LUISS

Department of Economics and Finance

Chair of Money and Banking

# The future of cash

*Evolutionary, regulatory, and ethical analysis of digital payments*

Prof. Paolo Paesani

SUPERVISOR

Luigi Ronci 225301

CANDIDATE

Academic year 2019/2020

**Table of contents**

## Introduction

Digital payments have already revolutionized the payment system, but their widespread diffusion is going to affect people's lives and economic systems in a deeper way, bringing advantages that were not even expected by the pioneers of these technologies.

The aim of this thesis is to analyze the evolution of electronic payment systems from a technical, regulatory, and ethical point of view, in order to define their role in the complex net of transactions that will connect consumers to businesses in the near future.

The development of digital payment systems has typically been considered as a trigger for the replacement of cash, although this is not the only possible outcome: in this thesis I will focus on the characteristics of digital payments that affect the future of cash as a means of payment, speculating on their role in increasing efficiency and financial inclusion.

The work is divided in three chapters, each discussing one side of the argument: the evolutionary section discusses the history of digital payment systems and their role in society through the years, from credit cards to smart speaker payments, giving an overview of how they have affected the overall system of payments, concluding with forecasts about the next technologies that will be adopted. The second chapter will discuss security concerns and will give an overview on the most crucial directives that countries are adopting in order to regulate digital payments and favor their diffusion in a safe environment for consumers and businesses. A specific section is devoted to the PSD2 Directive, which is considered the most advanced and complete set of regulations on this matter and which is being looked upon as a model for future laws to be implemented. Finally, the ethical aspect of digital payments, which is not usually taken into account when discussing this phenomenon, is going to be deeply analyzed in the third chapter, in parallel with the future role of governments and regulatory authorities in the further development of digital payments.

My analysis led to some considerations: first, digital payments are not meant to completely replace cash as a means of payments, a more realistic forecast is that the two systems will coexist to serve different scopes; second, digital payments (especially mobile payments) will represent the intermediate step from unbanked societies (mostly emerging market countries) to societies in which financial services - such as credit - are widely adopted and seen as an instrument to increase the overall welfare of citizens through the redistribution of resources.

# Chapter 1. Digital payment technologies

## 1.1 Evolution and adoption of electronic payments

The first iteration of electronic payments is the credit card, conceptualized by a group of businessmen in New York. An anecdote reported by Diners Club US suggests that the idea of a card used to replace cash to make payments was developed by Frank McNamara in 1949. He was dining out with his wife and realized that he had forgotten his wallet. In that case, his wife rescued him paying the bill, but the embarrassment he felt pushed him to find a solution to make payments without having to bring their wallets. In February 1950, McNamara returned to Major's Cabin Grill with his partner Ralph Schneider. When the bill arrived, he paid with a small cardboard card, known today as a Diners Club Card. Quite ironically, the name of this group of pioneers was linked to the services they used to buy – dinners. This event was hailed as the "First Supper", paving the way for the world's first multipurpose charge card. In its first year of business, Diners Club grew to 10,000 members from New York's business elite, with 28 restaurants and two hotels prepared to accept monthly billing from this selected clientele. The American Express card followed shortly thereafter, launching the first plastic card in 1959. (Mandell, 1990).

At first, retailers used to sell at one price for cash and at a higher price for credit (Batiz-Lazo and Del Angel, 2018), but with time and thanks to a growing number of banks committed to the cause merchants began accepting this new payment system and financial institutions introduced a new possibility: cardholders would not have to pay their bills at the end of each month, instead they would have the possibility of carrying their credit forward, for a nominal finance charge. Two associations were then formed, each of them including high-level executives from their member banks: Visa and MasterCard.

In 1966, debit cards were introduced; in contrast to credit cards, payments through debit cards are withdrawn directly from the personal account of the consumer instead of an intermediary account. The use of this system really took off during the 80’s. Since there are low transaction costs for using debit cards, unlike credit cards, this method is suitable for micropayments and currently it represents the most popular non-cash payment instrument globally (Capgemini and RBS, 2019). The technology behind the physical instrument itself, however, has always been closely linked to that of credit cards. We will then refer from now on indifferently to credit cards and debit cards

(unless specified), since the object of this paper is to discuss the instruments, rather than the actual process of payment.

The use of credit cards saw a dramatically increase between 1960 and 1980: most part of the USA population had fueled their consumption after the war with their savings, but the new consumerist approach to purchases decisions demanded for a fast way of receiving credit. Credit cards represented the easiest and quickest means to finance private consumption and brought a revolution to consumers' behavior. The use of credit cards had a major role in the welfare growth of American people, but at the time, the biggest change brought along by credit cards was neglected: the approach to a cashless society (Gießmann, 2015).

Nowadays, the gradual phasing out of cash has become a fundamental part of the system of transactions to which we are accustomed, and the adoption rate of credit cards has dramatically increased: according to data released Nov. 1, 2019 by the American Bankers Association, there were 374 million open credit card accounts in the U.S., with 1.06 billion credit cards in use. In Europe, the situation appears to be similar: in 2019, the ECB has released the number of cards carried per inhabitant, ranging from 0.8 to 3.9, Luxembourg citizens being the most frequent users. Globally, the trend is increasing and by 2026 we could be looking at an increase of about 50% in the value of card payments. (UK Cards association).

The technology behind card payments has evolved since they were first introduced, but not as much as one could imagine. In 1960, IBM implemented a system to uniquely distinguish one card from every other in circulation: a magnetic stripe which could communicate all the information relevant for the transaction, making the process of actually using a credit card more reliable and faster than ever before. It's not until the 2000s that another major innovation took place in this field: the arrival of radio – frequency identification (RFID), which enabled touchless ID verification between cards and card readers, while introducing trends like contactless bracelets, wristbands, and watches. As of now, the main security standard is represented by the EMV computer chip cards, which brings the advantage of a more secure ID verification, but still relying on a physical card and some form of secret code to insert to validate each purchase decision.

The electronic payment system is considered as the foundation of e-commerce and one of its most crucial aspects: it is a payment service that exploits the information and communication technologies including integrated circuit (IC) card, cryptography, and telecommunication networks. An efficient electronic payment system lessens the cost of trading and is thought to be

essential for the functioning of capital and inter-bank markets. With the advancement of technology, the electronic payment system has evolved from credit and debit cards, to electronic cash and check systems, smart cards, digital wallets, contactless payment methods, and mobile payments. The most promising alternative to card payments is constituted by what we could refer to as the "all-digital" payment method of transferring value from one person to the other without a physical object as a medium, be it a paper check or a plastic credit card. This form of completing transactions relies on the advantages brought along by the Internet of things: a wide net of servers that communicate with each other almost in real time, accessible via a computer, a smartphone, or a smartwatch.

Differently from the card-based payment system, "all-digital" payments have drastically evolved since first introduced at the end of the 90's.

### 1.1.1 **The pioneers: Millicent and Ecash**

Online payments began in the 1990s. However, early systems were not user friendly, requiring specialized knowledge of data transfer protocol. Millicent and Ecash were among the first companies to specialize in online and digital payments. The founding of e-commerce pioneer Amazon (1994) provided stimulus to these early digital payment efforts, but it was not until PayPal was added to the equation that the whole payment system really evolved.

Early players such as Millicent and Ecash relied on different technologies to allow the transfer of value over the Internet. Even though neither of the two companies managed to survive to our days, together with NetCash and others, they paved the way for the development of innovative online means of payment and for the proper introduction of crypto currencies.

