-settlement-mechanisms.

[31] Committee on Payment and Settlement Systems (CPSS) and Technical Committee of the

international standards for payment systems in the eurozone, outlining 24 principles that were first identified in 2012, in response to the global financial crisis, and then revised. For what concerns non-SIPs, the NCBs are in charge for their oversight, they are mostly retail payment systems, thus involve low-value transactions between individuals, and their regulation is based on a subset of PFMIs.

1.3.1 The regulatory framework for payment services

The increasing innovation in payments led the European Union to identify a regulatory framework. In 2000 the EU outlined the Electronic Money Directive 2000/46/EC (EMD1), to provide appropriate measures for credit institutions that dealt with e-money, responding to the takeover of pre-paid electronic products. Nevertheless, this piece of law proved to be misleading and not adequately definite, and consequently repealed by the E-money directive 2009/110/EC (EMD2) on 30 April 2011. It applies to entities pursing the e-money issuance activity[32], and provides a description for electronic money in its Article 2(2): *"electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] which is accepted by a natural or legal person other than the electronic money issuer".* In order to perform the issuance, is required an authorization from the Member State and the possession of a minimum amount of capital at least of 350 000 Euro. The e-money provider is forbidden from taking deposits or other repayable funds from individuals, as it represents an activity feasible only for banks, authorized from the competent authority[33].

Prior to the EMD2, the European Union took a decisive step towards a pan-European regulation in the market of retail payments, previously delineated by different rules applied by the banks in each country: in 2007 the European Parliament and the Council created the Directive 2007/64/EC, defined as "Payment Services Directive" (PSD). As mentioned earlier, it has fostered and supported the implementation of the

International Organization of Securities Commission's (IOSCO).

[32] The categories included are: credit institutions, electronic money institutions, post office giro institutions, the ECB and NCBs, ember States or their regional or local authorities (*Article 1 (1) of Directive 2009/110/EC).*

[33] Regulation (EU) 575/2013.

SEPA, with the provision of a regulatory framework for the Member States, in order to make their systems uniform for the payment services, which the directive regulated for the first time. In particular, this piece of law has specified their characteristics in the "Annex" section, identifying them as business actions that: permit individuals to withdraw or deposit money from/to an account, implement payment transactions (e.g. direct debits, credit transfers, etc.), distribute or receive payment instructions, execute money remittance. Specifically, the directive introduced a new operating group besides banks, the "*payment institutions"* which are able to process the online payments' communication with the banks, actions for which they need the authorization. Nevertheless, FinTech was not actually mentioned in the directive, and in that period, it was not seriously considered yet; in the meantime, technology developed and defined new risks, weaking protection. Moreover, as the European Commission stated in the "Green Paper[34]" in 2012, the European landscape for e-payments remained too fragmented. Consequently, since 13 January 2018 the PSD is replaced with Directive (EU) 2015/2366, the so-called Payment Services Directive 2.

[34] "*Green Paper Towards an Integrated European market for card, internet and mobile payment*s" of the European Commission, 2012. COM/2011/0491.

CHAPTER II: The advent of the Payment Services Directive 2 (PSD2)

The development of FinTech in the financial world has raised serious concerns about personal data because they are now accessible from tech firms. The PSD2 was created with the purpose of enabling innovation and the safety in payment services within the European internal market. Also, to provide customers with a wider range of services, and ensuring higher standards of protection for the usage of electronic devices, platforms and remote communications[35]. The security of electronic payments is crucial for the safeguard of users, and for the improvement of a stable e-commerce[36]. The responsibility in the matter of safety is entrusted to the European Banking Authority (EBA), which supervises and provides guidelines and technical standards, according to the Regulation (EU) 1093/2010[37]. It is possible to designate four main areas the directive aims to regulate: access to accounts, customer authentication, liability for payments and transparency of payments and charges.

The Directive is to be applied to payment services provided across the Union[38], and as happened in the PSD, it does not pronounce a unique explanation of their characteristics rather, as pronounces Article 4 (3), it lays out in *Annex I* a list of the activities included in such definition, namely:

"1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: (a) execution of direct debits, including one-off direct debits; (b) execution of payment

[35] European Commission: *"Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments*", Brussels, 27 November 2017.

[36] Recital (95), PSD2.

[37] Recital 33, PSD2.

[38] Art 2 (1), PSD2.

transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a payment service user: (a) execution of direct debits, including one-off direct debits; (b) execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders.

5. Issuing of payment instruments and/or acquiring of payment transactions.

6. Money remittance.

7. Payment initiation services.

8. Account information services."

The PSD2 underlines the importance of maintaining their description technologically neutral, in order to permit their innovation[39]. The payment services presented are eight, and it is possible to distinguish two new typologies: Payment initiation services and Account information services, whose providers represent the so-called Third-Party Payment service Providers (TPPs). Moreover, it introduced the new term "*Account servicing payment service provider"* (ASPSP), which identifies the classic payment service provider, that supports and maintains a payment account for a payer[40], thus it refers to banks and similar institutions. Additionally, the new Directive includes payment transactions[41] *"in a currency that is not the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union, in respect to those parts of the payments transaction which are carried out in the Union[42]"* which previously were not encompassed in the PSD.

[39] Recital (21) PSD2.

[40] Article 4 (17) PSD2.

[41] Defined in Article 4 (5) of PSD2 as "*an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee".*

[42] Article 1 (a), PSD2.

2.1. Access to accounts and Third-party payment service providers

The Directive regulates three particular types of access: to payment systems, to account services and the ones performed by the TPPs, defining in this way XS2A. The crucial matter in this concern, is the description of the TPPs, and the consequently introduction of the open banking, as they are enabled to enter the payment system. The new payment services, namely the initiation payment services, and the account information services, represent the innovation that the directive 2007/64/EC failed to include within its scope. The Directive underlines the prohibition of the provision of these services by natural or legal persons that are not payment service providers, or in any case not included within the scope[43], and defines differentiated requirements to obtain the authorisation.

Article 35 of the PSD2 delineates the "access to payment systems", affirming that any type of authorized business providing payment services, should be able to access to the payment system[44] in order to be allowed to carry out its activity. In particular, Member States shall ensure the rules, which have to be "*objective, non-discriminatory and proportionate"*. Also, payment systems shall not impose: *"restrictive rules on effective participation in other payment systems; rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; restriction on the basis of institutional status*[45]".

Article 36 of the PSD2 underlines the link with banks, defining the "access to accounts maintained with a credit institution". It states that payment institutions shall be able to access the bank account in an "*objective, non-discriminatory and proportionate basis"*, in order to perform the payment services efficiently. Member states shall ensure these conditions, and if the bank refuses the access, it has to provide

[43] Article 37, PSD2.

[44] The payment system is a *"fund transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions"* Article 4 (7) PSD2.

[45] Those rules shall not be imposed on *"payment service providers, on payment service users or on other payment systems"*.

motivated reasons for such choice. Payment institutions were previously identified by the PSD, and their requirements explained in *"Title II"* of the revised Directive have not significantly changed. In order to be operative, they need a license granted by their home Member State, for which they have to deliver the necessary information, such as a programme of operations, a business plan, a description of the internal mechanism control, the identity of the directors and all the other provisions listed in Article 5. Furthermore, they need a minimum initial capital[46] and have to enter in a specific public register[47] in their home Member State once authorized.

The Directive introduces for the first time the regulation of the TPPs, specifically in articles 66 and 67 defines their access to accounts, respectively about AISPs and PISPs. The government of these new entries is fundamental, as they are innovative non-banking entities offering payment services through a connection with the financial institutions, but are not the payer or the payee in the operations, they act on their behalf. In particular, customers can request the bank to make available their data to a third part and/or to initiate a digital payment through a third-party provider[48].

Account Information Services providers[49] (AISPs) allow the payment user to access the information about all the bank accounts of the payer, delivering a general view of the financial situation at any moment[50] and immediately. Are included in this category the operators that provide information to the final client (therefore are excluded those that never relate to him/her), operators delivering aggregated or consolidated data (not the single information) which are related only to payment accounts (for example, are not considered information connected to securities accounts)[51]. AISPs can provide several kinds of services, for example data could be used

[46] Article 7, PSD2.

[47] Article 14, PSD2.

[48] Deutsche Bank: "*PSD2, open banking and the value of personal data*" 28.06.18, Research.

[49] They provide *"an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider*". Article 4 (16) PSD2.

[50] Recital 28, PSD2.

[51] M. Catenacci, C. Fornasaro: *'PSD2: I prestatori di servizi d'informazioni sui conti (AISPS)'*, in Dir. Banc., 4/2018.

for the personalization of commercials, or to analyse the expenditures behaviour to define a pattern for the client, who can use it to plan and manage the future expenses. It is possible to define three models of AIS: a service realized in a standard manner, which displays the financial situation to the user; a service as a basis for other services of added value, namely the account data can be utilized to elaborate several services such as business management (invoice re-conciliation, services related to credit scoring, better planning for clients' future investments); AIS "as a service", in this situation can be identified a 'fourth part', probably a FinTech entity not regulated, to which data are provided. Thus, data can be transferred, for example in the case of a loan; however, the AISP cannot use them for reasons other than performing the account information service explicitly requested by the payment service user[52], also, data utilized shall be merely the ones related to the payment transaction.

In Article 4 (15), the PSD2 defines payment initiation service provider (PISP) as a "*service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider"*. Thus, it can be used for online purchases, as it creates a bridge between the website of the merchant and the online banking platform[53], gathering the information needed and without requiring the customer to open an account directly with the payment initiation service provider. These operations are possible only if the user has given explicit authorization[54], and the PISP shall not use the information collected for purposes other than the payment initiation service[55], or store sensitive payment data[56] of the payee.[57] Additionally, PISPs are not authorized to hold funds, they just have to perform the transaction on behalf of the actors involved. Three different models can be described referring to PIS: a standard service, which allows the user to perform online payments through SEPA bank transfer, or web or the mobile; a service solely for its clientele, as an

[52] Article 67 (2)(f), PSD2.
[53] Recital (27), PSD2.
[54] Article 64, PSD2.
[55] Article 66 (3)(g), PSD2.
[56] "*Including personalised security credentials which can be used to carry out fraud"*, Article 4 (32), PSD2.
[57] Article 66 (3)(e), PSD2.

additional means of payment for the services offered from the PISP, which become the beneficiary in the transaction; as a service only for business customers, by which small-medium enterprises can avoid the card upper limit and use it as an alternative payment method.

It is crucial to stress that the TPPs activities are possible only if the payment account is available online[58]. None of the TPPs can collect funds from the public and create current accounts, this is a prerogative only of financial institutions. In particular, in order to provide their services, PISPs need a minimum initial capital of 50’000 euros and the authorization, that if is granted, requires the inscription in the register of the Member State; AISPs, instead, only need to present demand for registration. All the information about TPPs are publicly and freely available on the EBA register, which is held online. Besides the other conditions listed in Article 5 (PSD2), TPPs shall hold a professional indemnity insurance covering the territories in which they perform their activities[59], or another similar guarantee. Especially, for PISPs it serves to cover the responsibility in the case of: unauthorised payment transactions (Article 73), the non-execution, defective or late execution of payment transactions (Articles 89 and 90), the right of recourse from other TPPs (Article 92). Furthermore, the third-party payment service providers shall give the security policy document to the Supervisory Authority, where they illustrate the risks involved in their payment services, including a description of security control and mitigation measures taken to guarantee protection against fraud and illegal use of information[60].

TPPs have a contractual relationship with the user for which they provide the account information, or initiate the payment; however, they are not obliged to establish a contractual relationship with ASPSPs, with whom they need to digitally interact, as stated in articles 66 (5) and 67 (4). For their part, ASPSPs must be available and let the third parties access to their accounts, to obtain the information or to initiate the payment (Article 66 (1) and Article 67 (1)), and reciprocally communicate in accordance

[58] Article 66 (1) and Article 67 (1), PSD2.

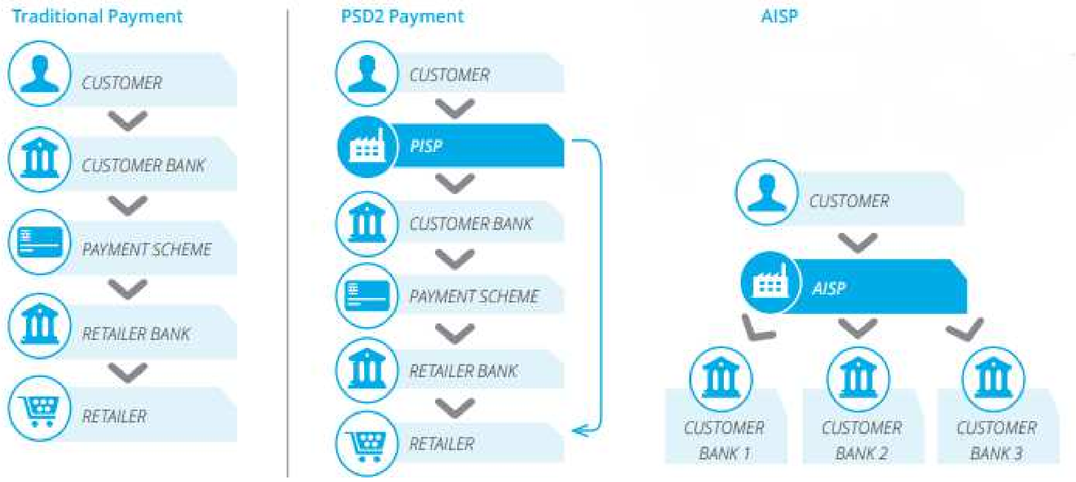
[59] Article 5 (2)(3), PSD2.

[60] Article 5 (1)(j), PSD2.

with Article 98 (1)(d). Insofar, they shall comply with the technical standards provided by the EBA, to ensure adequate safety for users and payment providers, of the funds and the personal data, to support a fair competition and assure the neutrality of technological models in order to allow the development and the innovation of payments. The obligation for ASPSPs to provide to TPPs the access to their accounts, is defined as XS2A (literally 'Access to accounts'). It is important that financial institutions provide facilities and access in an "*objective, proportionate and non-discriminatory manner to any other authorised or registered payment service provider*[61]*"*, and all the information requested without undue delay[62].

A simplified functioning of the payment service providers is presented in *Image 2*, which shows how the operations are now executed, compared to before. It is clear how they ease the process, delivering a faster transmission of data and execution of payments.

Image 2: Illustration of PSPs transactions



Source: Deloitte[63], 2016

[61] Recital 51, PSD2.

[62] Article 58, PSD2.

[63] Deloitte: 'Payments Service Directive 2 (PSD2) Il nostro approccio', 2016.

2.2 The Open Banking

With the provision of XS2A, emerged what can be defined as “open banking”, a term that identifies the new banking model accessible from outside entities. It has revolutionized the activities of financial institutions, which have been transformed into platforms that ease the communication with clients and foster trust. The competitive advantage lies in the “know-where”, that is the knowledge of where the actors contributing to the creation of value, for the bank, are located; this means that financial institutions shall be able to realize how to use their technological advantage[64]. Furthermore, it enhances competition and grants, in particular, SMEs and consumers with easier and more accessible payment services. In order to facilitate it, the bank needs an interface to allow payment service providers (including AISPs and PISPs) to identify themselves, and to communicate securely and receive the information needed[65]. With the aim of permitting the technological neutrality, it is not defined a particular interface to be used, thus financial institutions can decide it.

The EBA Regulatory Technical Standards propose two possible ways: indirect mode through a dedicated interface, or direct mode, known also as “screen scraping”, by utilizing the user interface (through the home banking, which has to account for TPPs constraints). In the latter form, the PISPs directly logs in into the customer account using the personal banking credentials and has access to all the information of the user, including the sensitive ones. Moreover, the bank is not able to identify if it is the TPP or the individual performing the requests, thus it is clear that this operation presents several risks and is not safe. Because of these motives, the EBA forbidden the use of screen scaping. Nevertheless, in the case that the indirect access mode provides inadequate solutions, there is the “fall-back option”, which permits the usage of the ‘home-banking’ method. Since this decision results quite burdensome for banks, as they should be able to put in place both direct and indirect access mode, the National

[64] "*Open banking e API: la banca del futuro”,* Deloitte, 2019.

[65] Article 27 (1) of EBA ‘*Final report: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)’* EBA/RTS/2017/02, 23.02.2017

Competent Authorities can delineate some exemptions for the fall-back option, reducing the burden for banks.

The preferred choice is the indirect access mode, in particular the Application Programming Interfaces (API), which can be defined as "a way for two computer applications to talk to each other over a network using a common language that they both understand[66]*"*. The EBA does not oblige the use of API but finds it suitable for the industry, indeed it represents the main mechanism used. As it is accessible from everybody, it is correct to talk about 'Open API'. It allows the exchange of information throughout networks that do not belong to the same domain; thus it makes possible to securely share data with third-party payment providers. It is a safe structure with defined characteristics and can be described as self-service as it is also reusable and scalable[67].

It is essential that ASPSPs provide access to PSPs, without contract and barriers, however their permission to XS2A is subject to a control from the financial institutions. They will check its identity, the authorization (hence that the PSP is recorded in its National Competent Authority register), and what particular service regulated from PSD2 it provides. Until these details are not validated, the ASPSPs will block the access[68]. For the identification, the article 34 of the EBA RTS affirms that PSPs shall "*rely on qualified certificates for electronic seals*[69] *or qualified website certificates*[70]*",* and for this purpose, they refer to the Regulation (EU) 910/2014[71] of the European Parliament and

[66] Jacobson et al., 2012.

[67] Euro Banking Association: "*Understanding the business relevance of Open APIs and Open banking for Banks*" EBA Working group on Electronic Alternative Payments, Information Paper. 7 (2016).

[68] Open Banking Europe: "*Third party provider user management for PSD2 Access to Account (XS2A)"*, PRETA S.A.S., 2017.

[69] *"qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III"* of regulation (EU) 910/2014.

[70] "*qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV"* of regulation (EU) 910/2014.

[71] on electronic identification and trust services for electronic transactions in the internal market.

of the Council, defined also as 'eIDAS regulation'. On its article 3 (30) and Article 3(39) it identifies the meaning of these requirements.

2.2.1 Transparency in the PSD2

The Directive lays down also rules to promote transparency in payment transactions. In this regard, in Article 15 PSD2 entrusts the EBA with the development and the control of the electronic register containing the details about authorized PSPs, which should be freely available online in its website. National competent authorities of Member States, are in charge to provide with accuracy the information about PSPs, as lays down Article 14 of the PSD2, and notify the EBA. In particular, the European Banking Authority has developed Regulatory Technical Standards in close cooperation with the ECB, as mandated by PSD2 in several articles[72], and also guidelines. The objective of the RTS defined in article 98 of the PSD2, are: ensuring safety and security for the payment service user and the PSP, including the personal data and funds, maintain fair competition, ensure technology neutrality, allow a user-friendly and easy development of means of payment[73].

Title III of the Directive disposes the transparency of conditions for payment services, it is essential that users obtain "*high level of clear information about payment services in order to make well-informed choices and be able to choose freely within the Union*[74]*"*. This section addresses "*the single payment transaction, framework contracts and payment transactions covered by them*[75]*"*. It does not exist a specific definition for single payment transaction, hence it can be considered as a transaction which is not ruled by a framework contract, term that instead retains an explanation. Article 4 (21) defines it as a "*payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account".* In any case, the PSP shall not charge the

[72] Recitals 41, 108. Articles 5 (6), 15 (4), 25 (5),

[73] EBA: '*Final report: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)'* EBA/RTS/2017/02, 23.02.2017

[74] Recital 54, PSD2.