The Millicent system was to represent a completely new way to buy and sell content over the Internet. It was announced in 1997 and was meant to revolutionize micro-payments over the web. It supported transactions from one-tenth of a cent to $5, eliminating the limit previously imposed of 25 cents. Micro commerce transactions in this range were important to online publishers who wanted to sell newspapers by the article, cartoons by the strip, or music by the song. Most importantly, Millicent could allow vendors to sell software and host-based applications on a per-use basis, for the first time. The Millicent approach made the pay-per-click approach affordable for all. It was designed from the ground up to achieve low-cost transactions by using a

revolutionary distributed brokers approach to speed verification and minimize cost (McKinley, 1997). Steve Glassman and his team (1996) described Millicent's operating mechanism in "The Millicent protocol for inexpensive electronic commerce" paper: the system achieves inexpensive and secure transactions using accounts based on scrip and brokers to sell scrip. A piece of scrip is formally an account the customer has established with a vendor at any given time, a vendor has outstanding scrip with the recently active customers whose balance is kept as value of the scrip. Whenever the customer makes a purchase, the cost is deducted from the scrip's value and a new scrip is returned as change, until a number of transactions have been completed and the user can cash in and close the account. Brokers, instead, serve as accounting intermediaries between customers and vendors: they buy and sell vendor scrip as a service to customers and vendors. Broker scrip is used as a common currency for customers to use when buying vendor scrip, and for vendors to give as a refund for unspent scrip. Millicent reduces costs because it does not need a centralized server or an expensive transaction-processing protocol; moreover, cryptographic costs are reduced to keep them in line with the scale of transactions: the developers' aim was that of making the cost of breaking the protocol greater than the value of the scrip itself. "Millicent answers the question of how companies can profitably use the Web," declared Robert Supnik, Project Manager at Millicent, in a 1997 interview "A publisher, for example, who now has hard copy and on-line subscriptions for sale, can offer the same information to Web users on a page-by-page or article-by-article basis, adding a new, high-volume, and profitable revenue stream. Users benefit because they select only the information of specific interest to them and pay only pennies a page or less for that information, not for the whole publication". According to Jay Zager, Digital vice president of business operations, Corporate Strategy and Technology group, "Millicent will open up a whole new level of electronic commerce products and services offered on the Internet. In addition to its appeal for traditional publishers, the Web will be much more attractive to electronic publishers, self-publishers, software publishers and service providers, who will now have an incentive to provide higher quality information to Web users and get paid for it. When you consider the on-line games industry and other entertainment applications, the possibilities are endless". Looking at the Millicent project in 2020, it's surprising to acknowledge that the vision these brilliant engineers had in mind has become reality: web services and mobile applications have become the main business of many of the most profitable companies worldwide. Without the input of Millicent, a project that does not exist anymore, we could probably be looking at a very different society.

Ecash, a concept introduced by David Chaum and developed through the company DigiCash, was a micropayment system that represented the first approach to electronic money. The solution relied on Chaum's most decisive invention: The Blind Signature Technology, designed to ensure the complete privacy of users who conduct online transactions. The idea of electronic money was presented by Chaum in his 1983 paper "Blind signatures for untraceable payments", but it was only in 1995 that DigiCash was able to implement such an innovation to payments. Ecash software stored money in a digital format, cryptographically signed by a bank on the user's local computer. The user could spend the digital money at any shop accepting eCash, without having to open an account with the vendor first or transmitting credit card number, thus embracing a degree of security never seen before. Even though the technology was promising and very advanced for the times, the project never really took off: only one bank in the United States implemented eCash, testing it as a micropayment system, but after a three-year trial, less than 5000 customers were interested in the service. In other parts of the world, where credit cards were relatively less popular, a larger number of financial institutes opted to offer an eCash service through DigiCash: in 1998 Credit Suisse enabled the system, followed by Deutsche Bank, Bank Austria, Den Norske Bank of Norway and a few others in Asia and Australia, but despite the optimism and the innovation brought along by the first electronic and secure payment system, people struggled to accept such a novelty, and DigiCash went bankrupt in 1998. Much could be inferred about the rise and fall of DigiCash, but in order to explain the reasons behind this failure, we should refer David Chaum's words during a 1999 intereview for Forbes : "As the Web grew, the average level of sophistication of users dropped. It was hard to explain the importance of privacy to them". The founder of DigiCash saw the lack of digital alphabetization as the main obstacle that stopped eCash from becoming a standard: Chaum was concerned with the public nature and open access to online payments and personal information, but users did not have enough familiarity with the Internet to understand how important security and privacy would be in the years to come.

Other services presented technologies similar to those of Millicent and DigiCash in the years to follow, but they suffered the same obstacle as the two providers analyzed: consumers were not attracted to digital payment solutions, both because the Web and online payments were not widely diffused, and because electronic card payments were considered the perfect instruments for cashless transactions. E-shopping pioneer Amazon pushed its users to welcome such innovations, but it clearly was not as influential as it is now.

It was not until 2000 that PayPal emerged as leader of this industry and made digital payments accessible not only to experienced Internet users, but to each of the consumers that shopped online – a number that had been consistently growing together with the popularization of personal computers and Internet-based services: Amazon and AuctionWeb (which would soon become known as eBay) had launched in 1995 and 5 years later could count respectively on 20 and 12 million accounts (Thestreet, 2019).

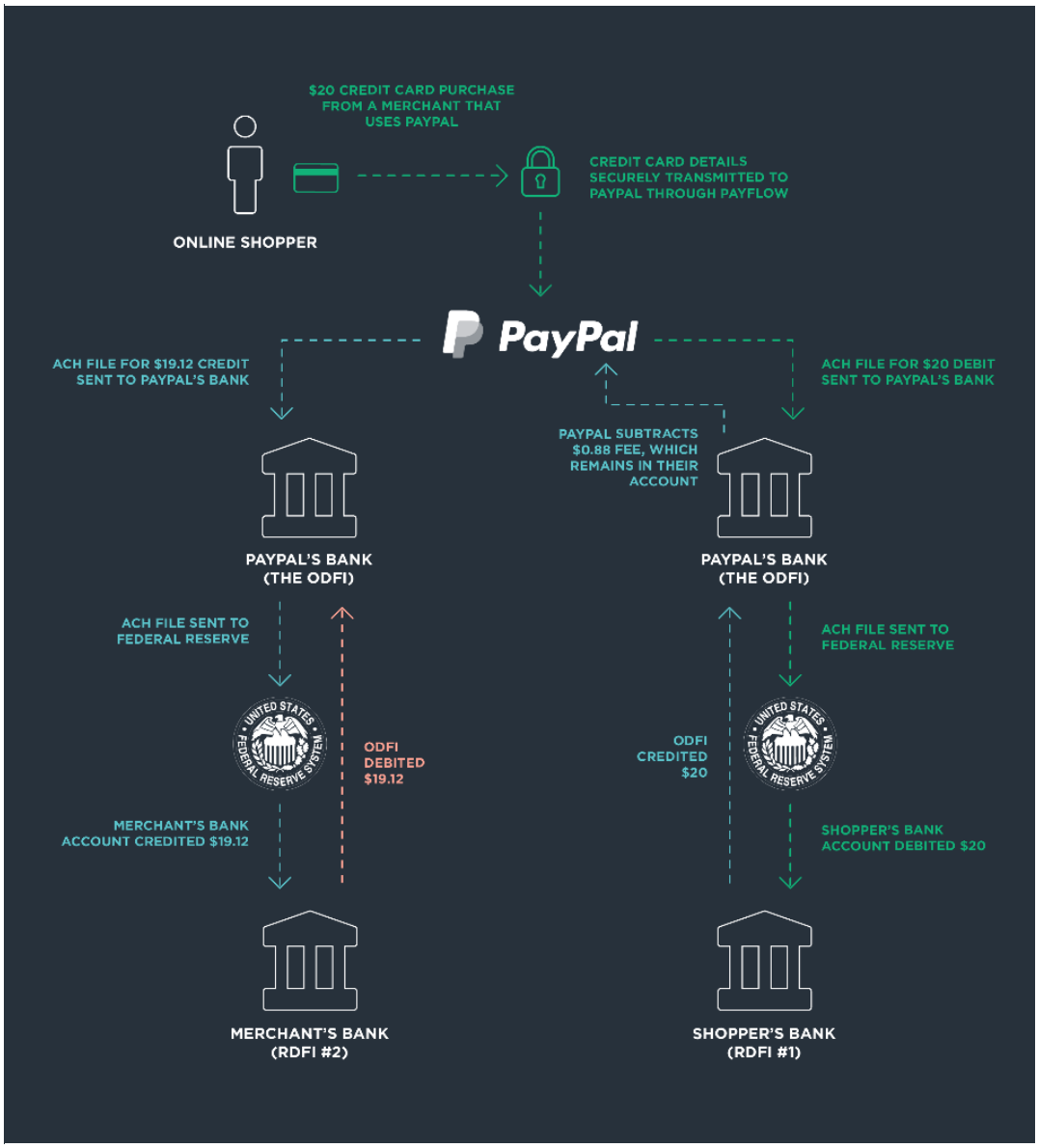
### 1.1.2 **The dominant players today: PayPal and Amazon**

PayPal was founded in 1998 by the security software company Confinity as a money transfer system and entered the digital payments industry in March 2000, merging with the online banking company X.com, founded by Elon Musk. In October of that year, Musk decided that the company would only focus on the newly born payment system, in 2001, X.com was renamed as PayPal, and went public shortly after. The excellent performances of the company further attracted the attention of eBay, an auction-based website whose listings were mostly transacted via PayPal. In 2002, The ecommerce giant bought the rising payment system service, which became the default method for completing transactions on eBay, competing with other customer-to-customer online money transfer tools Billpoint (eBay itself), c2it (Citibank) and PayDirect (Yahoo!). These three competitors failed after less than two years, while PayPal went on to become the worldwide standard for online payments. The reasons for this success are to be found in its innovative technology and impressive flexibility, which allowed users to make payments and donations, both through a P2P and a buyer-to-merchant solution.

PayPal uses a digital layer to allow more seamless Automated Clearing House (ACH) transfers between bank accounts, greatly decreasing the friction of online payments. The technology

enables an online merchant to collect payments from users whether or not they have a PayPal account.

*Figure 1. Paypal payment processing scheme*




*Source: Finplaid.com*

Figure 1. shows PayPal processing scheme (Pratini M., 2016): during a transaction, PayPal operates as an intermediary, initiating two different transactions:

I. Withdraw the money from the customer's account

II. Deliver the money to the merchant.

In case the customer does not have funds in their PayPal account, the merchant's website collects her payment details and securely sends them to the system, through a service called Payflow, then an ACH (Automated Clearing House) transaction is initiated: PayPal delivers an ACH file containing the key information for the transaction (value of the money owed and account to which they are to be sent) to its bank, the ODFI (Originating Depository Financial Institution), then the ACH files are sent to the Central Bank, which debits the customer's bank account at the merchants' bank in the RDFI (Receiving Depository Financial Institution) and credits PayPal's bank. At this stage, the settlement happens, and PayPal's revenues are generated: in the U.S., the company demands 2.9% on the value of the sale plus a fixed amount of $0.30. The fees are ultimately charged to the merchant, on a sale totaling $100, they effectively receive a total of $96.80. The process is much simpler in the event the customer has sufficient funds in their PayPal account to cover the value of the sale: the only necessary ACH transaction occurs when the merchant requests a transfer to its bank account, this is also what happens in P2P transactions, when users send money to friends (as long as they both have an account).

PayPal has acquired and established partnerships with several companies over the years, expanding its core technology to offer better payment experiences to consumers and backend systems to merchants: key acquisitions are VeriSign in 2005 (to provide added security support), IronPearl in 2013 (a start-up based in Palo Alto offering engagement software to further product development and mobile services), and Xoom Corporation, a digital money transfer company, to strengthen the international business.

Multiple partnerships with MasterCard and Discover Card have helped PayPal bring the possibility of profiting from the service even in physical shops, through a wide distribution of affiliated stores.

In 2014, the company interrupted its subsidiarity with eBay and became a separate publicly traded company, beginning to further expand its network of partnerships and collaborations, making its biggest acquisition in 2018, when the Swedish payment processor iZettle was acquired for $2.2 billion. In 2020, the company is still very strong in the sector of digital payments, counting more than 277 million accounts (255 million consumers and 22 million merchants), and offering services that range from P2P to C2B solutions, with the possibility of operating as intermediary for online and offline transactions, but many other players have entered the industry, foreseeing

the opportunities that a connected world was about to open. Several services offering P2P and C2B value transfers have been presented in the last years: Satispay, Venmo (a subsidiary of PayPal) and Dwolla are just three notable examples. These electronic payment systems are popular amongst the young generations, featuring catchy mobile applications and being easy and cheap to operate, while also offering a level of control for parents and tutors.

A similar approach was undertaken by Amazon, which presented WebPay a P2P payment service operated via website, that was promptly shut down in 2014 after the company declared: "we are not addressing a customer pain point particularly better than anyone else. We've learned a great deal about how and when customers want to send money and will look for ways to use these lessons in the future" (Wolfe D. 2016). Amazon's efforts to revolutionize the payment industry did not stop there. The company invested large R&D resources to launch several products that, although having failed in many cases, helped the industry to define consumers' preferences and future trends. Another example is Amazon Local Register: launched in 2014 as a physical device enabling consumers and merchants to make mobile POS transactions, was soon withdrawn from the market after receiving an average review score of 2 out of 5 from sellers.

After a failed experiment in the industry of crypto currencies – Amazon Coin -, Jeff Bezos' company introduced Amazon Wallet, a controller for digital payment cards available on Android devices. Despite its potential and Amazon's partnerships with BlackHawk Network to implement gift card features, the service still did not enable users to actually make payments and missed the point that was soon to be addressed by Apple and Google respectively introducing Google Wallet and Apple Pay, entering the market of mobile payments.

## 1.2 Mobile payments

A substantial and growing share of digital payments today is represented by mobile payments – a definition which indicates all the payments made through a mobile device. Mobile phones (especially smartphones) have become an essential commodity for an individual and, together with the Internet, they have become integral part of many people's lives. According to the 2019 Mobile Payments Market – Growth, Trends, and Forecast (2020-2025) report by Mordor Intelligence, The mobile payments market was valued at $ 1139.43 billion in 2019 and is expected to reach a value of $ 4690.65 billion by 2025, at a CAGR of 26.93% over the forecast period of 2020-2025. The stores and services across the world are rapidly adopting and integrating mobile

payment applications, such as PayPal, Samsung Pay, Apple Pay, AliPay, and WeChat Pay, to accept payments. Owing to changing lifestyle, daily commerce, and rapid growth in online retailing, this trend is expected to continue over for subsequent many years.

Mobile payments are not a novelty, they exist since the introduction of the SMS technology: premium SMS based transactional payments and Direct Mobile Billing exploited a two factor authentication to make payments whose value would result in the user's normal monthly bill or be deducted from their prepaid balance.

*Table 1. Number of active users of mobile payment services*

| Company | Active users | Latest figures from |
|---|---|---|
| Alipay | 1.2 billion+ | Alipay (Q3 2019) |
| WeChat | 1.151 billion | Tencent (Q3 2019) |
| Apple Pay | 441 million | Loup Ventures (Q3 2019) |
| PayPal | 305 million | PayPal (Q4 2019) |
| Samsung Pay | 51 million | Juniper (2018) |
| Amazon Pay | 50 million | Evercore ISI, Investopedia (May 2018) |
| Google Pay | 39 million | Juniper (2018) |

*Source: merchantsavy.co.uk*

Due to their slow operational speed and low reliability of the process, these systems never gained popularity, but new implementations of value transfers over mobile networks are meant to help emerging market countries (M-Pesa is an example of this effort, and we are going to discuss its advantages and characteristics in another section)

According to a Juniper Research study, in 2019 around 2.1 billion consumers worldwide used mobile wallets for payments or money transfers, with a 30% growth with respect to the year before, clearly representing where the trend is going. According to the Economic Times (2020), an e-wallet is a type of electronic card used for transactions made online through a computer or a smartphone. Its utility is the same as a credit or a debit card. An e-wallet needs to be linked with individual's bank account to make payments; an e-wallet is a type of pre-paid account in which users can store their money for any future online transaction, it is usually protected with a password. Reading this description, one could think that there are no major differences between an e-wallet and a credit card, apart from the latter lacking a physical counterpart. The argument to be made is much less obvious and requires us to acknowledge that an e-wallet is composed of two main elements: software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details. Security represents the biggest concern about the use of mobile wallets and will be the subject of a separate analysis. In this paper, the discussion is going to be focused specifically on mobile wallets, or m-wallets, because of the importance they will gain in the next years throughout the whole payment system and economy.

Table 1 (Merchantsavvy.co.uk, 2020) illustrates how the industry of mobile payments is dominated by m-wallets Chinese providers AliPay and WeChat, with more than 1 billion active users each, followed by Apple Pay, PayPal, Samsung Pay, Amazon Pay and Google Pay[1] (Although both AliPay and WeChat have recently launched their services globally, thanks to partnerships with banking institutions both in Europe and in the U.S., most part of their user base is located in China, which represents a very peculiar case that is going to be treated separately in a following section).

Apple Pay is a mobile wallet service globally available on iPhones and Apple watches from 2018. Based on Apple's partnership with a growing number of participating banking institutions and public services, it supports both international and country-specific international payment schemes. The service uses the EMV Payment Tokenisation Specification, a system that keeps customer payment information private from the retailer by switching the customer's credit or debit card FPAN (Funding Primary Account Number) and creating a dynamic security code, uniquely

[1] The data describe the situation as it was in 2019, but it is safe to say that the growth in user base during the last year has not been particularly biased towards one provider more than others, thus the proportions and positions in the leader board in 2020 are roughly the same as before.

generated for each transaction. Although users receive immediate notification of the transaction, the Apple Pay system is not an instant payment instrument: the funds transfer between counterparties is not immediate, and the settlement time depends on the payment method chosen by the customer. The service also embeds a form of P2P value transfer called Apple Cash. Available only in the U.S., it is a feature that allows the transfer of money from one user to another via iMessage. Although Apple Pay is largely diffused all around the world, its existence and use are subordinated to people's usage of Apple products. Being available only on proprietary handhelds, many analysts see in this lack of interoperability the main limit of the system. Although one could argue that a proprietary service can offer more protection to the user, since Apple has a higher level of control on its devices (for which it produces both hardware and software in house), it is clear that the high level of competition in the smartphone industry will not admit the company's monopoly of mobile payments anytime soon, thus hampering the possibility of it becoming a worldwide standard. Samsung Pay shares the same issue, being available only on Samsung devices.