[75] Article 38 (1), PSD2.

user about the information provided, unless there is an agreement between the two actors, under the client's request, for additional communications[76]. Nevertheless, the charges shall be reasonable[77] and the intention should not be making a profit. Additionally, the payment shall be performed in the currency agreed between the actors involves[78].

Chapter 2 refers to single payment transactions, article 45 of the PSD2 outlines the several information and conditions that PSPs have to make available to the payment users, as the applicable change rate and the maximum execution time of the service. Chapter 3, instead, focuses on framework contracts, and article 52 of the PSD2 is fundamental, as describes all the information and conditions that shall be provided to the payment user. They concern the payment service provider, specifically the name, the geographical address, the register of authorization and so on. Also, are explained those about the use of the payment service, thus its characteristics and how the process works. Are included specifications regarding charges, interest and exchange rate, communication, safeguards and corrective measures, redress and termination of framework contract.

2.3. The payment process

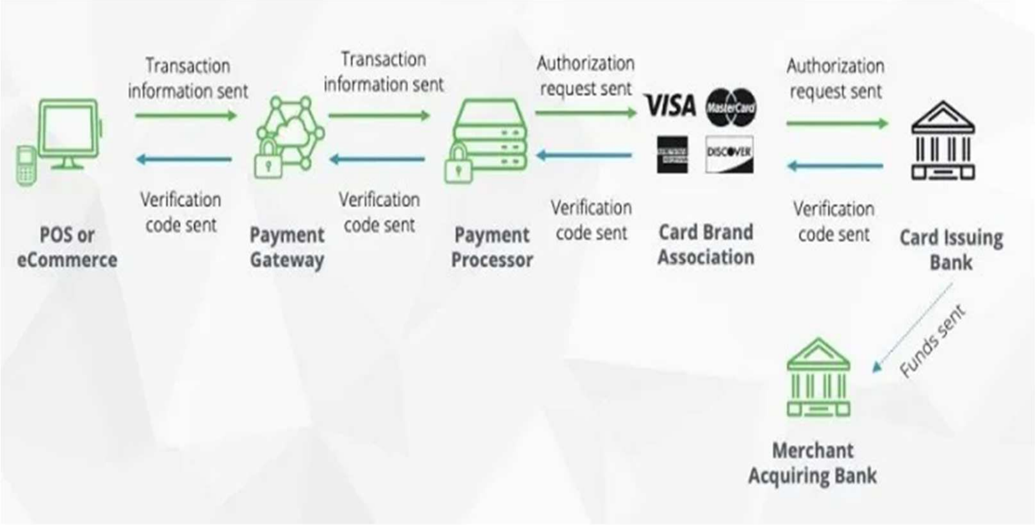
Focusing on the execution of payment transactions, it is possible to outline at least two parties involved: the payer and the payee. When the exchange is performed online, it is possible to identify two mechanisms: three-party model and four party-model. In the former, there is only one Payment Service Provider, impersonating both payer and payees (an example is American Express). For this reason, it is not under the scope of the PSD2, as are left out "*payment systems composed exclusively of payment service providers belonging to a group[79]*", in particular the PSD2 in Recital 52 excludes third-party schemes as *"they never operate as de facto four-party card schemes, for*

[76] Article 40 (1), (2), PSD2.
[77] Article 40 (3), PSD2.
[78] Article 59, PSD2.
[79] Article 32 (2)(b), PSD2.

example by relying upon licensees, agents or co-brand partners”. However, if the named model presents at least one licensee, agent or co-brand partner, it falls under the Directive regulation, as it resembles the four-party scheme and does not represent a ‘pure’ three-party one.

In the four-party model, as the term says, there are four actors involved in the transaction, namely: the customer who purchases the service or good, his/her bank which manages the funds, the merchant (the store) that accepts the payment and the acquiring bank, which holds the account of the merchant. Nevertheless, the operation is a bit more complex than how it appears, and as can be seen in *Chart 5,* there are other entities engaged.

Image 3: The four-party payment process



Source: NCR Corporation, 2021.

Thus, the real number of the parts involved is six: the customer, the acquirer, the issuer, the merchant account (or provider), the payment processor and the payment gateway. The client starts the payment in order to buy a good or a service in the online website, or using the card at the POS, and authorizes the transaction. Consequently, the payment gateway acts as a bridge that safely transmits the information between the payer and the merchant, and decides whether to allow or refuse the transaction, based on the credentials provided. It smooths the process and uses encryption[80] to enhance safety for the data involved. Then, the payment processor receives the information, authorizes the flow exchange and communicates with the Card Brand Association (which depends on the card used, it might be Visa or Mastercard for example). Subsequently, it connects with the issuing bank, which controls the effective availability of funds in the client's account, confirming or denying the transaction. The response is forwarded to the payment processor through the card network, if it is affirmative, it is then forwarded to the payment gateway which, in turn, provides the response to the interface used from the merchant. At the end of the day, the merchant will have to approve the transaction, or provide the order if online, and the funds will be placed from the issuing bank to the acquirer one. Nevertheless, the single payment service provider is able to deliver payment gateway, processing and acquiring services, where all the interactions with banks are made possible thanks to the XS2A, which permits the access through the APIs.

To make these transactions possible, the seller has to possess a merchant account, which is merely a bank account able to accept customers' funds, where the purpose is not saving money but being capable to receive them. The crucial parties involved in the transactions are represented by the payment processor and the payment gateway. The former denotes the firm that actually manages the card exchanges, also it offers the possibility to make purchases using several means of payment, which would represent an advantage for the business as it would meet the individuals' preferences. It is possible to identify front-end payment processors, which establish the connection with the cards network and manage the merchant account, and back-end ones, which instead arrange the transfer of funds. Focusing on payment gateways, they facilitate the online exchange and are present in almost each node of the procedure. They can be established with the firm of the credit card, or with the merchant account provider. Both payment processor and payment gateway can be chosen from the seller, according to the type of business he/she runs. Another alternative could be the payment aggregator, which does not entail the creation of the merchant account but might pose several risks.

[80] It is a process to encode the information, which transposes the original form into another which is safer.

The widest used one is PayPal, which has its own payment gateway, Payflow.

As it was introduced in *Paragraph 1.2.1,* it is possible to identify front-end providers, which are nothing but PISPs and AISPs, and end-to-end providers. These categories are defined basing in which segment of the payment transaction the provider operates. The first form identifies the TPPs, as they communicate with customers and the financial institutions, without being involved in the clearing and settlement stage, as shown in previous *Image 1.* They remove barriers and ease the transaction. However, people are becoming increasingly interested in end-to-end providers, closed platforms that fulfil the payment request without the assistance of financial institutions, except to perform a transfer of funds from the payment account in the FinTech involved. They do not rely on third parties and establish a direct relation with the payer and the payee, as they both possess an account with the same firm. This typically happens for third-party schemes, virtual currencies and PayPal (which is compliant with PSD2). Both front-end and end-to-end providers generate value in payment services and define innovative experiences for end-users[81]. Nevertheless, according to the classification provided by the Bank for International Settlements (BIS, 2014), exists another group, namely the back-end providers. They are dedicated to particular tasks of banks. The financial institution might require a FinTech firm to perform a defined service, under the existence of a contract, excluding the clearing and settlement activities.

2.4 The payment user authorization and the SCA

In a payment process is required the authorization of the payer, in order to perform the transaction. Its significance is identified in the Chapter 2 of Title IV in the Directive, in particular article 64 asserts that *"the payment transaction is considered authorized only if the payer has given consent to execute it [..] in the form agreed between the payer and payment service provider […] in absence of consent, a payment transaction shall be considered not authorized",* Member States shall assure its legitimacy. It is important that such authorization is explicit, and according to the EBA

[81] Namely, the payer and the payee.

"*where AIS or PIS are provided to a payment service user (PSU) following a contract that has been signed by both parties, ASPSPs do not have to check consent. It suffices that AISPs and PISPs can rely on the authentication procedures provided by the ASPSPs to the PSU, when it comes to the expression of explicit consent*[82]*"*. Thus, what defines the authorization is the authentication process, which is regulated in article 97 of the PSD2. The PSP does not handle the personal information of the customer, as it is not allowed to, instead they are transmitted through safe channels. Article 30 of the EBA RTS asserts that when information are transferred through the Internet, encryption is necessary between the collaborating parties, to protect privacy and the reliability of data. It is also crucial that PSPs arrange transaction monitoring mechanisms, to identify whether a payment exchange could be fraudulent[83].

Under these conditions, the Directive introduces the obligation for the payment service providers to apply the Strong Customer Authentication (SCA), a strict security requirement for electronic payments, to reduce the risk of frauds and protect the sensitive data of users. Thus, it is utilized whenever the payer accesses the online account, initiates an electronic transaction and performs any action through a remote channel which entails fraud risks[84]. The SCA is used to validate the payment user identity, and it is based on two or more elements, classified as knowledge, possession and inherence[85]. The first one indicates something that only the individual knows (such as a password, or the PIN), possession reflects an element that only the user possesses (as the card), and the last one defines something that just the interested person is, for example biometric features (as fingerprint or voice recognition)[86]. These elements are independent, hence the violation of one of them, does not jeopardise the other ones. The two-factor authentication provides the creation of an authentication code, which is used to perform the online operation. It cannot be falsified, also it is not possible to deliver a new code from a preexisting one, and it cannot reveal the elements of the SCA.

[82] *Opinion of the EBA on the implementation of the RTS on SCA and CSC*, (EBA-Op-2018-04), Paragraph 13.

[83] Article 2 (1), supra note.

[84] Article 98 (1), PSD2.

[85] Article 4 (1), EBA RTS.

[86] Recital (6), supra note.

An example of its implementation is the 3D Secure Standard. It represents a service that needs to be activated by the user and provides a temporary code sent to the mobile of the payer, in order to authorize the payment; since the year 2021, there is another enactment of this facility which entails the definition of a six-digit code, chosen by the card owner.

In the case of remote payment transactions, fraud risks are higher consequently, in order to enhance the security, the PSD2 requires the dynamic linking between the specific quantity to be paid and the specific payer[87]. According to article 5 (1) of the EBA RTS, PSPs shall ascertain that the payer is aware of the amount of the payment and of the payee; that the authentication code produced is specific to the indicated amount and the payee agreed to by the payer at the beginning of the transaction; eventually, that the authentication code accepted matches the specific amount and the specific payee, otherwise if these two elements change, the authentication code is no longer valid. The dynamic linking is feasible through authentication codes, for which the RTS do not provide stringent constraints, to allow for technological neutrality[88]. They could be one-time password, digital signature or other cryptographical keys.

The implementation of SCA has been challenging for many retailers, and so has been the realization of APIs for financial institutions. Thus, the expected due date for PSD2 compliance, that was on 14 September 2019, was rescheduled on 30 December 2020. This renewal aimed to provide further time for PSPs and Financial institutions to take all the necessary measures in order to be conforming to PSD2, accounting also for the crisis period caused by the covid-19 pandemic which has raised also other agendas. In June 2020, the EBA issued an opinion concerning obstacles encountered by PSPs on SCA. In particular, they addressed the issue of being redirected to the ASPSP, in order to authenticate the payment user. This represents an obstacle, as payment service providers want to offer their own service. The EBA pronounced that the redirection itself does not raise a concern, but it is when defines tension in the customer experience, as unnecessary procedures should be avoided. Moreover, the European Banking Authority

[87] Article 97 (2), PSD2.
[88] Recital 4, EBA RTS.

stated that if the PSP allows the individual to authenticate him/herself using the ASPSP mobile app, this falls within the two-factors authentication used for the SCA; however, in the case the user is using the PSP's app, after the authentication through the ASPSP app, he/she should be promptly redirected back to the PSP one, without having to manually re-access it, which would instead define an obstacle. In the case where the person is not using the PSP app in the mobile, the redirection to the ASPSP website page to insert the credentials, is not an impediment. Furthermore, an additional assertion was provided with respect to multiple SCAs. In the case the PISP communicates all the necessary information to the ASPSP, including the IBAN of the account to be charged, the EBA supports the requirement of a single SCA, as two would represent an obstacle.

There are some exemptions for the SCA implementation, specified in Chapter 3 of the EBA RTS, to promote user-friendly means of payment. For instance, are excluded low-value contactless payments (below 50 Euros), that also determines a maximum number of consecutive transactions or a defined fixed minimum value of consecutive transactions, without the SCA[89]. Are exempted also electronic payments transactions commenced at unattended terminals, where SCA would not be suitable because of security risks[90], as well as transactions considered low-risk. Furthermore, the derogation could be supplied because there is another authentication mode in force.

The SCA implies security credentials with the aim of reducing unauthorized payment transactions, and the risk of fraud. For what concerns these situations, the PSD2 defines the allocation of liability. In the case that the PSP does not apply the SCA, the payer will receive the full refund for the damage (if there is no fraud) as the PSP bears the liability for such losses. Article 75 of the PSD2 refers to direct debits[91] initiated through a card, where the amount of the exchange is not known in advance. In these circumstances, after the consent from the payer about the exact amount to be retained, the PSP can block the funds on his/her payment account and release them as soon as the exact sum becomes known. Articles 76 instead, states that in the case of a direct

[89] Recital 8, EBA RTS.

[90] Ibid.

[91] *Payment transaction initiated by the payee on the basis of consent of the payer to the payee.*

debit, already authorised and executed, the payer is allowed to receive the refund if: the precise amount of the exchange was not specified, and if the amount already paid exceeded the reasonable sum that the payer would have expected to pay, in such conditions. The burden of proof is on the payer, and according to article 77 of the PSD2, he/she can request the fund within 8 weeks from the disbursement, and the payer's service provider shall provide the refund, or a justification for its denial, within 10 days.

In the event of an unauthorised payment transaction, the payment user has to notify the PSP without undue delay on becoming conscious of such occurrence, in particular no later than 13 months from the charge[92]. Article 72 of the PSD2 underlines that if a payment user denies the authorization of a payment transaction, or states that it was not correctly executed, it is on the payment service provider to prove that it was actually authenticated and not affected from technological breakdown. Additionally, in case of an unauthorized payment transaction, the payer's payment service provider has to deliver the refund immediately, except in the case that it has justified suspicion of fraud, where it notifies the national relevant authority in writing[93].

If the unauthorized payment transaction is the result of a stole or lost payment instrument, or a misappropriated one, the payer will bear the losses up to a maximum of 50 Euros, unless such event is not noticeable from the payer before the payment. Nevertheless, the payment user will bear all the losses if he/she acted fraudulently[94]. There is not an upper limit also if the individual does not respect article 69 of the PSD2, which defines the obligations of "the payment service user related to the payment instruments and the personalised security credentials". Namely, the payment instrument shall be used in accordance with its defined terms, and the user must notify without undue delay the PSP in the case such instrument is lost or stolen. Moreover, it is essential that the individual keeps safe his/her security credentials, taking any possible measure for such objective.

[92] Article 71, PSD2.
[93] Article 73, PSD2.
[94] Article 74, PSD2.

2.5 Bodies of law in accordance with PSD2

The use of open banking rises several risks, as there are many interconnected subjects involved in the payment transaction, and particular troublesome is cyber risk. This term addresses the possibility that sensitive data can be violated, falsified, used improperly or for frauds, and that the system can be attacked, also from DOS[95]. With the aim of reducing these threats, the PSD2 cooperates with existing legislative frameworks. An important focus shall be given to Regulation EU 2016/679 of the European Parliament and of the Council, called also General Data Protection Regulation (GDPR), and to *Directive 2018/843* of the European Parliament and of the Council, defined as Anti-money laundering directive (AMLD5).

2.5.1 The General Data Protection Regulation

The GDPR is particularly relevant for the privacy of data, as it relates to the protection of natural persons with respect to the processing of their personal information[96] from people, organizations or firms. The regulation recognizes the need of personal data[97] protection, as their exchange throughout the EU and cross-borders has significantly increased[98]. Notably, the technological advancement has presented new challenges for safety, as people make their personal information publicly and globally available more easily, to both private and public entities[99]. Under these circumstances, the GDPR intends to enhance trust in order to allow the digital market development[100], and for this purpose, the regulation is planned to be technological neutral[101]. There is a strong relationship between the PSD2 and the mentioned

[95] The acronym stands for "Denial of Service" and denotes a malfunctioning of an online service, caused by a cyber-attack which compromises the entire system.

[96] Article 1 (1), GDPR.

[97] Article 3 (2) of GDPR identifies personal data as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

[98] Recital 5, GDPR.

[99] Recital 6, GDPR.

[100] Recital 7, GDPR.

[101] Recital 15, GDPR.

regulation, as PSPs make wide use of personal data, and it intends to provide safeguard to users. It is crucial that all payment service providers comply with the mandatory data protection and security requirements, laid down in the PSD2 and in the EBA RTS, although the Directive also provides a clear reference to the GDPR in its article 94 (1), more precisely it mentions Directive 95/46/EC[102]*,* but it was repealed with the regulation EU 2016/679. Recital 89 of the PSD2 states that when PSPs process personal data, they shall specify the exact intent, the relevant legal basis, the conformity to the relevant safety requirements of GDPR and that *"the principles of necessity, proportionality, purpose limitation and proportionate data retention period are respected".*

It is possible to distinguish between controllers and processors, among payment service providers. The formers "d*etermine the purposes and means of the processing of personal data*[103]*".* In order to process personal data, they need the legal basis, for which a restraining and detailed list provided in article 6 (1)[104] of GDPR. It is up to the PSP the definition of the suitable legal basis, based on the characteristics of the specific service, and the assurance of the compliance with the conditions. In particular, article 6 (1) (b) of GDPR defines the one for payment services, addressing the need of an existing

[102] This is due to the prior creation of the PSD2, compared to the GDPR.

[103] EDPB: "*Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0"*, June 2020.

[104] The lawfulness of the process is guaranteed if at least one of the following conditions is respected:
"a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

contract between the parties, which is consistent with recital 87[105] of the PSD2. Nevertheless, article 7 (4) of GDPR underlines the concept of "*necessary for the performance of the contract*" referring to the provision of service, which requires more than a merely contract term to permit the treatment of the user information. Thus, the controller shall demonstrate that the object of the agreement stipulated with the client, is not achievable without the process of personal data, but if it is not capable to demonstrate the necessity, there is not ground for such legal basis, and another one is required.

In order to define whether article 6 (1)(b) represents a sufficient legal basis, it is important to account for the particular aim, purpose, or objective of the service[106], in addition, article 5 (1) (b) introduces the principle of purpose limitation, stating that data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".* With the aim of processing the payment transfer, ASPSPs shall allow TPPs to enter in their user accounts, thus banks have access to personal information. There is not a contract, but a legal obligation, and the legal basis for such action is provided by article 6 (1) (c) of GDPR, nevertheless the duty for ASPSPs is to be enshrined by the national law. Paragraph 4 of article 6 in the GDPR, determines the possibility, for the controller, to use the payer's personal data also for other purposes than the initial one if she/he approved, providing consent. Nonetheless, as highlighted earlier, according to articles 66 and 67 of the PSD2, the TPPs shall not store or use the personal data collected for purposes different from the payment initiation and the access to account services, previously agreed with the payer. Therefore, the Directive significantly reduces the power of article 6 (4) of GDPR.