Google Pay, launched in 2011 as Pay with Google and later become Android Pay, it is a m-wallet app available globally and compatible with the same protocols as its competitors. Although its diffusion is linked to the number of banks and institutions that decide to partner with Google and to the company's ability to cooperate in this competitive sector, this service is the most promising among its peers, addressing the cross-platform interoperability issues brought along by Apple and Samsung, while also maintaining an advanced (although cloud-based and not locally stored, differently from the other two companies) multi-layered security system.

Electronic payments giant PayPal, has more experience processing mobile payments than other providers and has partnered with different kinds of firms, ranging from Google and Alibaba, to the major credit card companies. PayPal global leadership is triggered by its to be a consolidated mobile wallet not tied to a single payment brand, allowing consumers to use any card or mobile payment account they have stored within the system.

In terms of payment volume, PayPal is industry leader and has started to implement its P2P value transfer system Venmo as something more than a social-media friendly money transfer platform, but an as instant payment mobile solution, relying on the user's account balance. Thus, after having offered the possibility of making purchases in physical stores, launched in the U.S., Juniper's research concludes that PayPal has the greatest opportunities to develop a converged wallet on a worldwide basis (Juniper Research, 2019).

The success of mobile payment solutions will be decided by company specific implementations, as well as on the technological standards to which manufacturers and merchants will have to conform. The use and diffusion of e-wallets[2] are closely linked to the development of Near Field Communication (NFC) and other contactless technologies in mobile devices. NFC is an integration of Radio Frequency Identification (RFID) in smartphones and smartwatches which offers a quick and convenient method of interaction between humans and enabled terminals. It is a bidirectional source of communication with a range of 5-10 cm and data transmission rates of 106 to 424 Kbs. Its potential stems from the ability of these frequencies to emulate any kind of smart card and from its inexpensive implementation possibilities (Nambi S.N. et Al., 2019). NFC technology is now available in almost every new smartphone and the applications and services needed to make mobile payments are free and integrated in the two main mobile Operating Systems: Android and iOS, which occupy respectively 72.5% and 26.8% of the total mobile operating systems market, according to Statcounter (2020).

NFC is not the only technological standard available for mobile payments: the recent technological trend towards home automation has been pushing big tech companies like Google, Apple and Amazon to introduce smart speakers, respectively launching the Google Home line, the Homepod and Amazon Echo series of products. These act as intelligent virtual assistants and, besides being able to control home automation systems and surf the web, they can be used to make online purchases: linked to a specific online payment account (Google pay, Apple pay and Amazon pay), smart speakers are able to automate the process of buying and make it easier for the consumer. Although this system does not allow the user to perform a deep research on the products in which they are interested, smart speaker payments are being used (and the adoption rates are expected to grow in the next years) to buy groceries and make recurring payments: according to Statista, 35% of users use smart speakers for buying products like home care, groceries, and clothing. Interestingly, the same research has highlighted that 28% of users use smart speaker to send money or make direct payments, although the number seems to be decreasing due to security concerns (more on this matter in a following section).

QR code payment is another contactless payment method which does not need any kind of specific technology other than a basic smartphone with a camera and a free QR reader app. With “QR” standing for Quick Response, QR codes are “open source,” have a large data capacity, and can

[2] E-wallet is a broad term that refers to software that electronically stores credit card numbers, debit card numbers, and loyalty card numbers. A mobile wallet, m-wallet, is a type of e-wallet that resides on smartphones, on local apps or web-based apps.

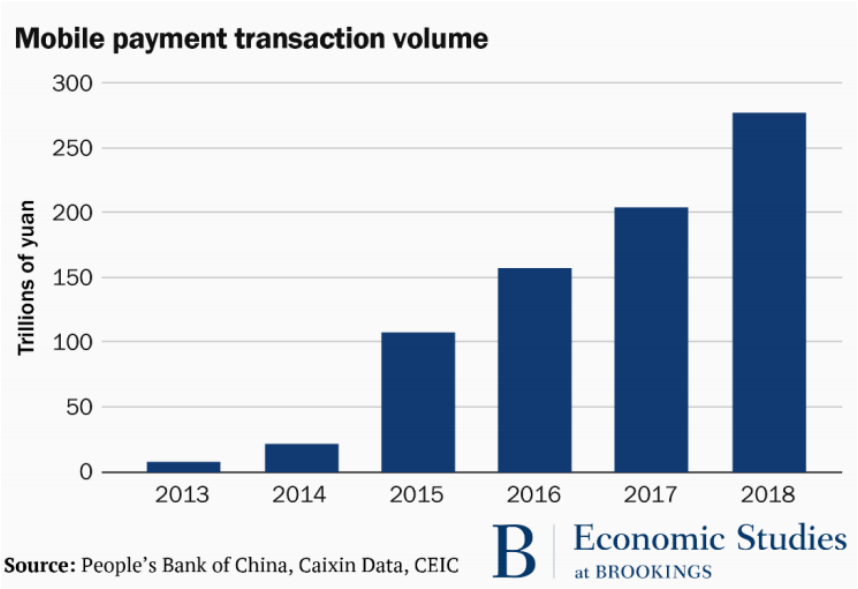
serve multiple uses such as storing contact details or digital payments. Instead of swiping an RFID card or using an NFC equipped smartphone, customers can just frame the merchant's QR code, uniquely assigned to each user, which contains all the necessary information for the money transfer and perform the transaction via compatible mobile apps. The payment starts when one party scans the other's QR code. It does not matter if this scanner is the payer or the payee. The scan can be done by one smartphone to another, or by a smartphone to a QR code that is digitally represented or physically printed on a piece of paper. The payer can total the amount due into the transaction for the payee to scan, or the payee can scan the code and insert the amount to be paid. This is analogous to swiping a credit or debit card into a card reader and either accepting the amount shown or entering an amount you want to pay. Although this system is not popular in Europe or the U.S., where people prefer to use credit cards or mobile wallets, QR code payment is the main technology used for mobile transactions in China, with AliPay and WeChat having more than 2 billion accounts combined.

### 1.3 China: unicum in mobile payments

A 2019 research presented by eMarketer and Kantar TNS clearly shows the Chinese dominance over mobile payments adoption rates, with 81.1% of smartphone users currently using mobile payments, Denmark comes second, with an adoption rate of 40.9%. This impressive discrepancy suggests that there is something more to say about China: this section of the thesis will focus on the analysis of mobile payments in this country, from a technological to a social point of view, and will try to provide explanations for its clear global leadership in the adoption rates. As a 2019 Center on Regulations and Markets by Brookings research (Klein A., 2019) suggests, China would seem an unlikely candidate to develop a new payment system: fostered by government benefits and incentives, the country has developed a strong banking industry, with the main banks collaborating to create UnionPay, a Chinese based card network launched in 2002. The organization is now the largest card payment organization in the world, with 7.6 billion cards, (6.9 billion being debit cards and 686 million being credit cards). With Chinese protectionism and the impossibility for international players like VISA, MasterCard and American Express to enter the markets, it seemed plausible that UnionPay would develop into the dominant payment system within China, mimicking the card-based system in other large economies.

However, due to fees and the costs to implement this technology, only 34 million point of sale had UnionPay payment terminals. Cash payments are currently preferred over card payments by Chinese consumers because of the low rate of card acceptance by stores, although they are not efficient: the highest circulating note is the 100 Yuan (worth about $15), significantly lower than the English £50, the American $100, and the European €500 bills. This allows for more flexibility and divisibility when referring to small transactions, but it could become a problem for large payments: it is not uncommon for Chinese stores to have cash counting machines to speed up the process and avoid counterfeit banknotes. Despite this difficulty, the 2018 World Cash Report highlighted that China is still very much reliant on cash transactions, but the trend seems to be negative: the cash in circulation per GDP has decreased by 13% from 2012 to 2016 and ATM withdrawals are declining rapidly in favor of mobile payment solutions. Other key findings of the research show that 52% of Chinese use cash for only 20% or less of their monthly consumption and that 84% reported that they could accept a totally cashless life.

*Figure 2 Mobile payment transaction volume*




*Source: Economic Studies at Brookings*

Figure 2. illustrates the exponential growth of mobile payment transactions in China in terms of volume: reasons behind the increasing popularity of mobile payments are:

I. The explosion of the Chinese smartphone market (Statista Market Outlook expects Chinese smartphone users to reach 870 million by 2023);

II. The growth of WeChat and AliPay. Starting from zero at the beginning of the decade, the two platforms are now the largest in China and among the largest in the world. Alipay reached one billion users in 2019 and WeChat Pay surpassed one billion users in 2018. These two forms of payment dominate the Chinese market. Over 90 percent of people in China's largest cities use WeChat and Alipay as their primary payment method, with cash second, and card-based debit/credit a distant third. Mobile payments in China have reached over $41 trillion (277 trillion yuan) annually. More than 92 percent of the mobile payments are made over the two dominant platforms: Alipay (53%) and WeChat Pay (39%) (Economic Studies at Brookings, 2019). This rise, fostered by Chinese government's effort to ban international services like Google Pay, is even more impressive when considering its rapidity: AliPay has now 10 times the users it had in 2013. The main advantage brought along by these applications stands in the QR technology: this solution allows to completely cut out the card reading terminal, working directly from account to account and without a processor in between the two counterparts. This increases speed and reduces costs, since users' accounts are prefunded through bank accounts and there is no need for a middleman to approve the transaction (differently from what happens with PayPal, as analyzed in Section 1.1).

Mobile payments are inevitably pushing Chinese society towards the abolition of cash. Even though representatives of both companies are quick to acknowledge that a totally cashless China is unlikely soon, WeChat and AliPay are promoting the concept through "Cashless week" (first week of August, AliPay), "Cashless Day" (August 8th, WeChat Pay) and "Cashless Month" (August, WeChat Pay).

As Aaron Klein points out in his 2019 paper about the Chinese payment system, it is likely that a growing number of international businesses will adapt to it, in contrast to the western payment structure, still bank centric and mostly card based. Partnerships between western financial institutions and Alipay or WeChat may make that transition easier, but without some form of integration, transaction costs and frictions may remain, creating impediments for non-Chinese firms to accept Chinese payment systems. The overall outcome seems clear: Chinese payment systems will merge into global payments.

However, Americans and Europeans are hardly abandoning their cards in favor to Chinese payment platforms. Policy restrictions, particularly the inability to link non-Chinese bank accounts to the payment systems, make it more difficult for foreigners to enter the ecosystem.

Second, wealthier consumers are economically better off with their current credit card systems and it will be difficult to make them switch. To the extent that a market opportunity exists, it is with lower-income users of prepaid or debit cards, which in many cases are not even granted regular credit cards by their banking institution of choice due to lack of financial requisites. Moreover, PayPal has recently introduced the possibility of making QR code payments through its already existing platform: each account, be it a PayPal account or a linked bank account, is associated to a unique QR code. Users are able to make transaction in the same way as WeChat and AliPay, although at a higher cost: as reported from Financefeeds (Adinah Brown, 2016), WeChat users can freely transfer money within the app ecosystem as long as the value of the transaction is below RMBY 1000, after this limit, they are charged a 0.1% transaction fee. PayPal, exploiting its market strengths, is able to charge a fixed fee of €0.20 plus a 0.5% for each transaction (PayPal, 2020).

Considered all this, the instance that Chinese payment systems like WeChat and AliPay will become a standard in western countries does not look to be in the foreseeable future, although QR code payments are expected to increase in terms of volume of transactions, it is expected that western users making payments in their domestic countries will stick to more familiar solutions like PayPal (or its subsidiary platform Venmo, more integrated in the system of social networks). Despite this, non-Asian business owners willing to interact with Asian businesses and customers might be forced to adopt Chinese payment systems as to avoid frictions. The recent opening of China towards American financial services providers such as American Express, MasterCard, Visa and PayPal Holdings (Bloomberg, 22 January 2020) indicates an increased interconnection of western and Chinese systems: in the future, services like WeChat Pay and AliPay might offer the possibility to link non-Chinese bank accounts to their services, or western services might develop further in Asia: in both cases, global integration is key to the development of an efficient net of digital payments, and the industry seems to be going in that direction.

### 1.4 Mobile payments in emerging market countries

A large number of adults in developing countries lack access to formal financial services and cash is still the most used payment instrument. Mobile payments might represent a cost effective way to increase people's financial emancipation and reduce frictions and inefficiencies linked to an economic system of exchanges completely relying on cash (helping fiscal control and political corruption, still a very relevant problem in developing countries, particularly in African nations).

The analysis of this section is going to focus on Sub-Saharan African nations: being in the early stages in the adoption of mobile payment system, they represent an interesting case study, allowing for forecasts and speculations.

In Africa, even though access to ATMs (the most direct measure of the use of cash in day-to-day transactions) and bank branches is improving, the 2018 World Cash Report highlights that it is still limited, with most African nations scoring well below the global average on both criteria. A study from Aina and Oluyombo (2014) shows that most people operate savings accounts, with a low ratio of 1.4 bank accounts per adult (including inactive accounts). According to the same study, a larger penetration of bank accounts reduces the use of cash payments, given the possibility to use easy means of payment such as cheques, credit cards, debit cards and electronic money transfers. Many academics, development organizations, and governments are urging Sub-Saharan nations to enter the formal economy, since financial inclusion is foundational for poverty reduction and economic growth. The highest self-reported barrier to the use of bank accounts is the lack of necessary documents; however we believe that a low banking density hampers financial education, hence citizens are not incentivized to open current accounts. Increase in public enlightenment campaign would be beneficial to low income earners, together with stable electricity supply to drive the infrastructural facilities of banks and telecommunication services.

It is clear that infrastructural and educational reforms require both time and investments, but a shorter-term solution might be represented by mobile payments. Mobile phones might be regarded as mini bank accounts for receiving money and paying for goods and services, without the discomforts brought along by traditional bank accounts. Services like M-Pesa, founded in 2007, are on the rise in Sub-Saharan nations. The solution allows users to deposit, withdraw, transfer money, pay for goods and services, and access credit and savings by only using their mobile phones, using technologies like PIN-Secured SMS text messages. Some of the most recent mobile usage statistics, from a 2018 Pew Research Center study, found that approximately 91% of South African adults own mobile phones, with 51% of adults owning smartphones and the remaining 40% percent owning standard cellphones. Ghana has an 80% ownership rate, and Senegal follows closely behind with a 79% ownership rate, with 34% of adults owning a smartphone and 46% of adults owning a standard smartphone. Nigeria and Kenya also had an 80% ownership rate, while in Tanzania 75% of adults reported owning a mobile phone. It is then not surprising to acknowledge M-Pesa's success: which currently has more than 15 million registered users.

African news website “Sun-connect” reported in a 2019 article that access to Kenya’s M-Pesa mobile payment system increased per capita consumption and helped 194,000 households, or two percent of Kenyan households, out of poverty. Governments consider the development of mobile payment systems as a way to move informal money “out from under the mattress” and to foster financial inclusion.

# Chapter 2. Regulatory overview

## 2.1 Security concerns

Every use of technology is subjected to fraud, data theft, and stealing. Clearly, the situation becomes more dangerous when the data contains significant financial information, thus, despite the fact that e-commerce is a growing field with an increasing use of online payment services, its further development and widespread use in future are dependent upon the security and authentication stability of various electronic payment systems (Aigbe and Akpojaro, 2014). The pace at which these new technologies will be widely implemented and used fundamentally depends on the trust consumers are willing to put in the hands of providers, which is indeed closely related to security concerns. People will not be willing to switch to a cashless lifestyle unless they have complete trust that their money is going to be safe, even more so if it's taken into account that the relation with paper money is still very much related to cultural factors. In this context, the role of the regulatory system is crucial in determining how companies are able to interact with customers, what policies they must follow and how users can be protected from all sorts of risk, from those related to the underlying technology to those concerning the human factor necessarily involved and the role of delegation that financial (and now even not strictly financial) firms are given when providing payment services (Bezhovski, 2016).

Together with the development of digital payments, the damage created by frauds and inefficiencies in the system has become more consistent and dangerous to the economic system as a whole. In 2018, Shift Processing reports, $ 24.26 billion have been lost due to payment fraud worldwide. This section of the thesis is going to be focused on an analysis of the main sources of risk deriving from electronic payment systems and will give an overview on the work companies are making in order to minimize risk and maximize adoption rates of their systems.

Before analyzing the specific threats to which each of the instruments we discussed in the previous chapter is subjected, we must first understand on a basic level the main general concerns:

I. Hacking: an individual breaking into an electronic system to initiate unauthorized transactions through another individual's account, directly stealing money. This does not just refer to the overall central system, but also to a single device.
II. Identity theft: an individual stealing customers' personal data and setting up illegitimate credit card accounts and/or bank accounts.

III. Cloning: strictly related to the identity theft, cloning refers to the risk that an individual could replicate the unique characteristics that make up a payment instrument, thus effectively creating a copy of the device and having access to all its features and services.

IV. Data corruption: an individual attacking the system as vandalism or to extort money from the financial institution. Another example of data corruption could happen in case of damaged servers (the net of computers that store data about transactions and users), thus without a wrongdoer necessarily attacking the electronic system, but rather their physical counterpart.