The limited use of personal data from TPPs is coherent with the concept of "data

[105] Recital 87 of PSD2 states: '*This Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider. However, the proper functioning of credit transfers and other payment services requires that payment service providers and their intermediaries, such as processors, have contracts in which their mutual rights and obligations are laid down".*

[106] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, page 8.

minimization” laid down in article 5 (1) (c) of GDPR, which states that data can be “*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”.* In particular, the AISPs shall select the pertinent information for the payment contract before the collection of data, and the ASPSPs are allowed to share data only after the permission from the user. For this purpose, the European Data Protection Board (EDPB) recommends the utilization of appropriate technical instruments from AISPs, that enable the merely collection of the relevant information.

Another crucial matter in GDPR is represented by consent, and in article 4 (11) of the regulation it is defined as “*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”*. Hence, “freely given, specific, informed, and unambiguous” are fundamental for the legitimacy of consent. It can describe a sufficient legal basis only if the interested party can have control and the real possibility of choosing whether to accept the terms proposed, or refuse them without suffering prejudice[107]. The controller has to supervise that all the requirements for consent are satisfied, in the case they are not, the data subject will have a deceptive control, and the legal basis is not valid. In particular, article 7 of GDPR enlists the conditions for consent; the controller must be capable to demonstrate the existence of consent when processing information, also “*the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language”,* and the data subject shall be able to withdraw consent at any time.

Article 9 of GDPR indicates certain categories of personal data that cannot be revealed, and the cases where the rule is not appropriate. This rule applies also to payment service providers, and the derogations of the paragraph 2 of the article that concern them, are letters a) and g). Respectively, they state that the prohibition does not apply in the case *“the data subject has given explicit consent to the processing of*

[107] EDPB: *“Guidelines 05/2020 on consent under Regulation 2016/679*”.

those personal data for one or more specified purposes", and when *"processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".* This is possible only if the PSP is capable of demonstrating the application of such exemptions.

In this context[108], is introduced the "explicit consent", where "explicit" identifies the mode used by interested part to provide consent, namely through a declaration. The safest way is a written signed declaration, but it could be possible also with a phone conversation, and when digital, the explicit consent can be guaranteed through an online form sent with the e-mail, or with a digital signature[109]. Under no circumstances the consent can be deducted from actions or declarations potentially ambiguous. Nevertheless, this argument is complex according to the EDPB, as also in the PSD2 appears the concept of "explicit consent". In particular, paragraph 2 of article 94 of the Directive asserts that PSPs shall access, process and retain personal data that are needed in order to deliver their services, if there is the explicit consent of the payment service user. Pursuant to article 33 of the PSD2, such requirement does not apply to AISPs, nevertheless it is demanded in article 67 (paragraph 2, letter a), in order to allow the access from the account initiation service providers. The EDPB[110] is of the opinion that the "explicit consent" identified in the PSD2 refers to the contractual consent, in the sense that when stipulating a payment contract with the PSP, the payment users have to be informed about the particular personal data needed for the transaction, the type of service and they have to accept the terms; thus, article 94 does not provide a legal basis, but aims to provide transparency and control to the payment user.

There is an important issue, the one arise by the "silent party data". This occurs when the personal data processed belong to individuals that are not users of the

[108] Article 9 (2) (a), GDPR.

[109] EDPB: "*Guidelines 05/2020 on consent under Regulation 2016/679*", page 24.

[110] EDPB: "*Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR".*

payment service provider, nonetheless they are used to execute a contract between the payment service user and the PSP. An example provided by the EDPB[111], is when the data subject A uses the services of an AISP, and the data subject B has performed a transaction to the account belonging to A; in this case, B can be defined as "silent party" and his/her information (for example, the account number or the amount of the exchange) are considered "silent party data". As stated earlier, article 5 of GDPR limits the use of personal data, however the regulation permits they usage of silent party data from PSPs "*for the purposes of the legitimate interests pursued by the controller or by a third party[112]",* only in the case where such interests are not *"overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data[113]".* The PSD2[114] does not explicitly consider "silent party data", but their usage from PSPs could have as legal basis the paragraph 2, letter f) of article 6, just referred. The handling of these data shall be limited and the controllers have to dispose of the necessary safeguards, including technical standards to ensure that personal data are not used for other purposes than the ones initially agreed, and protect the data subjects' interests.

2.5.2 The Anti-money Laundering Directive

The access from third-parties to individuals' personal data, granted by the PSD2, might arise risks, in particular fraud risks, money laundering risks, supervision and investigation risks[115]. It is possible that criminal PSPs enter the market, and in order to reduce such threats and enhance security, the PSD2 explicitly requires the compliance with the Directive (EU) 2015/843[116] of the European Parliament and of the Council, the so-defined anti money laundering directive (AMLD). The first ever anti money laundering directive was envisioned in 1991, it recognized the crucial influence of money laundering

[111] Ibid.

[112] Article 6 (2) (f), GDPR.

[113] Ibid.

[114] Recital 87 states *"this Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider",* it does not mention the "silent party".

[115] AMLC: "*The Second European Payment Services Directive (PSD2) and the Risks of Fraud and Money Laundering*", October 2017.

[116] In the Directive is indicated Directive (EU) 2015/849, thus the 'AML4', as the AML5 was defined after the PSD2 creation.

in the rise of criminal organizations and drug trafficking[117]. In the following years, it was amended from two subsequent new directives (AMLD2 in 2001 and AMLD3 in 2003), which introduced new requirements enhancing safety and supervision; in particular, were introduced the know your customer (KYC) and the Customer Due Diligence (CDD) rules, and the inclusion of Finance Terrorism Countering (CTF). Nevertheless, the AMLD was further changed after the global financial crisis, in 2015, with the introduction of AMLD4 which announced the risk-based approach outline. It was then repealed with the AMLD5 in 2018, which represented a "minimum harmonization directive", to allow for the different approaches that member States choose to apply. Nonetheless, this also implied issues, as firms have to report information using different methods and technologies, in accordance with the several countries, generating inefficiencies and preventing harmonization.

In May 2020, the European Parliament and the Council defined a proposal for a directive "on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849", implemented within June 2021. This so-called AMLD6, aims to enhance the harmonization within the EU and the protection from ML/FT in the money exchanges, and improves the previous indications of the AMLD5. The directive requires its compliance from "obliged identities[118]", recognized in its article 2. It is crucial to affirm that the AMLD applies also to payment service providers, as in its article 13 (2) (a), financial institutions are described also as "*payment services as defined in point (3) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council[119]*". They shall apply the risk-based approach, namely they have to evaluate the level of risk as first thing, and subsequently take the adjustment actions needed for the specific case. This requires the implementation of

[117] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

[118] "They are financial institutions, credit institutions, as well as trust organisation, estate agencies, gambling services and other legal persons trading in goods and of payments to the extent that payments are made or received in cash amounting to 10 000 Euro or more".

[119] Annex I of Directive 2013/36/EU of the European Parliament and of the Council, of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

the CDD, which according to article 13 (1), requires obliged entities to: "*identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source*" that could be in paper or digital form; "*identify the beneficial owner and take reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is*"; "*assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship"; "conduct ongoing monitoring of the business relationship, which includes transaction monitoring and keeping the underlying information up to date".*

In addition, article 11 indicates in which circumstances CDD shall be applied. Specifically, when the individual executes an occasional transaction, it does not exist a business relationship, and "*there is a transaction, or series of linked transactions*[120] *that: is equal to, or exceeds, EUR 15 000 and is not a transfer of funds as defined in Regulation (EU) 2015/847 (the Wire Transfer Regulation (WTR)), or is equal to, or exceeds, EUR 1000 and constitutes a transfer of funds as defined in the WTR*[121]*".* Nevertheless, the limit of 15.000 Euro has exposed weaknesses, for example financial institutions try to circumvent stringent applications of AML/CTF through the provision of products that lie within such constraint, also there might exist unobserved terrorist financing as the amount of funds is modest. Moreover, it is not evident how such threshold shall be applied to PISPs and AISPs, because the former group not always defines a business transaction with the payment customer, also, both TPPs never execute a payment transaction themselves and/or hold funds. In particular, AISPs are not involved in the payment chain. On these grounds, the ML/TF risk is reduced.

The EBA has developed Guidelines[122] to better explain how the AMLD shall be

[120] The directive does not provide a meaning for occasional 'transaction' and 'series of linked transaction'.

[121] EBA/REP/2020/25, "*EBA report on the future AML/CFT framework in the EU, Responses to the European Commission's call for advice on defending the scope of application and the enacting terms of a regulation to be adopted in the field of preventing money laundering and terrorism financing",* page 13.

[122] EBA: "*Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the*

applied, and tackles the TPPs subject. EBA states that when there is an assessment about the ML/TF risk for PISPs and AISPs, some conditions that might increase such threats shall be considered. Namely, the case where a payer provides the same payee with several transactions to different payment accounts, defining a large amount without a clear economic explanation; similarly, when an individual performs fund transfers from separate accounts in order to escape thresholds (in the case of AISPs); eventually, the event that the payment user "*receives funds from or sends funds to jurisdictions associated with higher ML/TF risk or to someone with known links to those jurisdictions*[123]*".* The risks decrease in the case that transactions (regarding PISPs) are performed in a Member State compliant with the AMLDV, and also if the accounts are held in such countries (related to AISPs).

As stated previously, PSPs fall under the scope of the anti-money laundering directive, thus they have to apply adequate instruments to identify the ML/TF risks, and the CCD rule in compliance with article 13 of AMLD. In this respect, PSPs have to "*rely on the source of funds as evidence of the customer's identity where the payment account details of the customer are known, and the payment account is held at an EEA-regulated payment service provider*[124]", verify the client's identity in a delayed moment with respect to the settlement of the relationship, and assume "t*he nature and purpose of the business relationship*[125]". AISPs shall always know every detail of the newly created account.

Nevertheless, there is a debate whether TPPs shall fall under the scope of the AMLD. The European Payment Institution Federation[126] (EPIF), in response to the EBA public consultation on AML/CTF guidelines, in June 2020 provided its scepticism about TPPs regulation within the anti-money laundering directive. It underlined the low-risk of

money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines"), amending Guidelines JC/2017/37", 5 February 2020.

[123] Ibid. page 132.

[124] Ibid. page 134.

[125] Ibid.

[126] Founded in 2011, represents the interests of the non-bank payment sector at the European level.

these entities, especially of the ASIPs as they do not carry out financial activities and represent merely ‘informants’. Furthermore, it questioned the definition[127] in the EBA guidelines provided for PISPs’ customers, and created its own: “*multiple business models can exist where the customer can either be the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user) in case of a stand-alone PIS, but where the PIS is provided to a merchant, the customer can be that merchant with the Payment service user not always being a customer as well”.* The EPIF addresses the importance of recognizing the existence of several PISPs, in particular the PISP might have a relationship with the merchant and possess all the relevant information, and at the same time no relation with the payer, hence it would not be possible to apply the CDD rule. Also, the ASPSP would have already performed the KYC on the client, before granting the access to the account. Thus, in EPIF’s opinion the compliance with the AMLD represents a burden for TPPs, which already have to apply the SCA in order to promote safety and recognize the customer identity.

Also the “European Third Party Providers association” (ETPPA)[128] has expressed similar concepts, in November 2021. It has requested the carve out of TPPs from the AMLD scope, stating that they should not be considered financial institution, rather “providers of software tools”, as they do not handle funds and conduct financial activities. Analogous ideas were provided also by the “Financial Data and Technology Association[129]” in February 2020. It requested to the European Commission the revision of the AMLDV, in order to eliminate the TPPs from its scope. As the previous opinions, also FDATA considers AISPs information providers, thus they do not entail the ML/TF risks, because there is not exchange of funds. What these entities provide is merely data, which are not a method for laundering actions. In particular, according to article 33 of

[127] “The customer is the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user)”.

[128]ETPPA is the leading EU fintech trade association for bank independent Third Party Providers (“TPPs”) under the EU’s second payment services Directive (“PSD2”) and beyond; it represents TPP interests on the key payment forums in Europe.

[129] FDATA is a not-for-profit global association for financial services companies operating in Open Banking and Open Finance.

the PSD2, which exempts AISPs from the need of authorisation, their inclusion in the AML provisions does not seem suitable. Instead, the compliance results costly and burdensome, preventing the innovation objective of open banking. Focusing on PISPs, the FDATA affirms that the necessity to request to users information as the name and the address, store them and utilize an electronic ID verification system, with the aim of comply with CDD, is costly and detrimental for competition. Moreover, these types of data shall not be collected from PISPs, as article 67 of the PSD2 prohibits such action, like the verification using the electronic ID. This would be in contrast also with article 5 (1) (c) of GDPR.

CHAPTER III: Cryptocurrencies and the role of PSD2 in their legal framework

3.1 An overview on cryptocurrencies

The evolution of the means of payment is still ongoing, and nowadays crypto-assets represent a new form to execute payment transactions. Their use for this purpose is still new, but they are rapidly revolutionizing the financial landscape. Their creation was triggered by the climate of mistrust caused by the global financial crisis, and in 2009 arose Bitcoin. It represents the first virtual currency ever created, produced by Satoshi Nakamoto with the purpose of escaping existing regulation and the need of intermediaries. It was developed as an alternative to the conventional financial system, deemed untrustworthy. Its creator[130] believed that it was necessary an electronic payment mechanism based on cryptographic proof instead of trust, a peer-to-peer version of electronic cash[131] that needed no intermediaries for online payments. Indeed, decentralization is the key aspect and a peculiarity of blockchain, the technology breakthrough that enabled the utilization of the most renowned virtual currency by using a distributed, cryptographically secure, and crypto-economically incentivized consensus engine.[132]

According to MiCAR (Regulation of the European Parliament and of the Council on Markets in Crypto assets proposal), a crypto asset can be defined as "*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technolog*y". In particular, cryptocurrencies represent a type of crypto asset. They do not embody a legal currency, because the three essential functions for such classification are not fulfilled. Indeed, decentralized[133] virtual currencies' value fluctuates, depending on the law of demand

[130] *Or creators, the name Satoshi Nakamoto is a pseudonym, the identity is unknown*.

[131] Nakamoto S., Bitcoin: "A Peer-to-Peer Electronic Cash System", 2008, p. 1.

[132] Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology (July 19, 2016), p.2.

[133] Decentralized virtual currencies are not backed to another fiat currency, and do not have a central issuer, they represent the typology of virtual currencies mainly considered in this paper.

and supply, therefore it is not possible to declare them as 'unit of account', hence they cannot be expressed in a common unit. This also entails a lack of intrinsic value, which does not involve a 'store of value'. Eventually, there is debate regarding 'medium of exchange' role, they are used as means of payment, but their volatility might create adverse conditions. Additionally, they do not present legal tender (henceforth they are not recognized as 'fiat money') in any Member State, thus their acceptance is not mandatory. When these characteristics are satisfied, instead, currency represents something that can be measured (a representation of debts and credits) that results in social relations and creates bonds, thus trust. The confidence in such instrument is given by its legitimacy, enhanced by a legal background and the European Central Bank, which is in charge.

However, cryptocurrencies can circulate, be electronically traded and used as means of payment. The EBA addressed the interchangeability between the terms 'cryptocurrencies' and 'virtual currencies', and over the years the European legislation has provided several descriptions. The ECB mentioned them for the first time in 2012[134], identifying: "*a type of unregulated, digital money"*, followed by the IMF[135], the FATF[136] and other legal entities. Nevertheless, the first real description was provided in the AMLD4, where virtual currencies were depicted as *"a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*".

Nowadays, they represent a controversial subject that has become relevant,

[134] ECB: "A *virtual currency scheme",* 2012.

[135] "*cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value, issued by private developers and denominated in their own unit of account*". IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016.

[136] "*digital representations of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but do not have legal tender status (i.e., when tendered to a creditor, are a valid and legal offer of payment) in any jurisdictio*n", FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014.

especially from a regulatory point of view. From a behavioural finance perspective, it is possible to define some characteristics of this market, with particular focus on Bitcoin (given the existent literacy about). As stated by Barberis and Thaler (2003): “Behavioural finance argues that some financial phenomena can plausibly be understood using models in which some agents are not fully rational[137]”, thus there is no such thing as the so called “homo economicus”, people have to deal with irrationality. Indeed, they are victims of their cognitive biases[138].

Considering Bitcoin price, it has significantly fluctuated over the years and great influence is given by the news, noteworthy is the impact of the famous entrepreneur Elon Musk whose tweets in the recent months have had a huge impact in this market, both with positive and negative effects. According to the empirical analysis conducted by Barots (2015), Bitcoin price promptly reacts on public information, following the Efficient Market Hypothesis, furthermore “price is higher during days of positive events and lower during days of negative events than during other days without any events[139]”. Nevertheless, it is possible to define a major impact of investors’ sentiment that affects decisions. There are noise traders who are overconfident in the cryptocurrency market, so they will push up the price that will become too high. They are easily influenced by other people’s expectations and behaviour, also they might present the saliency bias, thus overestimate the likelihood that a salient event will occur again (for example, the rise in the virtual currency’s price). Given these reasons, it is possible to state that investment decisions are heavily affected by herding factors, which might denote higher risks.

Moreover, Bitcoin traders have an arbitrary behaviour that leads to an instable

[137] Nicholas Barberis, Richard Thaler: “A survey of behavioral finance” (September 2002)

[138] “*A cognitive bias is a subconscious error in thinking that leads you to misinterpret information from the world around you and affects the rationality and accuracy of decisions and judgments. Biases are unconscious and automatic processes designed to make decision-making quicker and more efficient. Cognitive biases can be caused by a number of different things, such as heuristics (mental shortcuts), social pressures, and emotions*”; From *https://www.simplypsychology.org/cognitive-bias.html*, ‘What is cognitive bias?’

[139] Jakub Bartos, 2015. "Does Bitcoin follow the hypothesis of efficient market?," International Journal of Economic Sciences, International Institute of Social and Economic Sciences, vol. 4(2), pages 10-23, June.

exchange rate[140], indeed volatility is one characteristic of cryptocurrencies since there is no central authority. Furthermore, it is used especially for speculative trading rather than as a medium of exchange and a new form of currency[141]. Such behaviour, affected by irrational exuberance and the "FOMO" or "Fear of Missing Out", that is the concern of not participating in the market when an event valorises the virtual asset[142], could lead to a bubble. Some people already define Bitcoin in this way, such as economists like Krugman, Shiller, Stiglitz, others instead think it is an opportunity "too good to be missed"; the only constant is the unpredictability and the uncertainty of this market.

It is crucial to state that other cryptocurrencies exist besides Bitcoin, nevertheless, with a market capitalization of 639 billion of euros[143], it remains the most remarkable one. The other ones are defined as "Altcoins", and there are two categories of them: the ones using the same open-source protocol as Bitcoin (for example Litecoin), and those that, instead, have their own protocol and DLT, as Ethereum. Actually, Etherum represents the platform introduced in 2015, which runs "smart contracts[144]", its cryptocurrency is known as Ether, which is the second one for market capitalization. Another example is Ripple, "a P2P decentralized digital payment platform that allows for near-instantaneous transfers of currency regardless of their form (e.g. US Dollar, Yen, Bitcoin)[145]", whose virtual currency is XRP.