V. Data breach: the instance in which the system is attacked, and customers' personal information are publicly revealed. This is an issue that has been arising consistently especially in the last years. A notable example is represented by eBay. According to data published by CSO Apr. 17 2020, in May 2014, the e- commerce giant was victim of an attack that exposed its entire account list of 145 million users, revealing all kinds of personal information such as names, addresses, dates of birth and encrypted passwords. Allegedly, hackers used the credentials of three employees and had a complete free access to the network for 229 days – enough to compromise the entire database.

VI. Usage for illegal purposes: an individual exploiting the efficiency and encryption of the electronic system to fund illegal activities such as money laundering or terrorism. This is a central issue that will be discussed more deeply in the section of the work devoted to ethical concerns.

VII. Fraud: a general term to include all the risks arising from human interaction at the moment of a cashless transaction. Without cash directly being transferred hand to hand, tracking the amount of money one is paying may be difficult in some circumstances and merchants might have the incentive not to be transparent with clients

In a previous section of the work, we have analyzed the main instruments through which customers are able to make digital payments, and it is crucial to understand that none of them is completely free from risks. Although companies are concentrating their efforts to minimize them, each technology has its limits that must be understood and discussed.

As previously stated, credit cards are still the most popular cashless payment method, but they are far from being the safest. In the US, credit card fraud increased by almost 20 % and the trend seems to be increasing. Identity theft is the most common credit card fraud, representing 14.8% of the cases (Shiftprocessing, 2018). Specifically, credit cards can be easily cloned, scammers use skimmers on point-of-sale systems to get personal information and use it to make a duplicate card,

even though the RFID Technology is easily replicated, the introduction of smart chip credit cards is a step towards a higher degree of security: smart chips are microchips embedded in credit cards that encrypt the information contained in the magnetic strip. They cannot be deleted or modified and in case a scammer manages to disable it, each transaction they try to make will alert the point of sale staff to require some form of identification or decline the transaction.

E-wallets represent the future of the digital payment industries thanks to their flexibility and ease of use, but they are not exempt from risks worth noting (Brown S., 2019):

I. Phone theft: e-wallets are available through mobile applications that are not always properly secured with two-factor authentication, to the extent that losing a phone might be equivalent to losing a physical wallet.

II. Biometrics breach (DigiPay, 2020): Samsung Iris scanner, Apple TouchID and FaceID, and LG Palm scanner are some notable examples of biometric authentication implementation from smartphone providers. Most of these technologies have been certified to give payment authorizations, but they are not 100% safe. As of now, Apple's system appears to be the most reliable: as reported on Apple website, FaceID exploits cameras and infrared sensors to analyze more than 30 000 points and create an invisible map of users' faces. Adapting to changes like make up or facial hair, the possibility that a person different from the user manages to unlock the device and make payments is estimated to be close to 1 in a million. Most importantly, FaceID stores the mapping information locally, on an encrypted section of the phone's internal storage, as reported on Apple.com.

III. Wallet spoofing: credit card numbers are encrypted in all the main mobile wallet applications, meaning that there are masked by a code created by an algorithm, through a process called "tokenization". Different companies exploits different iterations of this technology, but if mobile users add cards to their account while connected to public Wireless Networks and without using a VPN service (Virtual Private Network), a wrongdoer could re-create ("spoof") that mobile wallet's registration and create their own account with legitimate payment information. Wallet spoofing is therefore the digital equivalent of credit card cloning, but companies and users themselves have a wide variety of instruments to protect their information. From local encryption companywide (used by Apple Pay) to VPN at individual level, e-wallets layers of security are increasing in number and effectiveness.

IV. Mobile malware: even though this is an issue that concerns the whole smartphone industry, and not specifically mobile wallets, it is worth noting that, just as PCs can be affected by malware, so do smartphones. Virtual viruses could propagate through the system and steal every information contained in it, from its IMEI identification code, to personal information stored in mobile wallets.

V. Smart speaker related security concerns: home assistants and smart speakers such as Google Home, Amazon Echo and Apple Homepod offer the possibility of making payments through company specific digital wallets such as Google Pay. Without the possibility of manually checking the transactions users are going to make, after having given a voice command, it is reasonable to understand that customers may have some reluctance in using these systems. Moreover, voice recognition algorithms, although advanced and growing in functionalities, are not completely reliable in distinguishing the owner's voice from those of others, thus potentially receiving and executing payment commands from wrong doers.

Companies such as Google and Apple understand that their services will be widespread only to the extent that their communication about privacy and security is transparent and provide detailed explanations of their security protocols themselves.

As we analyzed in the previous section of the thesis, QR Code payments are going to be adopted at an increasing rate due to their flexibility and their low costs of implementation, but, unfortunately, the underlying technology is prone to risks. An MIT research conducted by Peng, Sanabria, Wu and Zhu named "Security overview of QR Codes" highlighted the main issues related to this system:

I. Attacks on human interactions, related to the inability of humans to understand the information contained in the image of the code. Since users cannot read the data, they are prone to be attacked via phishing, pharming, and other social engineering attacks by hackers putting up fake or manipulated QR codes.

II. In case of payments, wrongdoers could modify the code associated to a merchant and redirect payments to their accounts.

The research proceeds then indicating, from a technical point of view, which solutions may be applicable in order to resolve this important issue: the answer is represented by the implementation of stronger security protocols and encryption, together with the resolution of bugs that further decrease the reliability of the system.

In conclusion, security concerns are a critical obstacle companies need to overcome in order for their services to be widely adopted: cyber security advances and improvement in the stability of the systems are the fundamentals of this process, together with the implementation of strict regulations to protect customers and make digital payments safe and transparent as well as efficient.

## 2.2 European regulatory framework under the PSD2

As stated by the EBA (European Banking Authority), the role of regulations for the industry is aimed at ensuring that payments across the EU are secure, easy, and efficient. These characteristics are of primary concern when referring to the overall payment system, but in the specific case of digital payments, still not as widely adopted as cash payments and thus requiring a higher level of attention.

The development of an integrated European market for safe electronic payments is crucial to support the growth of the union economy and to ensure that consumers and merchants enjoy choice and transparency. The Directive 2015/2366 of the European Parliament and of the Council (25 November 2015) - widely referred to as PSD2 Directive - is going to be the focus of this section of the thesis: nevertheless, there will not be a technical legal analysis of each article, rather a discussion on its main points to understand why it represents a crucial step towards the widespread adoption of digital payments. For every topic discussed, its position within the Directive is going to be provided, so as for the reader to be able to easily recover the full information in the text, given that our analysis will only grasp on the main points, particularly interesting for the scope of the thesis.

The objective of the PSD2 Directive, which applies to payment services provided within the Union, is to provide legal clarity and to ensure consistent application of the legislative framework in the sector of digital payments, guaranteeing equivalent operating conditions to both existing and new players on the market and enabling new means of payment to reach a broader market. Moreover, the directive aims at ensuring a high level of consumer protection in the use of electronic payment systems across the Union. The underlying general scope is to generate efficiencies and provide for more transparency of services, while strengthening the trust of consumers.

One of the most important issues discussed in the directive (Article 14) is the strict authorization process that a firm must undertake to be accepted as a payment institution and publicly registered in each Member State. Here the main requisites:

a) Sufficient initial capital and a business plan, including a forecast budget calculation for the first 3 financial years, which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;
b) Detailed procedures of internal control mechanisms, risk management, money laundering and terrorist financing;
c) Description of process in place to file, monitor, track and restrict access to sensitive payment data;

The directive explains in detail the activities a payment services provider must not undertake as it is not a banking institution, nor it should be. It is much more difficult for a new bank to be granted the authorization of operating, and payment service providers are not meant to replace banks. This specific topic has been discussed in several sections of the thesis, but it is crucial to make a separation of intents, clearly marked in Article 18 and 85 of the PSD2. Here the two main points:

a) Any funds received by payment institutions from payment service users shall not constitute a deposit or other repayable funds;
b) Payment institutions may grant credit, only at the condition that the credit is ancillary and granted exclusively in connection with the execution of a payment transaction, that it is in compliance with national rules on providing credit by credit cards, that such credit shall not be granted from the funds received or held for the purpose of executing a payment transaction, and that the own funds of the payment institution at all times are appropriate in view of the overall amount of credit granted.
c) Where a consumer places cash on a payment account with a payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after receipt of the funds.

The Directive then gives information about liability, record keeping, designation of competent supervisory authorities, and the application to exercise payment services in a Member State other than its home Member States.