3.1.1 The idea of blockchain as a trustless mechanism and "The Code"

Blockchain lies behind Bitcoin and the other digital currencies functioning, but it serves many purposes. It can be defined as a "distributed database of records, or public

[140] Alexander Keller, Michael Scolx:" Trading on Cryptocurrency Markets: Analyzing the Behavior of Trading on Cryptocurrency Markets: Analyzing the Behavior of Bitcoin Investors Bitcoin Investors" (2019), p.14.

[141] Brashar Almanasour, "Cryptocurrency Market: Behavioral Finance Perspective" (02/12/2020), pp. 159-166.

[142]Obryan Poyser Calderón, "Herding behavior in cryptocurrency markets" (November)

[143] https://www.coinbase.com/it/price, checked on 20.02.2022

[144] *"Smart contracts are "self-executing" contracts or applications that run exactly as programmed without any possibility of downtime".* European Parliament: "Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion", June 2018. Page 33.

[145] https://ripple.com/xrp/.

ledger of all transactions or digital events that have been executed and shared among participating parties[146]". Thus, data of transactions are recorded into blocks, linked nodes that once are verified through consensus method[147], and become part of the chain, it is not possible to alter (immutability characteristic). Moreover, blockchain guarantees anonymity, since participants use private keys as pseudonym, and also transparency, because all information are available. Whether it is a permissioned or a permissionless system[148], the DLT is widespread all over the world, both for financial and non-financial purposes.

What looks crucial in the dissemination of this decentralized technology, is the promise of change given by the absence of intermediaries, consequently economic transactions are not characterized by the prisoners' dilemma, where if trust is missing the trade does not take place[149]. Hence, blockchain does not require confidence in a counterparty and as highlighted in Bitcoin's white paper, the system for electronic transactions does not rely on trust[150]. There are some differences between trust and confidence. The former is about the relations among people and can be defined as the expectations of beneficial outcomes, pondering all the risks. The latter, instead, concerns relations between people and objects, is reason-based and relies on past performances[151]. They are connected and one depends on the other.

Blockchain is defined as a trustless system where confidence relies in the algorithm of the structure. Nonetheless, according to Nick Szabo, "There is no such thing as a fully trustless institution or technology"[152], only a part of vulnerability can be taken

[146] A. Stanciu, "Blockchain based distributed control system for Edge Computing," in 21st International Conference on Control Systems and ComputerScience Blockchain, 2017, pp. 667–671.

[147] *A mechanism based on the algorithm; in particular Bitcoin uses 'proof of work' where node participants confirm the work done in order to create new blocks in the chain.*

[148] *A permissionless system allows participation to everyone, instead a special permission is required in the permissioned one.*

[149] Vili Lehdonvirta, "The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy", Oxford Internet Institute, November 21, 2016.

[150] Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, p. 1.

[151] Ibid

[152] Nick Szabo, 'Money, Blockchains, and Social Scalability', Unenumerated, February 9, 2017.

away by innovation and it is not possible to anticipate the behaviour of all participants[153]. Regarding blockchain, there is no specification of what replaces trust, as a result this leads to an increase in confidence in order to permit transactions in the organization[154]. DLT systems present a multitude of economic players, they are socio-technological assemblages[155] where only few create, implement the code and have the authority to apply changes that affect the whole structure on which many other individuals rely on. Fundamental for people is to believe in the network they operate in, referring to blockchain system, it means that they need to have confidence in core players. This suggests that humans are always in the loop[156] and trust never really disappears.

Fundamental in order to foster and implement trust, is the law. Regulation is essential also in DLT system, to protect consumers, prevent illicit behaviours (such as the link between Silk Road[157] scandal and Bitcoin) and provide legal certainty. As stated in the European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)): *"the absence of flexible, but resilient and reliable, governance structures or indeed a definition of such structures, especially in some DLT applications such as Bitcoin, which creates uncertainty and consumer or – more broadly – user protection problems, especially in the event of challenges unforeseen by the original software designers".*

In this matter, regulators have to face a new body of law, Lex Cryptographia: "a set of rules administered through self-executing smart contracts and decentralized (and partially autonomous) organizations[158]". An early definition of smart contracts was provided by the scientist Nick Szabo in 1997, who described them as contractual clauses that can be embedded in the hardware and software, causing an expensive breach of

[153] Ibid, vulnerability as 'the need for or risk of trust in other people'

[154] Primavera De Filippi et al., "Blockchain as a confidence machine: The problem of trust & challenges of governance", . Technology in Society 62 (August) 2020, p.2.

[155] Ibid, p.7.

[156] Kevin Werbach, "Blockchain and the architecture of trust", 2018, p. 113.

[157] *Deep web market closed in 2014, where people made illegal purchases using Bitcoin*.

[158] Aron Wright, Primavera De Filippi, "Decentralized blockchain technology and the rise of Lex Cryptographia', 10 March 2015, p.25.

the contract[159]. Currently, there is not a single definition, but smart contracts can be described as an agreement whose execution is both automatable and enforceable[160]. Their first appearance does not coincide with the first time they were pronounced, they have existed long before[161], for instance, the vending machine is a representation since it self-executes an order and who inserts the coins participates in an exchange whit the seller[162]. In this way the contract is embedded in digital means[163], enhancing efficiency and does not require the intervention of a third party. Smart contracts exist also outside DLT, but its use increases efficiency.

Contractual law establishes obligations and rights of the parties involved in an agreement, as well as the liability in case of breach of the contract terms. Smart contracts, instead, cannot be violated because the code governing them is immutable[164] and this creates concerns with respect to customer protection. The challenge is transposing legal rules (wet code) into technical rules (dry code)[165], thus from an ambiguous language to a highly formalized one[166].

It is clear that with blockchain advent, law has to dialogue with a new set of rules represented by Code. *''The Code is law*" is a popular concept coined by Lawrence Lessig (1999), who highlighted the regulatory role that technology is assuming. Also, he defined a model composed by four constraints that regulate individuals' behaviour, which are considered as regulators: law, market, architecture, and norms[167]. These forces exist both in cyber and real world. In the former, code or software or architecture set outs the rules of the system, but they do not act totally on their own: in charge of the code

[159] Nick Szabo, Formalizing and Securing Relationships on Public Networks, 2 FIRST MONDAY (1997).
[160] Christopher D. Clack et al., Smart Contract Templates: Foundations, Design Landscape and Research Directions 2, Aug. 4, 2016, p.2.
[161] Max Raskin: 'The law and legality of smart contracts', 1 GEO. L. TECH. REV. 305 (2017).
[162] Supra note 158.
[163] Ibid.
[164] Primavera de Filippi et al, "Blockchain Technology as a regulatory technology", 2016.
[165] Supra note 157, p.25.
[166] Ibid, p. 11.
[167] Lessig Lawrence: "Code Version 2.0", pp. 123, 124.

there is its creator, the architect[168].

This is in accordance with the so-called "Vili's Paradox"; the professor Vili Lehdonvirta questioned the decentralization of blockchain, which functioning is based on Code. He highlighted the difference between enforcing and making the rules in an economic organization, for example, "laws are rules enforced by state bureaucracy and made by a legislature"[169]. Considering Bitcoin Protocol, rules are enforced by DLT, but there is somebody that has created them, and "who makes the rules matters at least as much as who enforces them, Bitcoin's error was to assume that technology alone could govern social interactions[170]". Thus, there is always someone responsible for the existence of the Code and, as stated before, the notion of trust never disappears, at the same time this also means that blockchain can be governed. "*Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services*[171]".

The European Union acknowledges the importance of legal certainty and a clear regulatory regime relating to blockchain-based applications[172], and aims to create a harmonised Fintech regulatory framework across member States. In this respect, in March 2018 the European Commission created the 'FinTech Action plan' that addresses the new challenges and how to tackle them. With the purpose of accelerating technological innovation, have also been created regulatory sandboxes where businesses, in a regulated environment, can test financial products or services, and the 'European Forum for Innovation Facilitators (EFIF)' which is a platform for supervisors to

[168] Ibid

[169] Vili Lehdonvirta, "The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy", Oxford Internet Institute, November 21, 2016.

[170] Ibid.

[171] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[172] European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain

meet and share ideas and experiences, to promote a further cooperation.

A step forward in virtual currencies' recognition was made by the Financial Action Task Force (FATF), which has been issuing several Guidance documents related to this topic for years, the most crucial ones are "Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014)" and "Guidance for a Risk-Based Approach to Virtual Currencies (2015)", which are continuously updated to include the new developments. In the latter document, the FATF[173] coined the term "Virtual Asset Service Providers" (VASPs), which identifies any legal or natural person conducting certain activities on behalf of another person, namely: "*Exchange between virtual assets and fiat currencies; Exchange between one or more forms of virtual assets; Transfer of virtual assets; and Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*". In this respect, a platform operating in decentralized finance (DeFi) shall not be comprised within this definition, unless is present someone retaining sufficient control power and influence in such environment. The recommendations highlighted in FATF's documents aim to provide jurisdictions with risks and regulatory compliances that virtual currencies arise, especially with a view of the Anti-money laundering directive.

3.2 Cryptocurrencies as a means of payment

The EBA, in August 2016, issued an opinion[174] where explicitly discouraged national authorities from buying, holding and selling virtual currencies. Nevertheless, according to the research conducted from Visa[175], the majority of the individuals interviewed asserted that the presence of financial institutions in the crypto-world would be fundamental for virtual currencies' expansion, especially if they were offered form credit institutions. The major interest of people in cryptocurrencies has changed

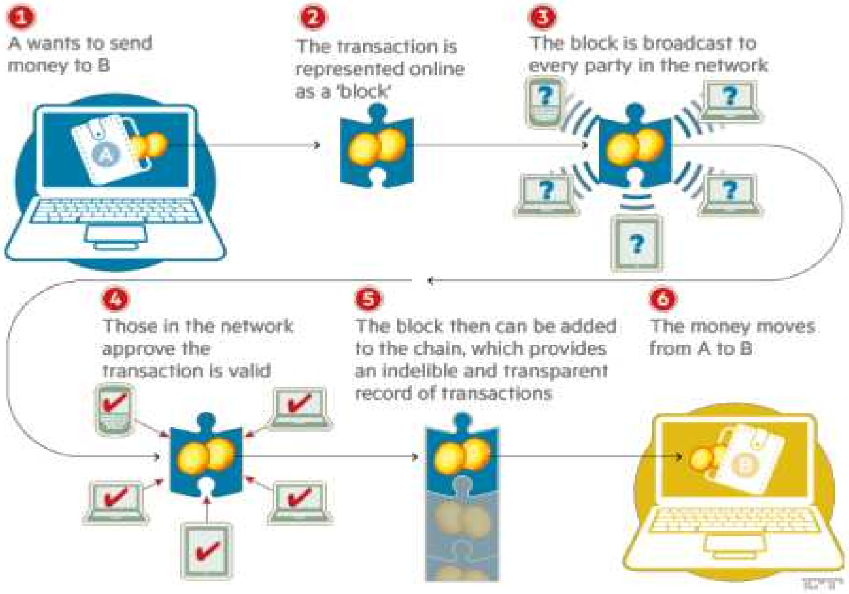
[173] Avaiable at: *http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html*

[174] EBA: "Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)", 11 August 2016.

[175] Visa: "The Crypto Phenomenon: Consumer Attitudes & Usage", 2021.

the legal authorities' perspective in such subject, thus their use is not dissuaded anymore, but several issues and warnings have been raised. Moreover, competent authorities have observed that financial institutions are interested in the practice of crypto-asset activities, hence they do not prohibit their holding or the provision of related services[176].

Image 4: Cryptocurrencies transactions using the blockchain


1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Source: "Technology: Banks seeks the key to blockchain", by J. Wild, M. Arnold and P. Stafford, 1 November 2015, Financial Times[177].

In peer-to-peer transactions can be identified the widest use of cryptocurrencies, in this case there is no master party involved as the exchange is directly performed between the parties in a dedicated platform, defined as "trading platform". In this situation, the individuals participating do not use private information, but two

[176] EBA: "*Report with advice for the European Commission*", 09 January 2019.

[177] Avaiable at https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?segid=0100320#axzz3qK4rCVQP.

cryptographic keys, a private one which defines a signature validating the user's identity, and a public one, visible from any participant in the network. The transaction is registered in the blockchain, and has to be validated by each node, in a process defined as "mining", in order to be performed. In this way, it is not possible to undo the exchange, the information registered are visible to all participants and cannot be altered, thus it is doubtful that a refund will be completed. In order to hold and transfer cryptocurrencies, it is essential to possess a wallet, where Bitcoin or Altcoin can be stored and exchanged, which can be online ("hot storage") or offline ("cold storage"). An example on how this transaction functions, is presented in *Image 4.* This exchange could be performed also for payment purposes, in this case the seller simply has to provide the buyer with the QR code or the e-mail address of its e-wallet, to which the cryptocurrency will be transferred.

Currently, cryptocurrencies are held mainly for investment and trading purposes, nonetheless, their usage as a means of payment is slightly becoming popular. Worth of mention is the European Justice Court sentence of 22 October 2015 (in the cause C-264/14 Skatteverket c/ David Hedqvist), where the ECJ stated that an exchange of Bitcoin for legal currency is exempted from VAT, and especially that "*the Bitcoin virtual currency is a direct means of payment between the operators that accept it*". Moreover, considering Visa's study[178] it is possible to identify "active owners" that represent the 21% of the global adult population, people who have used virtual currencies to perform exchanges, buy or sell goods/services. In particular, the majority of them has less than 35 years, thus the new generations might soon define a new pattern in payments. Also, according to the statistics[179], a great part of millennials sees in cryptocurrencies the future of payments and imagines a cashless society.

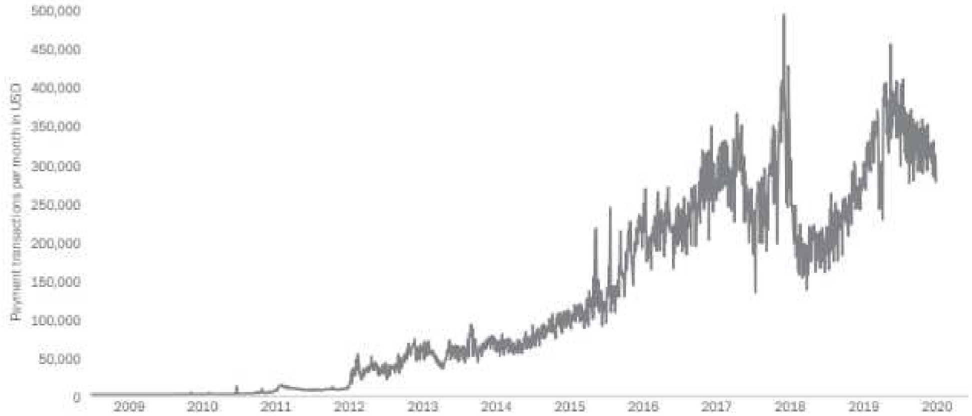
The Deutsche Bank research analyst Marion Laboure stated that Bitcoin is "not ready for mainstream use as a payments instrument", as its current usage to buy goods or services is not extremely widespread, owing to volatility, transaction costs and low

[178] Supra note 168.

[179] Deutsche Bank Research: "The future of payments: art III. Digital Currencies: the Ultimate Hard Power Tool #PositiveImpact", January 2020.

transaction speed. In particular, in the last three months of 2021, between 3% and 7% of clients holding Bitcoin performed payments using the cryptocurrency[180]. Of another opinion is the CEO of BitPay[181] Stephen Pair, who thinks that during the year 2022 things will change, as the interest in performing payments using cryptocurrencies is going to increase, especially for firms[182]. According to the "PYMNTS.com" research[183], the 50% of the companies considered is interested in cryptocurrencies' transactions, and there is a pressure for financial institutions to adapt platforms for virtual currencies' payments, in order to remain competitive.

Chart 3: Bitcoin payment transactions per month in USD



Source: blockchain.info. (Note: Number of daily confirmed Bitcoin transactions)

Although the use of cryptocurrencies for payment purposes is not prevalent, it exists and is rising, every day approximately from 250,000 to more than 1.5 million

[180] See: *https://www.marketwatch.com/story/bitcoin-as-a-universal-payment-method-this-deutsche-bank-chart-shows-one-big-thing-standing-in-the-way-11637075751.*

[181] A crypto payments processor.

[182] See: ht*tps://www.pymnts.com/accounts-payable/2022/xero-ap-automation-makes-big-difference-small-businesses-fight-fraud-unlock-efficiencies/.*

[183] PYMNTS.com: "The Cryptocurrency Payments Opportunity: Driving Crypto Adoption And Use Around The Globe", October 2021.

transactions using Bitcoin, Etherum and Litecoin are performed[184]. Such increase is shown in *Chart 3* which defines the pattern relating to Bitcoin. Specifically, cryptocurrencies function better as a means of payment when **"**the volume of transactions is larger relative to the individual transaction size[185]", namely in retail payments. Such transactions are appreciated from individuals as they are processed also during weekends, usually define lower transaction costs, and for merchants there is no risk that operations are relapsed, thus no risk of fraud. The perception is crucial in crypto's world, for example, if Tesla[186] decides to accept Bitcoin, the virtual currency will be consequently perceived as "a real thing with a real value[187]", because it would allow to get a good. Currently, some of the companies accepting payments performed using virtual assets are Microsoft, Expedia, Etsy, Airbnb is presently evaluating such option. Nevertheless, customers attracted to cryptocurrencies' payments, denote a little number of merchants offering such service.

3.2.1 Crypto payment gateways

Firms interested in accepting payments performed through virtual currencies can choose between two approaches: "hands-on" and "hands-off". In the former, the company decides to include cryptocurrencies in its accountability, nevertheless, how to register such entities is fairly complex. In the latter form, instead, cryptocurrencies are converted into fiat money before their transcription in the balance sheet, thus they remain off the books, and this outlines the preferred option. As previously stated, cryptocurrencies are decentralized and function through blockchain: there is no third party involved. However, when they are utilized as a means of payment, and specifically with a merchant, it is usual that transactions are performed by a third party, which arranges the exchanges between the buyer and the seller. In order to allow such payments, the merchant has to rely on a *crypto payment gateway*, which will coordinate

[184] See: *Visualizing the Rise of Cryptocurrency Transactions (visualcapitalist.com)*.

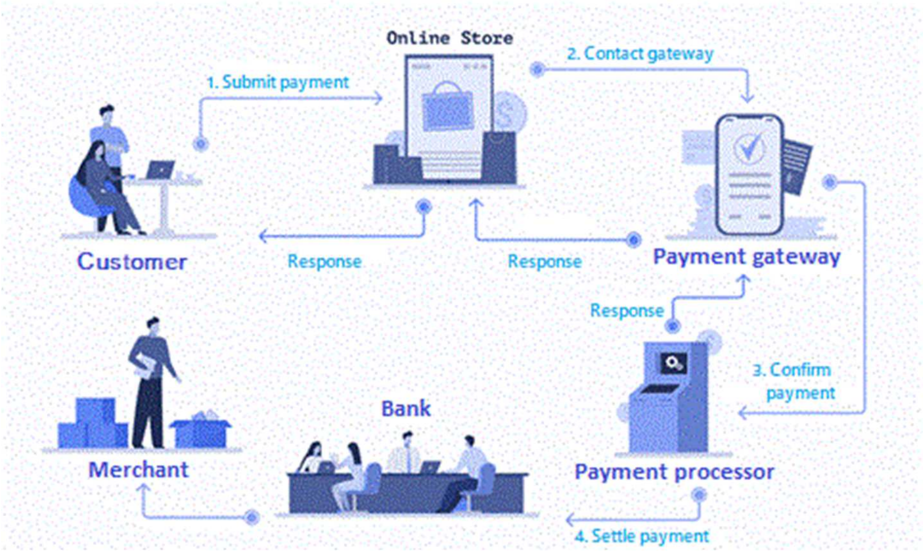
[185] Chiu Jonathan, Koeppl Thorsten V.: "The Economics of Cryptocurrencies – Bitcoin and Beyond", September 2018, page 34.

[186] Several announcements in this respect have been made from the CEO Elon Musk, with consequent effects in Bitcoin's price.

[187] Stated by Matthew Goldman, vice president of sales and partnerships for crypto card issuer *Apto Payments*, in October 2021.

the transactions on behalf of the business firm. In this case, the payment process does not significantly diverge with respect to the transactions performed using payment cards, illustrated in previous *Image 3.* Nevertheless, the major difference is that exchanges are executed through the blockchain using e-wallets, and not across the traditional channels of the payment system, explained in *Chapter 1;* how the process functions is exemplified in *Image 5.*

Image 5: The crypto payment process



Source: C#Corner: “Top 10 Payment Gateways For Cryptocurrency In 2021”, 28.06.21[188].

Exist several crypto payment gateways from which merchants can choose, the most renowned ones are Coinbase, BitPay, Coingate, and many others are currently emerging. The client simply places the order in the merchant’s website and decides to pay using the virtual currencies in his/her e-wallet, the information are promptly transmitted to the payment gateway and then to the payment processor; eventually, the payment gateway receives back the data and accepts the transaction for the

[188] Avaiable at: h*ttps://www.c-sharpcorner.com/article/top-10-payment-gateways-for-cryptocurrency-in-2021/.*

merchant, transferring the virtual assets from one account to the other. Such transactions are performed through blockchain, thus information are encrypted and secured with SSL[189], and the payment is processed on the chain, consequently, it will be validated and confirmed by each node.

Some platforms also offer the exchange from crypto to fiat money, and vice versa, thus function also as "crypto exchanges". In this case, they independently arrange the conversion, otherwise, if the payment gateway does not deliver such option, it has to rely on another service provider. In this instance, the cryptocurrencies are transferred from the customer's account to the payment gateway one, and they will be converted into fiat money by its crypto-exchange partner. Such funds will be then moved to its settlement account operating in the SEPA area, thus within a financial or payment institution, but they still belong to the merchant; therefore they will be credited to the payee's account through a SEPA bank transfer by the payment gateway, which will retain a percentage as a fee for the service.

Some individuals prefer converting cryptocurrencies into fiat money, in order to avoid a drastic change in their value due to volatility. It is feasible that the payment gateway, or the crypto exchange provider, supports the possibility to pay in a cryptocurrency different from the one initially chosen by the client (conceded that such Altcoin or Bitcoin is present in his/her wallet), in the instance that the virtual currency selected would define higher transaction costs with respect to the good's price. Thereby, this option might reduce the risk of walking out of the payment session.

3.3 Crypto payment gateways classification under the EU legal regime

In the European context there is not an explicit legal framework addressing crypto payment gateways' regulation. Analysing their functioning, they provide a payment service and, in this respect, they transfer the virtual currencies from the payer's crypto account to the payee one. Such a transaction seems representing an "acquiring

[189] Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client.

of payment transactions", which pursuant to article 4 (44) of the PSD2, is defined as *"a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee*". Thus, considering the assimilability between the definition just referred and the actions of the payment gateway, it appears that such entity is eligible to be under the scope of the Directive, with particular reference to its point 5 in Annex I[190]. Nevertheless, there is a clear reference to the term "funds" which does not encompasses crypto assets into its definition. Hence, cryptocurrencies are not in the field of application of the PSD2, since they are not banknotes, coins or e-money[191], consequently a legal tender.

The only crypto assets regulated under the PSD2 are those that fall within the definition of electronic money, and in this matter the EU refers to Directive 2009/110/EC (E-money Directive 2). As stated earlier in *Chapter 1*, electronic money are defined as "*electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic money issuer[192]*". In particular, this article provides an explicit reference to article 4 (5)[193] of PSD2, which specifically recalls the notion of funds. Thus, it is noticeable that decentralized cryptocurrencies are not comprised, also because they tend to not define a claim on the issuer, which is not certain, hence they cannot be considered e-money. Moreover, with reference to this matter, the EBA[194] provided some examples in which the EMD2's requirements are met from crypto assets, considering situations in which are involved the so-called stablecoins, namely virtual currencies that are usually pegged to a fiat currency. Consequently, such Report reiterates the inadmissibility of cryptocurrencies as Bitcoin into the definition of e-money.

[190] "Issuing of payment instruments and/or acquiring of payment transactions".

[191] Article 4 (25) PSD2.

[192] Article 2 (2) EMD2.

[193] *"payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee".*

[194] EBA: "Report with advice for the European Commission on crypto assets", 09.01.2019, p.12-14.

According to the ESMA's "Advice on Initial coin offerings and crypto-assets[195]", from a regulatory point of view, it is possible to qualify crypto assets as: e-money, financial instruments or none of the two categories. Thus, it also mentioned Directive 2014/65/EU (MIFID2[196]), which applies to financial instruments. Considering the list provided in Annex I, Section C (31) of MIFID2, it includes as well transferable securities, namely bonds, shares and similar instruments that are negotiable on the capital market[197]. In this respect, cryptocurrencies shall not be included. Nevertheless, as comes to light in the EBA questionary to NCAs[198], there are several definitions for the term 'negotiable' among countries, not just one widely accepted. Understanding whether a crypto asset can be defined as a financial instrument is a relevant issue. This task shall be carried out by jurisdictions, under national law. Considering Italy, for example, art. 1 of TUF does not include crypto-assets into the definition for financial instruments, and payment instruments (including cryptocurrencies) are not encompassed as well. However, CONSOB specified the existence of financial products: any form of investment financial in nature that requires a capital commitment, a revenue expectation, and some risk involved. In this view, crypto-assets can be financial products depending on the kind of offer to the public. This will be verified case-by-case, attesting that subsist the aforementioned requisites.

In order to understand what kind of rules crypto payment gateways abide to, in the following sub-paragraph are analysed the information provided on SpicePay website, which, according to several articles online, is one of the widest used platforms.

3.3.1 "SpicePay" payment gateway

SpicePay represents one of the several crypto payment gateways from which merchants can choose in order to allow for virtual currencies' payments in their websites. The headquarter of this platform is located in London, and it has been active in this market since the very first appearance of Bitcoin (2009), initially with different

[195] Of 09.01.2019.

[196] Markets in Financial Instruments Directive 2.

[197] ESMA, "Annex 1, Legal qualification of crypto-assets –survey to NCAs", January 2019. !!

[198] Ibid.

purposes than the current one. For almost five years it specifically functions as payment gateway to help merchants accepting cryptocurrencies[199]' payments, and, presently, it does not provide the exchange into fiat currency anymore. In its internet site, SpicePay provides clear information about its functioning and the terms to which clients agree when accepting its service.

First and foremost, the payment gateway frames itself as "storage of digital content and the provision of software services only", stressing that it does not represent a payment institution, thus, it is not compliant to PSD2 and EMD2. In order to use such service, the merchant has to register and create a merchant account. To accomplish that, he/she has to provide several information to confirm the identity, such as full name, cellular number and the name of the business. Nevertheless, SpicePay declares the possibility to process further data, as "account data[200]" for communication and service purposes, "ID data[201]" to assure the ownership of the account, thus, to prevent laundering, illicit and fraud activities, "transaction data[202]" referred to the operations taking place in the merchant account, and so on[203].

Moreover, is declared the possibility to deliver such information to external parties, for example to Google Analytics for market research reasons, lawyers in case of disputes, and third parties. In this last category, is included "WaveCrest Holding Limited", an e-money issuer[204], but also third-party websites that cannot be controlled by SpicePay and could potentially collect merchant's personal information. Regarding

[199] In particular: Bitcoin, Litecoin, Bitcoin Cash, Ethereum.

[200] full name, email address, username, country, telephone number, bank account, VAT number, PayPal account information, etc.

[201] ID data are full name, country, date of birth, document expiration date. It is processed also the company registration documents, which may contain the company's name and address, identification number, company type and company officer's full name and date of birth, etc.

[202] As timestamp, transaction amount, deposit address and transaction ID and other publicly available data from the bitcoin blockchain.

[203] Other information processed are: "communication data" (email address, username, IP address, full name, audio and video files and in the case of manual ID verification: photo of the user's personal ID, photo of the user, and photo of the user's bank statement/utility bill or related document), "notification data" (email address, phone number, username and full name), **"**merchant's customer data" **(**full name and an e-mail address).
Available at https://www.spicepay.com/privacy-policy/.

[204] Thus, under the scope of EMD2.

this, the platform encourages customers to be careful when using the website. Furthermore, it is explicitly asserted that the payment gateway stores and processes personal information "using third party servers located in data centres in the European Economic Area" applying all the needed security measures but, either way, such data are kept and transmitted to another entity.

It is clear that this platform, as several others, requires many data from its customers, some of which might be sensitive. Nonetheless, certain personal information of the merchant must be provided to SpicePay, as it has to comply with the rules laid out in the Anti-money laundering directive 5. Article 2 (1) (g) of the AMLD defines under the scope of the directive "*providers engaged in exchange services between virtual currencies and fiat currencies*", but this activity does not represent the one carried out from SpicePay, as it delivers a payment service and not an exchange one. In particular, payment gateways are not specifically named in this piece of law, where officially they might not represent "obliged entities". Nevertheless, recital 10 of the AMLD states that are under the scope of the directive "*all the potential uses of virtual currencies*".

Additionally, the platform considered (as the majority of this kind) supports customers with an online wallet, where virtual currencies are stored. Hence, it might be covered within the definition of "custodian wallet provider[205]", contained in the AMLD. It is important for this type of wallet provider to be controlled because it does not only display the public information of the users, but it retains both the public and private keys. Namely, data that can lead back to the owner's identity. In this regard, its functioning is similar to that of a bank account, as it preserves the client's cryptocurrencies. Likewise, the United Kingdom, home country of SpicePay, requires the compliance to the UK AML regime also for activities concerning the "exchange tokens[206]". Such conformity is indicated on the website of the considered platform,

[205] Article 2 (1) (h): *"an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies".*

[206] Often referred to as "cryptocurrencies" such as Bitcoin, Litecoin and equivalent. They utilise a DLT platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or investment. *See: https://www.globallegalinsights.com/practice-*

hence, it applies the Customer Due Diligence, namely the KYC rule, for which personal information of the merchant are essential to contrast illicit and fraudulent operations. Other rules[207] are followed as well.

SpicePay also declares to observe the General Data Protection Regulation (GDPR), assuring that data will not be retained longer than the necessary period to provide its service. In particular, if the customer has initiated crypto transactions and his/her request for the removal of the account has been granted, data are cancelled within five years since the erasure of the account; instead, if the client has performed no transactions, the information are deleted immediately. Nevertheless, the application of GDPR to blockchain denotes some obstacles. The assumption that data can be erased ("right to be forgotten"), thus with reference to articles 16 and 17, is difficult to achieve in a technology characterized by 'immutability', where once the information is stored, it cannot be eliminated; also, unilateral adjustment results burdensome. In this respect, the "data minimisation[208]" concept is challenging to recognize, as blockchains are built through a continuous addition of information to the chain.

The aforementioned characteristics of SpicePay, regulation included, pertain to the majority of crypto payment gateways. Thus, they are currently subject to the AMLD, the GDPR, and to the provisions of their home country. Nevertheless, at the European level there is not a precise legal framework addressing these entities, whose operations arise also the counter party risk: the payment gateway, before the transfer to the merchant's account, retain the cryptocurrencies in its own account; no real guarantees against its risk to default are offered, unless they are explicitly required from the merchant.

areas/blockchain-laws-and-regulations/united-kingdom.

[207] Namely, are indicated: Verifying customer identification using a multi-level system; filing reports as required by local regulations; responding to law enforcement requests; determining and obtaining necessary Licensing in countries of operation; compliance with local regulatory requirements; employee and Compliance Officer training; ongoing transaction monitoring.

[208] Article 5 (1) (c) of GDPR: data can be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".*

3.4 The application of the Payment Services Directive 2 to cryptocurrencies

The PSD2 applies to payment services provided across the Union[209], where transactions take place in the currency decided between the payer and the payee[210]. First of all, cryptocurrencies cannot be considered "currency", as they are not legal tender, they do not comprise the three[211] fundamental functions of money earlier explained. Moreover, as argued in the previous paragraph, the Directive clearly refers to "funds", hence it is evident that virtual currencies are not under the scope of PSD2. Nevertheless, it is possible to define a meeting point between the two of them: crypto payment gateways. As previously described, they perform an activity similar to the one fulfilled from payment institutions: they arrange the transaction between the payer and the payee, transferring the virtual currencies (funds in the case of PSD2) from one account to another, identifying the "acquiring" process. Thus, could payment gateways be included within the scope of the PSD2?

Apparently, it might seem valid to rely on the principle "same risk same rule" in order to apply the PSD2 to crypto payment gateways, as their functioning does not significantly differ compared to platforms involving funds. Nevertheless, virtual currencies have distinct peculiarities and denote different risks, in particular they are illiquid and volatile. Moreover, for what concerns crypto-assets, currently there is not a single definition widely accepted, there is no taxonomy which allows for the precise application of regulations. Moreover, according to Valkel[212] et al. (2015), it is not possible to include cryptocurrencies under the PSD2 scope, as they are comprised into the exceptions outlined in article 3 (k), especially they could qualify as instruments used in a "limited network", namely "*payment instruments that can be used only in a limited way".* This classification is plausible because virtual currencies have not yet been used as means of payment on large-scale, but define limited acceptance.

[209] Recital 33, PSD2.

[210] Article 59 (1).

[211] Store of value, medium of exchange and unit of account.

[212] Valcke, P. Vandezande, N. Van de Velde, N.: "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, p. 49 and 53.

Nonetheless, payment gateways enter in possession of the funds of the merchant, once the cryptocurrencies are converted, and then transfer them to his/her bank account. For this specific activity, they could be under the scope of the Directive. If they were, they would need a specific authorisation for the provision of the payment service, and thus comply with strict requirements in order to obtain it. Article 5 of the PSD2 precisely lists all the conditions, for instance, they shall have a minimum initial capital, a detailed business plan of the activity including budget forecasts, descriptions of the activities carried out, of the possible risks, and many others in order to protect data and assets of customers. Among other conditions, such authorisation shall be granted from the Member State only if the payment service provider had in place safe and sound governance arrangements, including *"a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective procedures to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures*[213]*"* Nevertheless, it is crucial the difference in crypto world: payments are not executed through the classical infrastructures, rather through the blockchain.

The establishment of such requirements in this decentralized technological environment is not straightforward. The payment gateway is 'in charge' of the transfer of virtual currencies, and could uphold to certain constraints, but it still relies on the blockchain functioning, which does not possess legal protection. Moreover, issues could be raised also regarding liability. Article 89 of the PSD2 argues that in case of "*non-execution, defective or late execution of payment transactions*" the PSP shall be retained liable and provide a refund. Nonetheless, in DLT there are several entities engaged in the transactions, in particular miners validating[214] them which could delay or fail the exchanges' confirmation; technically, such rule would be difficult to apply when dealing with blockchain. Also, should not be underestimated the impossibility to undue the transaction: once the transfer of cryptocurrencies is confirmed, it cannot be retrieved.

[213] Article 11 (4) PSD2.

[214] For instance, payment transactions performed using Bitcoin wallet, require six validations before being approved.

Another fundamental consideration when utilizing blockchain, regards the governing law to be applied. Merchants and crypto payment gateways shall be cautious in this respect, as the provision of the platform's service might necessitate further authorizations or requirements in the Country where it is performed.

At the European level, the issue of crypto payment gateways has not been tackled. Nonetheless, have been considered the challenges posed by crypto-assets activities, regarding customers protection and regulation. In 2016, the European Commission conducted an "Impact Assessment[215]" addressing the risks posed by suspicious transactions performed using virtual currencies. The outcome of this document is the identification of crypto activities that should be under the scope of the AMLD, and the decision to not include them within the PSD2, instead. Specifically, the application of the PSD2 to crypto exchange platforms is considered to be too troublesome for the exchanges, as well as for custodian wallet providers, because of the several requirements commanded by the Directive. Moreover, the Member States declared their scepticisms about the inclusion of virtual currencies into the scope of PSD2, as it would provide a distorted view on these entities, that could be perceived as safe when they are not[216]. Such decision to leave out cryptocurrencies from the Directive's field of application, was endorsed also by the EBA in its "Opinion on virtual currencies" (2014) and also in its "Report with advice for the European Commission on crypto-assets" (2019). In the latter document, in particular, the EBA emphasized that under the scope of PSD2 there are only crypto-assets considered as e-money; moreover, if a company uses DLT to outline a payment service, it is considered to be compliant with the Directive only if the crypto involved represents e-money, thus cryptocurrencies are not encompassed.

[215] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final. *https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.*

[216] European Parliament: "Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion", 07.2018, page 65.

3.4.1 Stablecoins

The virtual currencies considered so far are decentralized ones, thus their value is volatile because they are not backed by a fiat currency or commodity, also they are not issued by a central authority. Nonetheless, the focus has recently been transposed to another type of crypto-asset: stablecoins. They are quite different from Bitcoin and Altcoins, it is possible to define them as "digital units of value that are not a form of any specific currency, or basket thereof, and that rely on a set of stabilisation tools to minimise fluctuations of their price against such currency, or currencies[217]". Two broad categories of stablecoins can be identified: asset-linked and algorithm-based. The former group refers to stablecoins whose value is linked to a currency, commodity, financial instrument or crypto-asset, the latter, instead, utilizes algorithms for their value's stabilization[218]. In particular, asset-linked stablecoins[219] could be: "tokenised funds" (thus funds, as e-money, cash or deposits), "off-chain collateralised stablecoin" (assets held through an accountable entity, as commodities, securities) and "on-chain collateralised stablecoin" (held directly on the DLT). The two main classes are different under some circumstances[220], but the fundamental aspect is their value's attachment to another entity, which significantly reduces volatility.

The interest in this topic has been growing in these last years, nonetheless the first stablecoins can be dated back to the 2014 (for example Tether, BitShares). What has triggered such attention was the announcement of Facebook plan to create "Diem" (formerly Libra) its own stablecoin, in June 2019. This has drawn awareness on this topic from a regulatory point of view, especially for the "global stablecoins" (GSCs), which characterize the initiatives taken from large technological firms in this matter (just like

[217] ECB crypto-asset Task Force: "Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area" CB Occasional Paper Series No 247 / September 2020, page 7.

[218] FSI Insight on policy implementation No 33: "Fintech and payments: regulating digital payment services and e-money", 07.2021.

[219] Supra note 216, page 8.

[220] In particular, according to the FSI, asset-linked stablecoins are claim based (i.e. payment involves the transfer of ownership of a claim on value existing elsewhere from one party to another), instead algorithm-based stablecoins are object-based (i.e. payment involves the hand-over of an object which triggers immediate settlement as long as the parties deem the object to be valid).