Articles 45 to 49 contain the most important guidelines that a payment service provider must follow regarding the information and conditions provided to the user. The discussion of this section is crucial for the analysis that we want to take on, since it strictly relates to users' trust in

the payment system: the more specific it is, the more consumers will be willing to engage in digital payment activities. Not only shall a payment service provider be transparent and compliant with respect to competent authorities in terms of the activities it undertakes, but it has the moral and legal obligation to clearly provide information to its user base. One of the most important protections that the European legislation gives to consumers is therefore contained in this section of the Directive. These are the main information that a payment service provider must make available to users:

a) A specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly initiated or executed and the maximum execution time for the payment service to be provided;
b) All charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges;
c) Where applicable, the actual reference exchange rate to be applied to the payment transaction.
d) The name of the payment initiation service provider, the geographical address of is head office and, any other details, including electronic mail address, relevant for communication with the payment initiation provider, together with the contact details of the competent authority.
e) The confirmation of the successful initiation of a payment order, together with a reference enabling the counterparts to identify the payment transaction, its amount, and, where applicable, a breakdown of any charges payable to the payment initiation service, and any information transferred with the transaction.

The PSD2 systematically indicates the contractual conditions applicable to the relation between user and provider, together with a detailed explanation of the charges and exchange rates applicable, refund conditions and liability in case of noncompliance to the Directive itself.

Another section which is fundamentally linked to the scope of this thesis is Article 94 – Data protection -, which states that Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. Moreover, the provision of information to individuals about the processing of personal data for the purpose of the Directive shall be carried out with Directive 95/46/EC, which relates to the protection of physical persons, with regard to personal data treatment ant their free circulation. Payment service providers shall only access, process and retain

personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. Clearly, the protection of personal data is a fundamental matter in every circumstance, but it is especially important to people when the matter is of financial nature, thus requiring service providers to engage in a more transparent and clear communication with users.

The management of operational and security risks is also thoroughly discussed in the Directive, together with procedures about incident reporting and technical standards on authentication and communication.

It is important to highlight that the Directive also provides information about the withdrawal of the authorization, which happens in case the provider no longer meet the conditions for granting the authorization or fails to inform the competent authority on major developments in this respect, or the continuing of its payment services business would constitute a threat to the stability of - or the trust in - the payment system. The competent authority shall make public the withdrawal of an authorization, for reasons of transparency and consumers protection.

Noteworthy, the PSD2 represent the first systematic set of rules provided to ensure protection and fairness in the specific matter of electronic and digital payments, and it is not exempt from flaws, such as the ambiguity about the technical standards to use to authorize a transaction – a fundamental issue in the matter of security concerns, as we explained in section 2.1 - : the only indication is contained in Article 97, which states that "[…] Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee". In a following revision, it may be necessary to rethink about this section, conceptualized at the end of 2014, when mobile payments where not as common as they are now, in order to give more specific information in terms of technical standards such as a list of biometric authentication methods accepted to initiate a transaction, based on their level of security and reliability.

Nevertheless, the existence of such a directive represents a statement by the European Union: digital payments are going to be increasingly popular and integrated with the life of European citizens. Besides the specific norms discussed in the text, what should be the first and main concern is to acknowledge the existence of a new way of intending money and transactions, thus requiring a dedicated set of rules. This issue is of growing concern, and many other countries have decided to innovate their regulatory systems to make them coherent with the innovations in electronic and digital payments.

In the next section, we analyze the most recent regulatory introductions adopted by different countries worldwide, so as to understand what problems are being recognized as such by global players and study their take on them. This will enable us, in the final section of the thesis, to make predictions about the future of cash and speculate on the possible solutions to the problems and challenges that, inevitably, countries and industry leaders will have to face.

## 2.3 Trends in worldwide regulations

As analyzed in the 2019 World Payments Report, interoperability and standardization have become a key point for regulators to address amid disparate payment standards, systems, and scopes. Globally, many countries are planning initiatives to ensure uniformity and increase security standards and protections for users. It is clear to everyone that global adoption of digital payment systems is subjected to the trust that customers have with respect to this issue, in turn determined by the level of security offered within the systems.

A notable set of guidelines with respect to interoperability has been enacted by the Reserve Bank of India in October 2018. This regulatory innovation enables mobile wallet users to transfer funds from one wallet to another and, eventually, from their wallets to bank accounts through India's unified payments interface platform. It is not common for mobile wallets provided by different companies to have such a high level of interoperability, but we think that this move will foster competition and thus innovation in the sector of digital payments. Moreover, the direct link between bank accounts and mobile wallets that the RBI has created is crucial for the widespread diffusion of cashless transactions, and, perhaps more importantly, to increase the level of financial inclusion in a country where internet based services are growing substantially: the use of mobile wallets as an intermediate passage for people to engage in the formal financial system has already been discussed in section 1.4, and is a crucial aspect for regulators to take into account when making policies about digital payments, especially in emerging market countries with a large portion of the population living in rural areas, thus having less access to bank branches and financial services, such as India[3].

Asia-Pacific Economic Cooperation (a regional economic forum that today has 21 members, among which USA, Canada, Russia, and Japan) has developed several data protection initiatives,

[3] Rural population in India was reported at 65.97% in 2018, according to the World Bank collection of development indicators.

such as the CBPR (Cross-Border Privacy Rules) system. This is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized data privacy protections. It is important to underline the fundamental importance of cross-border shared policy, an aspect that is going to be discussed in a following section and that will determine the fortune of digital payments in the years to come.

Important innovations in cybersecurity regulations have been made as well, following the implementation of PSD2 in January 2018. The US, Japan, India (which spent 10% of its annual IT budget to cybersecurity efforts in 2018 as reported in the World Payments Report 2019), Australia and New Zealand have recently implemented a series of laws and guidelines to improve transparency and enable banks and financial institutes to thoroughly address risk management, business continuity and incident response, together with efforts at reducing the misuse of encrypted communication networks and transactions for reasons of money laundering and terrorism. In Europe, the EU cybersecurity act was enforced in June 2019 to establish an EU-wide cybersecurity certification framework for digital products, services, and processes.

Data privacy and protection issues are also being addressed more carefully by almost every country, after the 2018 implementation of the General Data Protection Regulation in the EU, but a notable directive has been introduced in India, where a proposal has been submitted to the parliament in order for banks and financial institutes to store Indian citizens' personal data only on India-based servers. The reason for doing so is to minimize the possibility of data breach, together with the limitation of the damages that such event would cause. The location of servers in India would allow for a higher level of control of local authorities in case some wrongdoer tried to access them and steal information.

## Chapter 3. Future opportunities and main challenges

Although the use of digital payments has been growing substantially in the last years, they have not yet substituted cash for daily transactions. This adoption lag, besides it being physiological for a new technology, is to be explained by reasons of standardization, ethical concerns, and institutional decisions. In the next section of the thesis, the analysis is going to be focused on these issues: we will give an overview of the main problems and provide possible solutions for them, with the objective of investigating on the future of digital payments, and speculating on them becoming the next standard or not.

### 3.1 The need for shared policies

With multiple service providers and technologies available, standardization is not easy nor immediate to achieve: although it is not possible for regulators to impose a specific technological standard, they can make the process automatic and smooth by operating on a set of policies and regulations shared by the largest number of countries and organizations. For local players with operations across multiple geographies, the present global fragmented regulatory landscape is one of the main sources of costs and frictions.

Before analyzing the different sectors in which shared policies are to be implemented in the next two to five years, it is crucial to disclose the main idea behind all this: why do we need shared policies? The main purpose of digital payments is to increase the speed and efficiency of the payment system through the reduction of transaction costs, in terms of money and effort. Besides having to be safe to use, these payment methods must be fast and cheap to operate. The goal of having a set of clear policies and regulations, shared by at least the most important international players, indeed operates towards this direction. In particular, two fundamental problems must be solved in the next years (Deloitte, 2019):

a) Discrepancies within the different regulatory frameworks: although at this point many countries have implemented laws and directives regulating digital payments from a security point of view and have their own standards to evaluate the reliability of each specific service, the international expansion of providers, and thus the widespread adoption of a common payment method is seriously hindered by the discrepancies in cross-country regulations. A clear example is represented by WeChat Pay and AliPay: the two

Chinese giants, world leaders in terms of transaction volumes, still cannot be used effectively outside China, because the underlying QR Code technology is still considered not secure enough by western governments. Clearly, in this specific case this reluctance may be due to political reasons as well, but still the point is that different standards decrease the possibility of a widespread adoption of a common digital payment interface.