Facebook). In particular, in June 2019 the G20 designated the FATFA to consider the AML/CFT risks in this environment and since then, many documents relating stablecoins have been issued, as the "G7 working group report on stablecoins" (2019) which addressed risks and peculiarities. Stablecoins denote less volatility than decentralized cryptocurrencies, and their current market capitalization does not pose particular risks for financial stability. Nonetheless, the interest in such subject has increased during the Coronavirus pandemic, and they are beginning to be referred as store of value and means of payment.

It is not clear the exact role stablecoins will take, currently the EU is making hypothesis about it[221]. Nevertheless, they are usually considered similar to the classical cryptocurrencies for what concerns their functioning. Indeed, they are mainly used for trading purposes[222], but can be employed as a means of payment too. They are used through the blockchain, but when considering payment purposes, the high transaction fees discourage their use in this respect. When contemplating tokenised funds[223], thus stablecoins collateralised by fiat money, they result under the oversight of the Eurosystem, and most of the time qualify as e-money, hence, they fall under the scope of the PSD2. This means that payment gateways offering the possibility to pay using this kind of stablecoins, must obtain a license and comply with all the requirements laid down in the PSD2, although the use of blockchain makes it difficult to uphold certain requests. Despite the resemblance of these stablecoins to cash, they cannot guarantee the anonymity of the payer, and they cannot represent a public good as they pertain to private entities.

A massive use of stablecoins could undermine the financial stability, as big techs

[221] The ECB identified three scenarios for stablecoins' implication: as "crypto-asset accessory function", "new payment method" and "alternative store of value". From ECB: "Occasional Paper Series Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area" September 2020.

[222] In September 2021 around 75% of all trading on crypto trading platforms involved a stablecoin. *https://www.ecb.europa.eu/pub/financialstability/fsr/focus/2021/html/ecb.fsrbox202111_04~45293c08fc.en.html.*

[223] The ones with the higher market capitalization, worth more than $78 billion. Available at https://coinmarketcap.com/tokens/ (last access on 27/01/2022).

could use them as a comparative advantage by controlling payment infrastructures and exploiting people's personal data. It is also true that Facebook's Diem has encountered several regulatory constraints for its existence, which forced the firm to change the GSC name and characteristics, getting to the point that the whole project might be closed[224]. Nonetheless, it represents only the first GSC development. In this respect, banks are starting to create their own stablecoin, namely "Central Bank Digital Currency" (CBDC), as the ECB "digital euro". It would be a "form of sovereign money provided by the ECB in electronic format", thus a "complement of cash". It is fundamentally different form cryptocurrencies, stablecoins included, as it has the sovereignty of the ECB, and the same characteristics of the euro in the form of banknotes and coins, with the advantage of being used electronically. Nonetheless, its online usage represents a challenge that will be faced, as the EU has already started the digital euro project.

[224] https://www.investopedia.com/meta-diem-project-reportedly-shutting-down-5217204

CHAPTER IV: Regulatory evidence for cryptocurrencies in the EU

4.1 The digital financial package

*"*The future of finance is digital" is the opening of the 'Digital Finance Package' published by the European Commission on 24 September 2020. The EU acknowledges the main role of technology in the financial landscape, and intends to promote it in a regulated environment. The programme has four main goals: "promoting data-driven finance, addressing the challenges and the risks in the digital world and improving the resilience of the system, removing the fragmentation in the digital market, and guaranteeing the digital innovation under the EU regulatory framework"[225]. An important objective is also the creation of a level playing field in crypto-asset regulation across the European Union, according to the principle 'same risk same rule', so activities with similar risk should be subject to similar regulation and supervision. The strategy is composed by: the Regulation on "Digital Operational Resilience" (DORA), which relates to ICT[226] and the associated risks; the "Retail Payment Strategy" that aims to ensure consistent safeguards to customers, avoiding risks for participants in the retail payment system, and promotes instant payments, emending also existing European directives, such as the PSD2; "The Pilot Regime" intends to facilitate DLT experimentation for securities and markets, also involving a regulatory sandbox; eventually, the "Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA)", regulates the crypto-asset landscape, introducing the first classification of tokens and new rules for their issuance.

4.1.1 The "Retail Payment Strategy" and the review of the PSD2

The retail payment environment is extremely affected by technology, and innovations are continuous and fast. As a result, nowadays exist several ways to perform payments, as explained in *Chapter 1,* they are less visible and progressively dematerialized. In particular, what matters is the provision of tailored, fast, and easy

[225] Dirk Zietsche et al., "The Markets in Crypto-Assets regulation (MICA) and the EU Digital Finance Strategy", paper number 2020-018, 06/11/2020.

[226] Information and Communications Technology.

mechanisms to customers. This landscape, which saw also the intrusion of cryptocurrencies (stablecoins included), results fragmented, especially across national boards, despite the improvements defined by the SEPA. Hence, the Strategy aims to outline a clear governance framework in this matter, establishing its basis on four pillars[227]: improving digital and instant payment options, creating retail payment markets that are innovative and competitive, defining sound and efficient retail payment systems, ensuring efficient international payments (also remittances). In this context, the Strategy recalls the importance of having strong rights and obligations also for Payment Service Providers, which now have several ways to compete across the Union, thanks to the new developments.

Thus, the EC calls for a review of the PSD2. The Directive has introduced new providers, the TPPs, that have innovated the payments landscape, and enhanced the security in this field because of the SCA. Nonetheless, it has also posed several challenges for its application, due to the existence of many APIs and the unreadiness of markets, for example. The Strategy intends to assess whether additional procedures for frauds identification are necessary, and to balance the risks with suitability when considering contactless payments, for which also the existing €50 limit will be evaluated. In order to further harmonise the environment of PSPs, the EC intends to analyse the similarities and differences between the PSD2 and the EMD, because a distinct authorisation for payment institutions and e-money ones, does not seem always appropriate anymore, different supervision regimes included. A single framework might be more suitable. Furthermore, it is necessary to revise some services that are exempted from the PSD2. Some unregulated activities shall be under the scope of the Directive, if justified, in particular "technical services ancillary to the provision of regulated payment or e-money services[228]". The Commission will also "evaluate the need for changes in prudential, operational and consumer protection requirements[229]".

[227] EC: "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Retail Payments Strategy for the EU", Brussels, 24.9.2020 COM(2020) 592 final.

[228] Ibid.

[229] Ibid.

Eventually, the EBA shall provide a report to the Commission by 30 June 2022, to identify the revisions applicable to the PSD2. The amendments that will be made to the PSD2 only regard the improvement of the existing articles of the Directive, to ensure a more efficient payments landscape that accounts for the new technologies. No drastic changes are envisaged. In particular, the inclusion of crypto-assets (other than stablecoins linked to fiat currency that are e-money) within the scope of the PSD2 is not considered, they are intended to be still left out. Nonetheless, the 'Digital Financial Package' addresses them in another piece of law, the MiCAR.

4.1.2 The MiCAR Proposal

The MiCA regulation proposal represents a crucial step towards harmonisation, there is not a specific date for its implementation, but the EC is confident it will happen within four years. It provides the first definition for crypto-asset[230], and in article 3 outlines three categories of tokens: utility tokens, asset-referenced tokens, and e-money tokens. The first group refers to crypto-assets that provide digital access to a good or a service, they are placed in the market by an issuer and the holder is not entitled to a financial return[231]. The second type of tokens maintain their value stable by linking to several currencies that have legal tender, or commodities, or crypto-assets[232]. The last class is used as means of payment and retains a stable value by referring to one fiat currency[233]. Art. 2, comma 2 of the regulation, specifies that in its scope are included all crypto-assets that do not fall under the legislation of existing laws, hence are left out: electronic money (Directive 2009/110/EC), structured deposits (Directive 2014/65/EU), securitisations (Regulation 2017/2402/EU), deposits (Directive 2014/49/EU), and financial instruments (Directive 2014/65/EU).

Would be exempted from MiCA regulation also the so-called security tokens (or investment tokens). We refer to STOs (Security Tokens Offerings) which represent an offer of financial instruments representing traditional asset classes, as stocks, bonds, or

[230] *See Paragraph 3.1 "An overview on cryptocurrencies", page 47.*
[231] Art 3 (5) MiCAR.
[232] Art 3 (3) MiCAR.
[233] Art 3 (4) MiCAR.

also crypto-assets. They are incorporated into a smart contract e digitalized through a token, using DLT. STOs represent an evolved form of ICOs (Initial Coin Offering), a process used to create new cryptocurrencies or as an alternative way to raise funds. It is similar to an IPO (Initial public Offering), implemented by a company that wishes to become public, but in the former case, investors receive tokens representing a stake in an external asset or enterprise. On 13 November 2017, ESMA issued a statement addressing the rapid growth of ICOs and indicating that they may fall outside of the scope of the existing rules and hence outside of the regulated space[234], differently from STOs.

The 'Markets in Crypto-assets regulation' introduces important rules for crypto-assets issuers[235] and/or service providers[236] (CASPs). First of all, they must be a legal entity. In particular, they have to comply with strict requirements with regard to asset-referenced tokens and significant asset-referenced tokens, presented in Title III and IV. For instance, the former group must receive authorization by the competent authority of home Member State to perform its tasks and the latter is under the supervision of EBA. Title II of the Proposal establishes the obligations for issuers of crypto-asset (other than asset-referenced token) to draft a white paper containing all relevant information, for an issue of transparency, which must be notified to authorities 20 days prior its publication. Title V outlines several conditions for CASPs, first and foremost they need authorization from national supervisory authority, moreover they have to abide by rules concerning the initial capital reserve, governance model, security of the infrastructure, and further obligations related to investors protection. MiCAR outlines what crypto-asset service means, namely article 3 (9) indicates:

"a) the custody and administration of crypto-assets on behalf of third parties;

b) the operation of a trading platform for crypto-assets;

c) the exchange of crypto-assets for fiat currency that is legal tender;

[234] "ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements", (13 November 2017), ESMA 50-157-828.

[235] Article 3 (6) MiCAR: *"legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-assets*".

[236] Article 3 (8) MiCAR: "*any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis".*

d) the exchange of crypto-assets for other crypto-assets;

e) the execution of orders for crypto-assets on behalf of third parties;

f) placing of crypto-assets;

g) the reception and transmission of orders for crypto-assets on behalf of third parties

h) providing advice on crypto-assets."

This piece of law does not pronounce the term crypto payment gateway, nonetheless its service as custodian wallet provider could be found in the point a) of the article 3 (9), as it indicates "*safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys*[237]". In this case, there should be a contractual relation with customers[238]. Moreover, Recital 56 states that if the CASP has to retain the funds of the client, such funds (as defined by PSD2) shall be transferred to a credit institution or central bank, and this is what happens when the payment gateway holds in its account the converted money that will be then relocated to the transaction's payer one.

Although, focusing on the token definitions provided by the regulation, it is not easy to establish where virtual currencies like Bitcoin, would fit. According to the Swiss Financial Market Supervisory Authority, that with farsightedness had classified tokens already in 2018, they are included among payment tokens, since cryptocurrencies are accepted as means of payment. But, in MiCA regulation subsists the specification of "stable value by referencing only one fiat currency", which is a strong constraint. Decentralized cryptocurrencies do not meet such requirement, they are volatile. However, they are not explicitly excluded or considered illegal in the proposal, but due to their nature they cannot comply with some requirements laid down. In particular, the concern dwells in the denotation of "legal person", a characteristic implausible to be met for them. There are not indications about decentralized entities, as virtual currencies and crypto payment gateways, which still falls outside the scope of the existing regulation. Moreover, according to a survey[239] conducted by 'The International

[237] Article 3(10) MiCAR.

[238] Recital 59 MiCAR.

[239] "Blockchain ecosystem's response to MICA Regulation Proposal" Survey & Stakeholders'

Association for Trusted Blockchain Applications' (INATBA), in February 2020, asking whether "MiCA sufficiently facilitates certain emerging crypto sub-industries, such as decentralised finance (DeFi)", most of the people (49%) provided a negative response. Also, INATBA warned that under MiCAR emergent markets like DeFi "would likely no longer be accessible to Europe and her citizens", representing an issue in terms of competition and protection.

4.2 The regulatory framework in some countries

4.2.1 Italy

The PSD2 officially entered into force in Italy on 13 January 2018, with the legislative decree number 218 of the 15 December 2017. Since the implementation date until the end of the year 2020, in Italy four e-money institutions and three payment institutions have been authorized to perform PIS and AIS services, and two payments institutions exclusively AIS service. The authorized Italian banks can perform the activities required by the PSD2 without the need of further requests. Nevertheless, the monitoring from the Bank of Italy[240] shows a limited use of the Open Banking services, in terms of the clients involved and transactions performed, despite a discreet number of TPPs (equal to 103 performing at least an activity on an open banking platform, in the second semester of 2020). The AIS service is the widest used one, however there is a relative high number of transactions that were not successful (10.5% of the total, in the second semester of 2020), designating the whole process as in an experimental stage.

Differently from the provisions of the European directive, the Italian operators provide diversified business models. The PIS services are not only used to provide online payments for merchants, but also for consumers and business customer's needs, as to recharge prepaid cards or to pay commercial invoices. Also, AIS service has a broader usage, for instance to establish timetables or as support for credit scoring. Nonetheless,

Engagement Sessions, available at https://inatba.org/wp-content/uploads/2021/03/2021-02-Blockchain-Ecosystems-Response-to-MiCA-Regulation-Proposal-Final.pdf

[240] Banca d'Italia: "PSD2 e open banking: nuovi modelli di business e rischi emergenti" November 2021.

the strategies put in place from banks, once finalized the compliance phase, still regard the standard services of TPPs, but they are trying to compete with non-banking providers.

There are also several risks identified, In particular the cyber one, because of the increase in the *attack surface*, given by the presence of many actors involved in the payment transactions (TPPs, banks, operators providing online accounts, four parts are merchants who are not under the perimeter of supervision). The ASPSPs tend to apply online “passive gateways”, meaning platforms that do not pertain to the ASPSP, and are used to link their services with the TPPs which usually use “active gateways”. There is a high degree of interconnectedness between the parties involved, and is sufficient the damage of only one part in the ‘chain’ to compromise safety, it is possible that information are retained from unauthorized subjects, the service is made unavailable and that there is a ‘single point of failure’ individuated form an attacker. Nonetheless, the risks involved are the same present in any ICT system, namely the risks of data violation, falsification, systems’ malfunctioning and so on. Poses numerous risks also the existence of multiple authentication keys which have to be correctly handled, as the widespread APIs, which necessitate an adequate use of best practices for their software development.

In January 2021, Italy defined an authentication rate (inherent to the SCA through the 3DS) equal to 42.3%, positioning itself as the last country in the EU, data that improved during March of the same year, when it was 51.1%, but still quite low[241]. There might be some reasons because of this tardiness, as the failure to be authenticated from the responsible subject (the Access Control Server) which counts for the 60% of failed authentications, the abandonment of the process from the customer (14.3%) or the missing of the 3DS2 protocols from the card used (28.4%). Thus, there is a clear slowdown in the implementation of the PSD2 services.

Focusing once again on crypto payment gateways, there is not a specific mention

[241] Avaiable at *https://www.axerve.com/approfondimenti/insight/autenticazione-forte-sca-pagamenti-online.*

in the country's regulation, and as explained in the previous chapter, they are not under the PSD2 scope. Nevertheless, Italy has recently defined a decree law to regulate the activities of the operators involving cryptocurrencies, introducing for the first time a specific regulation in this matter. The Country does not have an explicit definition for virtual currencies, nonetheless, for Anti Money laundering purposes, the Legislative Decree n.90 of 2017 pronounced a description which depicts them as: a digital representation of value which is not issued by a central bank or public authority, which not necessarily is attached to a legal tender, but is used as a means of exchange to purchase goods or services for investment purposes, that can be transferred, stored, or electronically negotiated.

The new regulatory regime identified in the decree, envisages monitoring and data transmission of crypto and e-money trade companies. The objective is the census of these operators, that will have to sign up on a specific section of the register of the competent system (the "Organismo degli agenti e mediatori"), an indispensable condition to perform their activity. Moreover, they will have to provide quarterly several information to the OAM, namely: the data of their clients, the total number and turnover in euros of the crypto, the number of operations related to conversion, the number of exchange operations, and so on. Not only Italian entities will have to comply with this framework, but also foreign crypto operators providing services in Italy, which represent the 98% in this market, otherwise their website will be blocked and they will not be able to carry out any activity. Such constrictions have been contested, as they seem too much restrictive from market operators.

Further information will be collected once the full text will be available, but currently, this regulatory structure is said to be applied to crypto exchanges and wallet providers. Nonetheless, even if not specifically mentioned, crypto payment gateways could be under its scope, as they tend to also deliver the wallet function, whose information regarding the operations performed will have to be communicated.

4.2.2 Malta

The Country regulates payment services in the "Financial Institutions Act" (chapter

376 of the laws of Malta), and the PSD2 provisions have been transposed into the regulatory framework in 2019. The existing credit institutions do not need a further authorization to perform the services indicated in the Directive, nonetheless, the use of open banking is restricted because of the relatively small presence of TPPs in Malta.

Considering Fintech, Malta represents one of the most advanced countries in its regulation. The Malta Financial Service Authority (MFSA) was the first one to issue a regulation on crypto-assets, in 2018. It defined three important acts: Malta Digital Innovation Authority (MDIA) Act, Innovative Technology Arrangements and Services (ITAS) Act and Virtual Financials Assets (VFA) Act. The first one is dedicated to the supervision of DLT platforms and smart contracts. The ITAS act defines the procedure for any technology wishing to be registered, and thus certificated by the approval of System Auditors. The last represents the functioning of the financial instrument test, which defines whether a crypto-asset falls under the European Union legislation. The VFA test classifies tokens in four possible categories, that are: financial instruments, electronic money, virtual token, and virtual financial asset. Moreover, it provides protection to investors and users of cryptocurrencies. Malta has also defined a 'Fintech strategy' which is based on six pillars and includes a public regulatory sandbox.

The VFA defines the need of a license for crypto platforms. In particular, it individuates four classes: class one relates to operators offering crypto investment advice; class two refers to P2P transactions and wallet providers; class three is for those wanting to operate in OTC markets; class four is about crypto exchanges. Considering the last class, service operators "can operate a VFA exchange, hold or control clients' money, VFA and private cryptographic keys". There is not a clear indication about crypto payment gateways, nonetheless, in a broader sense they could fall under the fourth class. In this case, they would follow the rules of Chapter 3 of the VFA Rulebook, which lays out the conditions for the authorization of all classes.

First of all, the MFSA must be contacted in writing, and if satisfied with the information received, issues an "in principle approval" which is valid for three months, during which the crypto operator shall comply with all the necessary conditions, that if are fulfilled, the license is granted. Successively, the "license holder" shall maintain a correct behaviour[242], otherwise the permission can be withdrawn. For instance, he/she shall document all the activities, maintain internal control, reporting and communication, and so on. At the same time, risks shall be monitored and safety ensured. Moreover, resilient and effective systems shall be put in place, able to provide services even under circumstances of market stress.

In this respect, the MFSA has authorized in 2021 a decentralized platform to carry out activities involving virtual currencies. Such entity is "Everest", and represents the first decentralized platform in the world performing crypto activities to be licensed, thus regulated. It is allowed to hold clients' assets and money, to execute orders on behalf of other individuals and to provide wallet custody. Nonetheless, it is not identified as crypto payment gateway, and is registered under Class 2, as it provides P2P transactions and wallet service.

4.2.3 Switzerland

Switzerland is one of the most innovative countries within the European continent. The Open Banking approach has provided positive results, the Country uses an 'industry-driven' mode, expecting that the market will regulate itself thanks to competition and collaboration. Financial institutions do not need further authorizations

[242] According to R3-3.1.2.1.3 of Virtual financial assets rulebook, Chapter 3: Virtual financial assets rules for VFA service providers, *the Licence Holder shall:*
i.establish, implement and maintain decision-making procedures and an organisational structure which clearly and in a documented manner specifies reporting lines and allocates functions and responsibilities;
ii. ensure that its relevant persons are aware of the procedures which must be followed for the proper discharge of their responsibilities;
iii. establish, implement and maintain adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the Licence Holder;
iv. employ personnel with the skills, knowledge and expertise necessary for the discharge of responsibilities allocated to them;
v. establish, implement and maintain effective internal reporting and communication of information at all relevant levels of the Licence Holder;
vi. maintain adequate and orderly records of its business and internal organisation; and
vii. ensure that the performance of multiple functions by its relevant persons does not, and is not likely to, prevent those persons from discharging any particular function soundly, honestly and professionally.

to perform these services, nonetheless, many of them apply a passive behaviour towards open banking; for what concerns TPPs, there are several ones operating in the country, coherently with the high digital evolution of Switzerland.

Indeed, it is highly innovative. It is the house of 'Crypto Valley' in Zug, an ecosystem of blockchain innovation, and has a favourable crypto-asset regulation framework. On June 2014, FINMA (Swiss Financial Market Supervisory Authority) addressed the topic of virtual currency providing a sort of definition, in this way preceding the European Union by several years. Cryptocurrencies are under the scope of Switzerland's AML law since 2016, and do not represent a legal tender. Since last year, the Canton of Zug should even accept Bitcoin and Ether for tax payments, representing the first canton to allow it. In 2018, FINMA published a guideline that applies to existing legislation for ICOs, and with farsightedness separated tokens in three definitions: payment tokens (used as mean of payment), utility tokens (provide digital access to services/goods) and asset tokens (represent an asset). In 2020 the parliament approved the 'Blockchain Act' which will enhance Switzerland's Fintech landscape. Nonetheless, despite the advanced technology consideration in Switzerland, there is not an existing framework for crypto payments, which are allowed within the country.

4.2.4 Estonia

Estonia has always been at the fore-front for what concerns innovation, in particular in the financial sector. Already in 1996, the Country had online banking, and the majority of transactions is currently performed digitally, thus the PSD2 results rightly implemented, and it is possible to individuate eight ASPSPs and seven TPPs. At the same time, the Country represents an important place for Fintechs, especially for crypto companies. Since 2017 it regulates virtual currencies service providers, and currently it is possible to identify four hundred licensed companies. Such term individuated wallet service and virtual currency exchange service providers, regulated under the AML Act.

Nonetheless, Estonia intends to make a change and include within the definition of virtual currencies service providers also: "*virtual currency transfer service, which enables at least partially electronic transaction through a virtual currency service* *provider on behalf of the originator for the purpose of transferring the virtual currency through the virtual currency service provider to the recipient's virtual currency wallet or account, regardless of whether the originator and recipient are the same person or the recipient uses the same service provider".* New requirements will be introduced as well, for instance VASPs will have to: identify customers, not provide anonymous wallets, have an initial capital at least equal to 350.000 Euros, at least one member of the board shall have a university degree and two years of experience in the sector, and comply with all the previous rules[243].

[243] *i) the own resources of a virtual currency service provider shall at all times correspond to one of the following amounts, whichever is greater: the amount of share capital or at least a quarter of the fixed overheads of the previous financial year;*
ii) state fee for the application is EUR 10,000;
iii) the registered office, seat, and place of business of the virtual currency service provider must be in Estonia;
iv)it should be possible at any time to ensure that a representative of the supervisory or investigative body has access to the data collected and stored by the service provider;
v) if the licensed virtual currency service provider wishes to operate abroad, including establishing a branch abroad or providing cross-border services abroad, the virtual currency service provider shall submit an application and relevant documents to the FIU. The FIU will then decide whether to approve the application or not within one month from the receipt of the required documents. The decision shall be made based on, among other things, the applicant's financial state, organizational structure, and business plan;
vi) the contact person may not be the contact person or the head of a structural unit of another virtual currency service provider;
vii) a member of the management board may work as a contact person or as the head of a corresponding structural unit only in those virtual currency service providers where he or she is a member of the management board;
vii) a person that may acquire, hold and increase a qualifying holding shall have an impeccable business reputation, strong financial position, ability to ensure that the service provider is able to comply with the own funds and asset management requirements, absence of reasonable doubt that the acquisition is related to money laundering or terrorist financing and absence of international sanctions.;

All requirements available at: *https://www.sorainen.com/publications/update-for-virtual-currency-service-providers/*

Conclusion

The payments landscape has drastically changed during the last decades, becoming increasingly digitalized. The technology that represents the new normality in the financial world corresponds to FinTech, a phenomenon that is affecting the whole sector. Despite the recent interest in such topic, it has been existing for decades. It is possible to recognise three distinct waves in its history: *FinTech 1.0* is identified with the invention of the telegraph that has triggered the financial globalization, *FinTech 2.0* represents a period during which transactions began to be performed online, thanks to the dissemination of the World Wide Web. Eventually, *FinTech 3.0* denotes what we know today and what has really gained attention from people. It was caused by the global financial crisis in 2008, and has dramatically transformed the financial sector introducing the 'data economy', a reality where also non-financial entities can operate alongside banks and enter in possession of individuals' data.

Within this context, the way of performing retail payments is becoming more and more innovative. Nowadays, cash still represents the most common way to discharge obligations, nonetheless, people preferences are shifting towards faster, easier and tailored services. According to the SPACE research of the ECB (2019), individuals tend to favour non-cash payments, especially cards, and are starting to utilize electronic money, choices also driven by the Covid-19 outbreak. E-money transactions are the most innovative ones, within this field are included P2P transactions and the e-wallets, which could be internet-based as PayPal, or device-based wallets which utilize the NFC technology or the QR code. During the 2019, 22% of the payment transactions in the EU were performed using mobile phones, and as a result, the existence of physical cards is dwindling. In this perspective, it is possible to identify third parties arranging the payment transactions performed via internet, through the use of online platforms.

Under this framework, the EU shall guarantee a sound regulatory environment to ensure financial stability and a safe payment system. For such purposes, in 2007 the European Parliament and the Council created the Directive 2007/64/EC, defined as "Payment Services Directive" (PSD), in order to provide a level playing field for payments within the European Union. Such Directive introduced several rules for the payment services, announcing also *"payment institutions"*, term identifying entities processing the online payments' communication with the banks. Nevertheless, this piece of law has proven not sufficiently far-sighted, as it did not mention FinTech and the situation remained fragmented, arising risks. Consequently, the Directive was repealed by Directive (EU) 2015/2366, the so-called Payment Services Directive 2 since 13 January 2018.

The PSD2 intends to harmonise the payments landscape within the EU, with the provision of new services to customers, ensuring safety and the technological innovation. As mentioned earlier, it lists the payment services[244] that are under scope of the Directive in the Annex section, with reference to its article 4 (3). The majority of them was already included in the PSD, but there are two new typologies: Payment initiation services and Account information services, whose providers represent the so-called Third-Party Payment service Providers (TPPs); moreover, the PSD2 introduced the new term *"Account servicing payment service provider"* (ASPSP), which identifies the classic payment service provider, that supports and maintains a payment account for a payer[245]. It is fundamental to regulate payment service providers, as they arrange the transactions on behalf of the payee and the payer, entering into possession of their data, without being the actual party paying or receiving the exchange. Nonetheless, they

[244] *1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.*
2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.
3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: (a) execution of direct debits, including one-off direct debits; (b) execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders.
4. Execution of payment transactions where the funds are covered by a credit line for a payment service user: (a) execution of direct debits, including one-off direct debits; (b) execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders.
5. Issuing of payment instruments and/or acquiring of payment transactions.
6. Money remittance.
7. Payment initiation services.
8. Account information services

[245] Article 4 (17) PSD2.

cannot, in any case, collect funds from the public, which represents a prerogative of licensed banks.

The regulation requires payment service providers to obtain an authorization in order to carry out their activities, for which they have to comply to several constraints. For instance, they shall retain a minimum initial capital, provide detailed description of the activities performed and the risks involved, have in place sound and prudent management. Once the license is granted, the PSP is signed up in the Member State's register. In order to ensure transparency, the Directive entrusts the EBA with the development and the management of a public register of all the PSPs, available on its website, containing all the relevant information.

The PSD2 underlines the link with banks, affirming that payment institutions shall be able to access to the bank's account in order to carry out their activities, and such access shall be guaranteed in the payment system too. Nonetheless, the crucial innovation that the Directive has introduced is the 'Open banking'. The term identifies the possibility for PSPs to have access to the information of the parties involved in the transaction, thanks to the provision XS2A. Thus, using the Application Programming Interfaces (API) the PSP is able to connect to the ASPSPs. In particular, considering the TPPs, the PISP creates a bridge between the merchant's website and the online banking platform, gathering the information needed to initiate the payment. The AIS, instead, delivers a general view of the financial status of the individual. Such services are available only if the payment account is held online, and in any case, the TPP cannot hold sensitive information.

Focusing the attention on the payment transactions performed online, it is possible to identify the 'four-party model'. Despite the name, there are actually six parts involved: the customer, the acquirer, the issuer, the merchant account (or provider), the payment processor and the payment gateway. The customer simply starts the online transaction in order to buy a good or a service, promptly the information are transferred to the payment gateway, which decides whether to authorize such exchange. Consequently, it communicates with the payment processor which connects with the issuing bank to determine if there are sufficient funds available; eventually, all the information are sent back to the payment gateway which provides a response to the merchant, transferring the funds to his/her account. Such interactions with the bank are made possible by the XS2A, and in order to obtain the data needed, the PSP shall possess the authorization under the PSD2.

The processing of several data related to clients by PSPs, might involve risks. Thus, it is mandatory the application of the Strong Customer Authentication, which validates the identity of the user performing the payment, and it is based on two or more elements pertaining to the individual, namely knowledge, possession and inherence. Moreover, in order to enhance safety, the PSD2 is to be applied in accordance with other legal frameworks. In particular, the AMLD which aims to contrast illicit and fraudulently behaviour, and requires the application of the KYC rule in order to identify who is performing the activity. Eventually, also the GDPR is fundamental, especially for sensitive information, as it requires the process of data only if the PSP is able to demonstrate that their use is strictly necessary for the provision of the service.

The PSD2 represents a fundamental piece of law for payments, accounting for innovation in a constantly evolving field, as it is intended to be technological neutral in its definitions. Because of its significance and the major changes that it introduces, its implementation required further time, hence the compliance deadline was moved from 14 September 2019 to 30 December 2020. In particular, the application of the SCA and the API have been quite challenging. On September 2021, there were approximately three hundred TPPs within the EEA, and an estimated number of transactions equal to 500 million monthly. Nonetheless, the situation within the EU is fragmentized, for instance in Estonia the conformity to the new legal framework has not created issues, and it has been sufficiently prompt. In Italy, instead, the application is going slow, and the situation appears to be at an early stage.

Despite the consideration of FinTech in the new regulations, technology continues to change the financial environment and to introduce new entities. Such transformations also affect the payments landscape, which is now characterized by new instruments and systems. Currently, people possess a major interest towards cryptocurrencies, the phenomenon that has radically altered the financial world. Their first appearance is to be dated back to the global financial crisis, with the creation of Bitcoin with the purpose of escaping current regulation. As many other altcoins, it represents a virtual currency that is not legal tender, as it is not a 'store of value' or a 'unit of account', possibly it could represent only a 'medium of exchange'. It is based on blockchain, a decentralized technology that has attracted many people for its presentation as a 'trustless system'. However, trust and confidence are always central, participants in the blockchain create relations and put their faith on the person that is in charge of the 'Code'. There is no such thing as 'In code we trust' because its existence depends on someone, thus it is not merely high-tech.

This new technology permits the functioning of Bitcoin, the cryptocurrency par excellence, and other crypto-assets. The widespread use of the most renowned virtual currency represents a concern due to traders' behaviour, especially the uninformed ones. In this respect, regulation is key to diminish uncertainty and provide confidence to consumers, and also to reduce the risk of this market to become a 'bubble'. Nonetheless, during the years have been issued by the ESAs only warnings about possible risks involved for cryptocurrencies, as the ESMA advice in 2019. The first time that such phenomenon was provided with a definition happened with the creation of the AMLD4, where virtual currencies are depicted as "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".*

These entities are mainly used for investment purposes, nevertheless they are starting to be utilized also as a means of payment. The P2P transactions designate the most common usage of virtual currencies in this field; thus they are simply transferred from one e-wallet to another. However, regardless of the claim of decentralization, payments are also performed by third parties, namely crypto payment gateways, which allow merchants to accept cryptocurrencies. In this case, once the transaction is validated through the blockchain nodes, the virtual currencies are transferred from the client's e-wallet to the merchant's one. Possibly, they are converted into fiat money that are relocated via a bank transfer to the merchant's bank account. Such exchange is immediate, fast and easy to accomplish. Indeed, an increasing number of individuals, and companies, is becoming interested in such activity, especially young people who might determine a new pattern for payments in the future.

The whole payment exchange has a similar functioning to the one where the legal currency is involved. In fact, there is a payment gateway representing a third party that arranges the transaction, transferring the amount from the payer to the payee. Thus, it is possible to identify in crypto payment gateways the meeting point between the PSD2 and virtual currencies. Since they perform activities similar to the PSPs, namely the acquiring one, does it mean that they are under the scope of the directive and qualify as payment institutions?

First and foremost it is important to underline that such entity in not explicitly present in any regulation or directive of the EU. Nonetheless, since they perform activities related to virtual assets, they result to be regulated under the AMLD, thus crypto payment gateways have to apply the KYC rule in order to identify who is performing the transaction, to contrast illicit activities. Moreover, since personal data are involved, they are compliant also to the GDPR. Nonetheless, the application of such regulation to the blockchain is not straightforward, as the assumption that data can be erased ("right to be forgotten") is difficult to achieve in a technology characterized by 'immutability'. Once the information is registered in the chain it cannot be eliminated, hence the "data minimisation" concept is challenging to recognize, as blockchain is built through a continuous addition of information.

Focusing on the PSD2, within its filed of application crypto assets, and consequently cryptocurrencies, are not included unless they represent e-money[246], and

[246] Hence, they are "*electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic*

thus are regulated under the Directive 2009/110/EC (E-money Directive 2). In such category might fall also the so-called stablecoins, if they are backed to a currency representing legal tender, and qualify as e-money. Moreover, the Directive specifically mentions the transfer of 'funds', term which does not encompasses virtual assets that do not represent coins, e-money or scriptural money, hence cryptocurrencies. The fact that these entities are not considered to be regulated under this Directive is clear, but it is crucial to consider the fact that the crypto payment gateways do not only transfer cryptocurrencies, but also funds once they are converted. In this situation, they clearly perform a payment service activity, and could be classified as PISPs, as they arrange the payment transaction on behalf of the payer, and serve as a bridge between the merchant and his/her bank account.

Nonetheless, such activity is not sufficient to declare them under the scope of the PSD2. Crypto payment gateways' nature is decentralized and their functioning is based on blockchain. The establishment of certain requirements of the Directive would be challenging, as the definition of a sound structure where all the responsibilities are well defined and transparent. In DLT such conditions could not be met, as the identity of the people involved along the chain is unknown. Moreover, also liability could represent a challenge, as in DLT there are several entities engaged in the transactions, in particular miners validating them through the nodes, which could delay or fail the exchanges' confirmation. Hence, the responsibility in case of non-execution or delay in the process, cannot be totally attributed to the crypto payment gateway.

Moreover, the purpose of their functioning is the transfer of cryptocurrencies, and not funds. Crypto payment gateways themselves declare that they are not compliant to PSD2[247], because their primary asset is to be identified in virtual currencies. Despite their evident non-inclusion in such framework, would it be worthwhile to regulate them under the Payment Services Directive 2?

Undoubtedly crypto payment gateways need to be supervised and regulated, it

money issuer".

[247] As Spicepay on its website.

is crucial to provide consumers protection and trust in this market, given the many potential risks. In particular, they do not only handle virtual currencies, but also funds, when they are transferred to the merchant's account. Nonetheless, the PSD2 does not represent the most suitable legal framework. The crypto payment gateway could abide to certain requirements, but some of them might be too stringent and challenging to be respected, because of the reliance on blockchain. It is real that DLTs do not depend on merely 'trustless' systems, because many people are involved, and someone is always in charge of their creation. But the biggest issue is defining who the creator is and how to make him/her comply with the rules.

The conformity to the AMLD and to the GDPR is not sufficient, because if these entities gain major attention and begin to be utilized frequently, they could undermine financial stability. Thus, a specific piece of law addressing the risks and the opportunities of crypto payment gateways might be the best choice. It is also important that regulation does not banish this innovation. It is fundamental that a thriving activity such as cryptocurrencies remains legal, otherwise the European Union would lose competition and transactions. The financial landscape is constantly evolving and technology represents the main impetus. Thus, it shall not be hindered, rather monitored.

Noted that the PSD2 does not represent the best legal framework for crypto payment gateways, we might wonder which one is the most suitable. Currently, there is not a specific regulation addressing them, such topic does not seem to be explicitly tackled. Some countries have defined the obligation for crypto providers to abide to certain rules and to be registered, as Malta, others are starting to require the same conditions, as Italy and Estonia. This indicates that regulation is starting to consider crypto-assets. In this field, on September 2020 the EU designed the 'Digital Financial Package', a programme that aims to account for technology in retail payments, representing a major breakthrough.

It also envisages a revision of the PSD2, in order to remain at the forefront of the new innovations. However, the scope of the Directive is intended to remain the same, cryptocurrencies will continue to be left out. Nevertheless, the MiCAR proposal for the first time will deliver a taxonomy for crypto assets, and create a level playing field in their legislation within the Member States. It individuates CASPs, which will be monitored and will have to comply with several rules. Within their definition crypto payment gateways could be included as well. However, what it looks like is that such piece of law has been designed, in particular, for the 'threat' posed by Facebook project of the stablecoin 'Diem'. Indeed, there are strict rules for asset-referenced tokens issuers. But what about decentralized virtual currencies?

They are not mentioned in the regulation, and do not fit any of the tokens' descriptions. Although, MiCAR intends to cover all crypto-assets that are not already under the scope of EU legislation, so they should be included as well. But decentralization makes it difficult to comply with the requirements defined. Should decentralized cryptocurrencies be considered illegal? It is not clear what their role is, in MiCAR perspective. Because of these reasons, crypto payment gateways relating only to virtual currencies as Bitcoin, do not seem to be under the MiCAR scope. The greatest contributions in this matter, so far, are given by the AML directives. In particular AMLD VI has defined the responsibility of cybercrime, also considering cryptocurrencies likewise Bitcoin. Nevertheless, they are not exhaustive and do not circle the phenomena fully.

The PSD2 is fundamental in the payments landscape, it has enabled a new form to perform transactions, accounting for the technology evolution. Its compliance is not fully satisfied yet in some countries within the EU, but its significance is undeniable. Moreover, the legislator intends to make adjustments in order to enhance its regulatory framework. Despite its consideration of FinTech, it does not account for the newest technology, namely crypto payment gateways, whose main instruments are cryptocurrencies. Nonetheless, the inclusion of such entities in its field of application would be detrimental in terms of competition and innovation.

The issue is that it does not exist a specific legal framework for crypto payment gateways. The only piece of law that seem to be suitable is MiCAR, but decentralized cryptocurrencies remain a great unknown in this context, thus it does not appear to be applicable. What is recognizable is the constantly tardiness of the European legislator for what concerns technological innovation. Markets are in continuous evolution, and their regulation would not only provide safety, but also permit to harness their added value and enhance their potential. The EU has not provided a prompt response in terms of Fintech regulation, although in the last years it has started to address the new phenomenon. How regulators can intervene to provide trust, safety and, at the same time, guarantee the development of innovation represents a major challenge. However, it needs to be tackled in order to ensure the financial stability.

Bibliography

AMLC: "*The Second European Payment Services Directive (PSD2) and the Risks of Fraud and Money Laundering*", October 2017.
https://www.amlc.eu/wp-content/uploads/2019/04/The-PSD2-and-the-Risks-of-Fraud-and-Money-Laundering.pdf

Anja Simic, '*What Is SWIFT and How Does It Work*?', Deel., 12.08.2021
https://www.letsdeel.com/blog/what-is-swift

Annunziata Filippo, '*Towards an EU Legislation for crypto-assets: reflections on the MiCAR Proposal'* Seminar, 11 March 2021, Venice.

Arner, Douglas W. and Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., '*The Evolution of Fintech: A New Post-Crisis Paradigm?*' (October 1, 2015). University of Hong Kong Faculty of Law Research Paper No. 2015/047, UNSW Law Research Paper No. 2016-62.
Available at SSRN: https://ssrn.com/abstract=2676553

Arner, Douglas W. and Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., '*FinTech, RegTech and the Reconceptualization of Financial Regulation'* (October 1, 2016). Northwestern Journal of International Law & Business, Forthcoming, University of Hong Kong Faculty of Law Research Paper No. 2016/035.
Available at SSRN: https://ssrn.com/abstract=2847806

Axepta BNP Paribas: '*E wallet: che cos'è e come funziona il portafoglio elettronico',* 29.04.19
https://www.axepta.it/e-wallet-che-cose-e-come-funziona/

Banca d'Italia: '*Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems); TARGET2 Il sistema europeo per il regolamento dei pagamenti di*

importo rilevante' 07.2021.
https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2021-009/index.html

Banca d'Italia: '*PSD2 e open banking: nuovi modelli di business e rischi emergenti'* 11.2021.
https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/2021-PSD2-Open-Banking.pdf?pk_campaign=EmailAlertBdi&pk_kwd=it

BEUC: *'CRYPTO-ASSETS: BEUC response to the Commission's consultation'* 13.05.2020
http://www.beuc.eu/publications/beuc-x-2020-037_crypto_asset_position_paper.pdf

Capgemini: '*World payment report 2021'*, 07.10.2021
https://www.capgemini.com/it-it/news/world-payments-report-2021/

Carbone Fabio: '*L'anagrafe delle criptovalute e delle valute digitali sbarca in Italia'*, 03.02.2022, Yahoo!finanza.
https://it.finance.yahoo.com/notizie/l-anagrafe-delle-criptovalute-e-082116585.html

Chawla Hermit: '*The Benefits of Crypto Payment Gateway Development'*, 06.01.2022, The World financial review.
https://worldfinancialreview.com/the-benefits-of-crypto-payment-gateway-development-2/

Chiu Jonathan, Koeppl Thorsten V.: '*The Economics of Cryptocurrencies – Bitcoin and Beyond'*, September 2018.
https://www.bis.org/events/eopix_1810/chiu_paper.pdf

Christopher D. Clack et al., *'Smart Contract Templates: Foundations, Design Landscape and Research Directions 2*' (Aug. 4, 2016).
https://www.researchgate.net/deref/http%3A%2F%2Farxiv.org%2Fabs%2F1608.00771

Cong, Lin and Li, Xi and Tang, Ke and Yang, Yang, '*Crypto Wash Trading*' (December 20, 2019).
Available at SSRN: *https://ssrn.com/abstract=3530220*

Consob: C. Schena, A. Tanda, C. Arlotta, G. Potenza, *'Lo sviluppo del FinTech: Opportunità e rischi per l'industria finanziaria nell'era digitale'*, Quaderni FinTech, 03.2018.
https://www.consob.it/documents/46180/46181/FinTech_1.pdf/35712ee6-1ae5-4fbc-b4ca-e45b7bf80963

Dalaiti Francesco, '*Cripto-valute e abusivismo finanziario: cripto-analogia o interpretazione estensiva?'*, in Sistema Penale, 1/2021, p. 5ss.
https://www.sistemapenale.it/it/fascicoli/fascicolo-mensile-1-2020

Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, '*Disrupting Governance: The New Institutional Economics of Distributed Ledger Technolog*y' (July 19, 2016).
Available at SSRN: *https://ssrn.com/abstract=2811995*

De Filippi, Primavera, Morshed Mannan, and Wessel Reijers. (2020) *'Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance'*. Technology in Society 62 (August): 101284.
https://doi.org/10.1016/j.techsoc.2020.101284

Deloitte: '*Payments Service Directive 2 (PSD2) Il nostro approccio'*, 2016.
https://www2.deloitte.com/content/dam/Deloitte/it/Documents/technology/B_Payment%20Service%20Directive-new.pdf

Deloitte: '*Open banking e API: la banca del futuro'*, 2019.
https://www2.deloitte.com/it/it/pages/financial-services/events/open-banking-ed-api-economy--la-banca-del-futuro---deloitte-ital.html

Deloitte: *'The rise of using cryptocurrency in business, considering the benefits of crypto'* 2021 *https://www2.deloitte.com/us/en/pages/audit/articles/corporates-using-crypto.html*

Deutsche Bank: ‘*PSD2, open banking and the value of personal data’* 28.06.18 *https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000471102/PSD_2%2C_open_banking_and_the_value_of_personal_data.PDF*

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32007L0064*

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance). *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110*

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036*

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance). *http://data.europa.eu/eli/dir/2018/843/oj*

Dublino Jennifer: ‘*Payment gateway vs payment processor’* 06.08.2021, business.com. *https://www.business.com/articles/payment-gateway-vs-payment-processor/*

Earle, T.C. (2009), '*Trust, Confidence, and the 2008 Global Financial Crisis*'. Risk Analysis, 29: 785-792.
https://doi.org/10.1111/j.1539-6924.2009.01230.x

EBA: '*Final report: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)'* EBA/RTS/2017/02, 23.02.2017
http://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

EBA: '*The EBA's Fintech roadmap conclusions from the consultation on the EBA's approach to financial technology (FinTech)*', 15.03.2018
https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/79d2cbc6-ce28-482a-9291-34cfba8e0c02/EBA%20FinTech%20Roadmap.pdf

EBA: *'Opinion of the EBA on the implementation of the RTS on SCA and CSC'* EBA-Op-2018-04, Paragraph 13.
https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

EBA: "*Report with advice for the European Commission on crypto assets",* 09.01.2019
https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

EBA: '*EBA report on the future AML/CFT framework in the EU',* EBA/REP/2020/25, 2020
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/931093/EBA%20Report%20on%20the%20future%20of%20AML%20CFT%20framework%20in%20the%20EU.pdf

EBA: '*Report on the use of digital platforms in the EU banking and payments sector',* EBA/REP/2021/26.09.2021
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publicati

ons/Reports/2021/1019865/EBA%20Digital%20platforms%20report%20-%20210921.pdf

EC: '*Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments',* Brussels, 27.11.2017
https://europa.eu/rapid/press-release_MEMO-17-4961_en.htm

EC: *'Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion'* 07.2018.
https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

EC: *'Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions on a Retail Payments Strategy for the EU*', Brussels, COM(2020) 592 final, 24.9.2020.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0592

EC: 'Legal and regulatory framework for blockchain' 13.04.2021.
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain.

ECB: '*The payment system'* 2010.
https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf

ECB: "*Virtual currency schemes – a further analysis*", February 2015.
https://www.ecb.europa.eu

ECB: '*Eurosystem oversight policy framework Revised version'*, 07.2016
https://www.ecb.europa.eu/pub/pdf/other/eurosystemoversightpolicyframework201607.en.pdf

ECB: '*Payments statistics: 2020'*, 23.04.2020 *https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2020~5d0ea9dfa5.en.html*

ECB: *'Occasional Paper Series Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area'* 09.2020
https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf

ECB: '*Study on the payment attitudes of consumers in the euro area (SPACE)'* 12.2020.
https://www.ecb.europa.eu/stats/ecb_surveys/space/html/index.en.html

ECRI: *'The Business Models and Economics of Peer-to-Peer Lending'*, N.17, 05.2016.
https://blog.osservatori.net/it_it/fintech-significato#open-banking

EDPB: *'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects'* 16.10.2019
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

EDPB: *'Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR Versione 2.0'* 15.12.2020
https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_it.pdf

ESMA: '*ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements'*, 13.11.2017, ESMA 50-157-828.
https://www.esma.europa.eu

ESMA, '*Annex 1, Legal qualification of crypto-assets –survey to NCAs'*, January 2019.
https://www.esma.europa.eu/document/annex-legal-qualification-crypto-assets-%E2%80%93-survey-ncas

FATF: ‘*Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’*, FATF, Paris, 2021
www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.htm

Filippi, P. D., & Hassan, S. (2016). ‘*Blockchain technology as a regulatory technology: From code is law to law is code*’. First Monday, 21(12).
https://doi.org/10.5210/fm.v21i12.7113

FSI : ‘*Fintech and payments: regulating digital payment services and e-money’*, Insight on policy implementation No 33, 07.2021.
https://www.bis.org/fsi/publ/insights33.pdf

Gauci Ian, Abela Grech Cherise, ‘*Fintech Malta’*, 11.2021.
https://www.gtgadvocates.com/2point3/wp-content/uploads/2021/04/024_MALTA.pdf?fbclid=IwAR0AM_Vf3AaEf3xbobSRh3ZG_nqbEArDH95xTjvUKbkILxQyKSrcwCpGg3A

Hamukuaya, Hashali, ‘*The Development of Cryptocurrencies as a Payment Method in South Africa’* (June 17, 2021). Hamukuaya. (2021). The Development of Cryptocurrencies as a Payment Method in South Africa. Potchefstroom Electronic Law Journal, 24, 1 - 23. *Available at SSRN:* https://ssrn.com/abstract=3875264

IMF: Tanai Khiaonarong, Terry Goh, *‘Fintech and Payments Regulation: Analytical Framework’,* WP/20/75, 29.05.2020.
https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020075-print-pdf.ashx

Jakub Bartos, 2015. ‘*Does Bitcoin follow the hypothesis of efficient market?’* International Journal of Economic Sciences, International Institute of Social and Economic Sciences, vol. 4(2), pages 10-23, June.
https://ideas.repec.org/a/sek/jijoes/v4y2015i2p10-23.html

Kaleigh Moore: ‘*Payment Gateways: Keeping Your Ecommerce Transactions Safe + Customers Happy’*, 2020, Bigcommerce.
https://www.bigcommerce.com/blog/payment-gateways/#what-is-a-paymentgateway

Keller Alexander, Scolx Michael: ‘Trading on Cryptocurrency Markets: Analyzing the Behavior of Trading on Cryptocurrency Markets: Analyzing the Behavior of Bitcoin Investors Bitcoin Investors’ (2019).
https://www.researchgate.net/publication/341679301_Trading_on_Cryptocurrency_Markets_Analyzing_the_Behavior_of_Bitcoin_Investors

Kollmeyer Barbara: ‘*Bitcoin as a universal payment method? This Deutsche Bank chart shows one big thing standing in the way*’ 16.11.2021, MarketWatch
https://www.marketwatch.com/story/bitcoin-as-a-universal-payment-method-this-deutsche-bank-chart-shows-one-big-thing-standing-in-the-way-11637075751

Lael Brainard, 2017. "*Where Do Banks Fit in the Fintech Stack? : a speech at the Northwestern Kellogg Public-Private Interface Conference on* \"New Developments in Consumer Finance: Research & Practice\", April 28," Speech 950, Board of Governors of the Federal Reserve System (U.S.).

La Repubblica: *‘Criptovalute, per gli operatori in Italia obbligo di registrazione e di trasmissione dei dati dei clienti’*, 03.02.2022
https://www.repubblica.it/economia/2022/02/03/news/criptovalute_mef-336286731/

Lessig Lawrence: “*Code Version 2.0*”, New York, Basic Books (2006).
Mersch Yves, *‘TIPS and the future of innovative retail payment solutions in Europe’*, speech 30.11.2018
https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181130.en.html

McInnes Scott: *‘Interchange Fee Regulation (IFR) and PSD2 - Two important judgments* *from the Court of Justice of the European Union (CJEU*)', 02.2018, Bird&Bird. *https://www.twobirds.com/en/news/articles/2018/global/interchange-fee-regulation-and-psd2-important-judgments-from-the-european-court-of-justice#5*

MFSA: *'Virtual financial assets rulebook, Chapter 3: Virtual financial assets rules for VFA service providers'*, 25.02,2019
https://www.mfsa.mt/wp-content/uploads/2019/03/VFAR_Chapter3_Updated.pdf

Morganti Margaux, '*FinTech and its regulatory challenges – Malta's approach'* Seminar, 19 February 2021, Venice.

Nabilou, Hossein, '*The Dark Side of Licensing Cryptocurrency Exchanges as Payment Institutions'* (March 3, 2019). Law and Financial Markets Review (2019), 14(1), 39-47.
Available at SSRN: *https://ssrn.com/abstract=3346035*

Nakamoto S., '*Bitcoin: A Peer-to-Peer Electronic Cash System'*, (2008).
https://bitcoin.org/it/documento-bitcoin

Navaretti Giorgio Barba, Calzolari Giacomo, Franco Pozzolo Alberto: '*FinTech and Banks: Friends or Foes?*' ISSN 2421-6917, 02.2017
https://european-economy.eu/wp-content/uploads/2018/01/EE_2.2017-2.pdf

NCR: *'Payment Gateway vs Payment Processor: Everything you need to know'* 20.05.2021
https://www.ncr.com/blogs/payments/payment-gateway-vs-payment-processor

Noble, Elisabeth, *'Crypto-Assets: Overcoming Challenges to Scaling - An EU Approach'* 14.10.2020.
Available at SSRN: *https://ssrn.com/abstract=3748343*

Open Banking Europe, PRETA S.A.S.: '*Third party provider user management for PSD2 Access to Account (XS2A)'*, 2017.

https://www.openbankingeurope.eu/media/1176/preta-obe-mg-001-002-psd2-xs2a-tpp-user-management-guide.pdf

Pavithra R: *'Everest receives VFA license to provide regulated DeFi globally'* 06.2021, Ibisi intelligence.
https://ibsintelligence.com/ibsi-news/everest-receives-vfa-license-to-provide-regulated-defi-globally/

PYMNTS.com: "*The Cryptocurrency Payments Opportunity: Driving Crypto Adoption And Use Around The Globe*", October 2021.
https://www.pymnts.com/tracker/the-cryptocurrency-payments-opportunity-digital-payments-virtual-currencies/

Prasad Yadav, Miklesh and Arora, Madhu, '*Study on Impact on Customer Satisfaction for E-Wallet Using Path Analysis Model'* (April 10, 2019). International Journal of Information Systems & Management Science, Vol. 2, No. 1, 2019.
Available at SSRN: *https://ssrn.com/abstract=3369651*

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on *Markets in Crypto-assets*, and amending Directive (EU) 2019/1937.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Raskin, Max, *'The Law and Legality of Smart Contracts'* (September 22, 2016). 1 Georgetown Law Technology Review 304 (2017).
Available at SSRN: https://ssrn.com/abstract=2959166

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
http://data.europa.eu/eli/reg/2014/910/oj

Rui Zhang, Rui Xue, and Ling Liu. 2019. *'Security and Privacy on Blockchain'*. ACM

Comput. Surv.1, 1, Article 1(January 2019),35pages.
https://doi.org/10.1145/3316481

Szabo, N. (1997). *'Formalizing and Securing Relationships on Public Networks'*. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Szabo Nick, '*Money, Blockchains, and Social Scalability'*, Unenumerated, February 9, 2017.
http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

VALCKE, Peggy, , VANDEZANDE, Niels, , VAN DE VELDE, Nathan, '*The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4'*, SWIFT Institute Working Paper, 2015/001, [Florence School of Regulation].
Retrieved from Cadmus, European University Institute Research Repository, at: *http://hdl.handle.net/1814/39423*

Vili Lehdonvirta, '*The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy*', Oxford Internet Institute, November 21, 2016. *https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/*

VISA: '*Open Banking in Switzerland Part I'* 09.2021
https://mastercardcontentexchange.com/news/media/wxwih35b/2mc20299_mc_ch_whitepaper_part_1_en_vf_31-9.pdf

Werbach Kevin: "*The Blockchain and the new architecture of trust*", Cambridge (MA), MIT Press (2018).

Wright, Aaron and De Filippi, Primavera, '*Decentralized Blockchain Technology and the Rise of Lex Cryptographia'* (March 10, 2015).
Available at SSRN: https://ssrn.com/abstract=2580664

Zachariadis, Markos and Ozcan, Pinar, *’The API Economy and Digital Transformation in Financial Services: The Case of Open Banking’* (June 15, 2017). SWIFT Institute Working Paper No. 2016-001.
Available at SSRN: https://ssrn.com/abstract=2975199

Zetzsche, Dirk Andreas and Annunziata, Filippo and Arner, Douglas W. and Buckley, Ross P., ‘*The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy’* (November 5, 2020). European Banking Institute Working Paper Series No. 2020/77, University of Luxembourg Law Working Paper Series No. 2020-018, University of Hong Kong Faculty of Law Research Paper No. 2020/059.
Available at SSRN: https://ssrn.com/abstract=3725395

Zunzunegui, Fernando, ‘*Digitalisation of Payment Services’* (September 27, 2018). Ibero-American Institute for Law and Finance Working Paper No. 5/2018.
Available at SSRN: https://ssrn.com/abstract=3256281

Sitography

Bank of Italy: *https://www.bancaditalia.it*

Bank of International Settlements (BIS): *https://www.bis.org/*

Dedagroup: *https://www.deda.group*

Deloitte: *https://www2.deloitte.com/it/it.html*

European Banking Authority (EBA): *https://www.eba.europa.eu/*

European Central Bank (ECB): *https://www.ecb.europa.eu/home/html/index.en.html*

European Commission (EC): *https://ec.europa.eu/growth/index_en*

European Payments Council (EPC): *https://www.europeanpaymentscouncil.eu*

European Securities and markets authority (ESMA): *https://www.esma.europa.eu/*

EUR-lex: *https://eur-lex.europa.eu/homepage.html*

Everest: *https://www.everest.org/*

Global Legal Insights, *https://www.globallegalinsights.com/*

Nordigen: *https://nordigen.com/en/banks/open-banking/location/ee/*

PYMNTS.com*: https://www.pymnts.com/*

SpicePay: *https://www.spicepay.com/*

Swift: *https://www.swift.com/*

WesternUnion: *https://www.westernunion.com/blog/it/storia-di-western-union/*

Visa: *https://www.visa.co.uk/about-visa/our_business/history-of-visa.html*