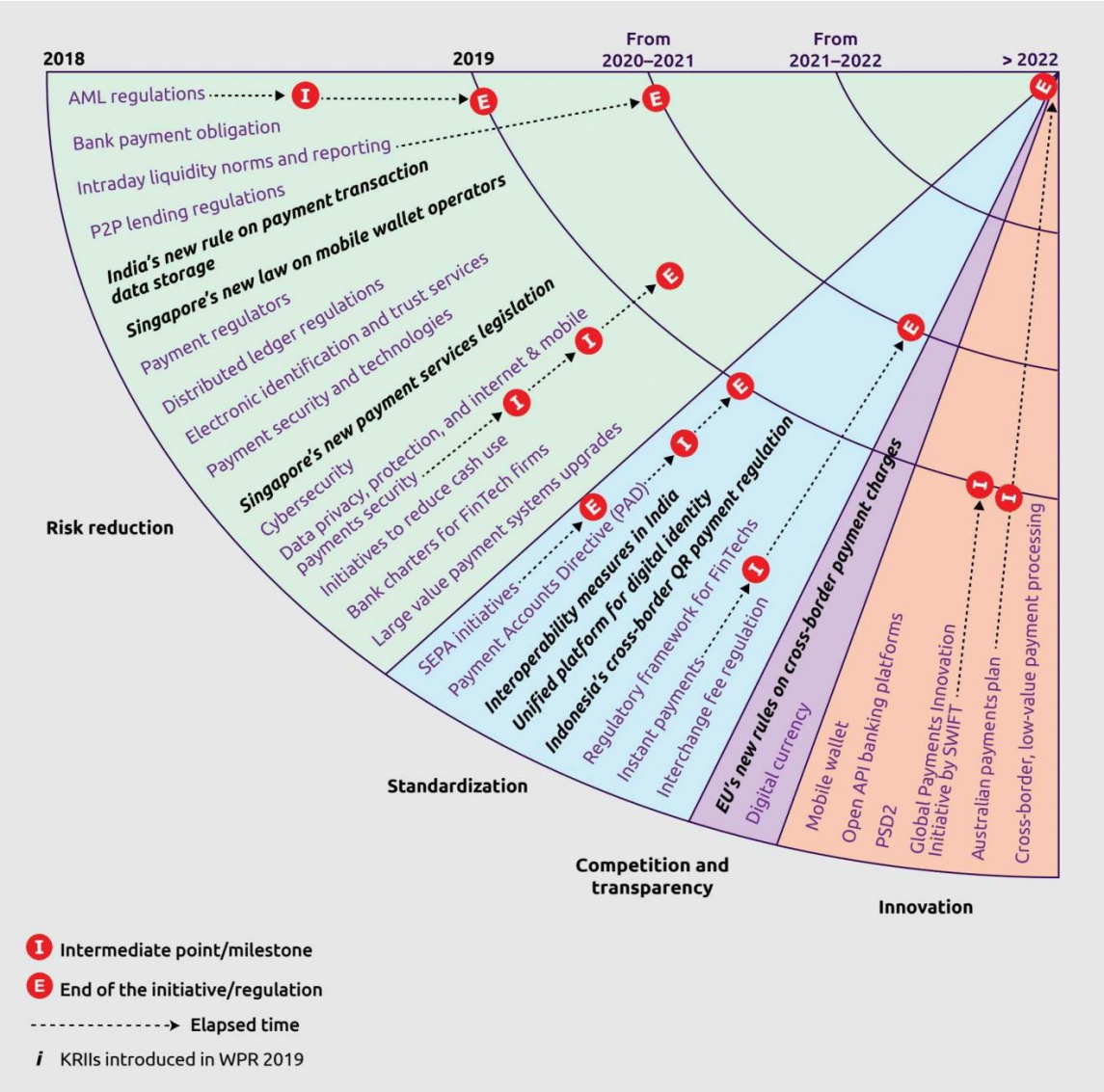
b) Cross-border payment processing: international payments are still considered too costly for such a globalized world and integrated net of transactions. Many merchants still rely on third party services to manage their international payments, and this works against the fundamental logic of digital payments to reduce the number of intermediaries and middlemen. Within the next decade, cryptocurrencies linked to digital payment methods are forecasted to dominate the sector of international transactions, shrinking down the volume of overhead costs, but as long as fiat currencies are the main means of payment, governments should harmonized their policies in order for businesses not to be stopped in the process of internationalization, fearing excessive costs.

Figure 3 illustrates, as reported by the Global Payments Report 2019, the temporal path for future regulations and policies in the sector of payments. The most notable regulations that are to be implemented soon, concern risk reduction, standardization, competition, transparency, and innovation. Although they would seem mainly country-related, there is a clear bias towards cross-border implementation of already existing rules, such as the new EU rules on cross-border payment charges, that would substantially contribute to reducing costs and regulatory barriers for the adoption of digital payments as the main form of payment.

In section 1.1.1, we have introduced Millicent, micro payments conceptualized in 1983. Millicent was innovative and futuristic and low value transactions have not been fully implemented within the payment system, due to high payment processing costs and efforts, especially in an international framework of transactions. Regulations will address this matter within the next couple of years.

The absence of shared policies is not the only factor to limit the widespread adoption of digital payments: cultural inclinations and lack of trust in these means of exchanging money play a crucial role as well. In the next section, we are going to focus the analysis on the ethical concerns behind the use of non-cash related payment methods, trying to understand how different cultures and lifestyles affect their diffusion.

*Figure 3 Regulations temporal path*




*Source: World Payments Report 2019*

## 3.2 Ethical concerns

Although it may seem inappropriate to associate payment instruments to ethical beliefs, in this section we will try to analyse positive and negative implications of digital and mobile payments from an ethical point of view.

In section 1.4, the analysis has covered the essential role that digital payments are expected to have in terms of financial inclusion for emerging market countries. As Peterson K. Ozili has cleverly noted in his paper "Impact of digital finance on financial inclusion and stability", there are several obstacles to financial inclusion and to a widespread adoption of financial services, but one of the most damaging is the so-called "voluntary financial exclusion": the voluntary refusal of some individuals in the unbanked population to participate in the formal financial system, either because they are not willing to deal directly with banks or internet companies, they lack financial requisites to obtain credit, or they are not educated about how to use digital finance platforms and about the tangible benefits they could obtain.

Although the school system plays a fundamental role on this matter, one of the main aspects, perhaps the most interesting to point out and the least prone to change, is represented by cultural factors and religious beliefs: in some countries, especially in countries where religious teachings discourage followers from embracing technological changes, leaving cash and adopting a completely new and digital way of making payments do not represent a viable option. Money in itself is often seen as harmful: "For the love of money is the root of all evil…"(1 Timothy 6:10) is just a symbol of the original contempt expressed by Christianity towards money and ancient forms of credit[4]. Despite this, other religions - such as Islam - embrace the use of money, even of electronic money, as long as it is backed by a commodity at a fixed exchange rate. Purely cultural factors influence the adoption rate of digital payment system as well: some communities believe that their money must circulate only among their members, thus discouraging and imposing penalties on individuals that send money outside the community through banks and financial providers, due to their nature of collecting money and redistributing them to other borrowers. The reluctance of some people is to be attributed to their countries' market failures and frequency of banking crises, as Ozili states in his 2017 paper, that determine a low level of trust from citizens

[4] This section of the Bible has been interpreted in several ways, later translations mainly focus on greed and avarice representing what is called "the love of money", but still it is possible to acknowledge some sort of reluctance towards the financial and banking system. Although many aspects have changed and it is common knowledge that the Bible is not to be interpreted in a completely literal fashion, it is not to exclude that the lack of trust in financial institutions from a portion of the population might come from this line of thought.

towards financial institutions. It is not easy – and probably not even possible – to say whether these ideas are right or wrong, but it is certainly crucial to understand that a trade-off has to be made between the efficiency of the economic system, fostered by financial inclusion and banking services development, and personal beliefs.

Digital and mobile payments could help resolve this issue in an original fashion: p2p based payment systems like WeChat pay, M-pesa, Venmo or the upcoming Apple Cash are not directly linked to a banking institution and users can take advantage of them without any financial requirements. Although, as we previously examined, these systems are not meant to replace traditional banks, they could represent an effective intermediate step towards formal financial emancipation: their ease of use and high level of reliability could enhance citizens' trust with respect to the financial system and push them to open their first bank account and exploit the advantages of credit for economic development and welfare.

Digital payments play a major role in the transformation from a cash-based to a cash-less society, particularly, their widespread adoption might be able to effectively reduce criminal activities such as tax evasion. A research conducted by Giovanni Immordino and Francesco Flaviano Russo for the CSEF (Centre for Studies in Economics and Finance) was successful in demonstrating the negative relationship that exist between the use of digital payments and VAT tax evasion. In that specific paper, the analysis was focused on credit cards and debit cards, but it is possible to extend the conclusions of the research to all kinds of traceable digital payments. Notably, each type of digital payment we analyzed is traceable: personal information is protected by encryption mechanisms, but the history of transactions between two counterparties is recorded in databases and servers, thus, in case of need and for justifiable reasons, the flows of money are easily traced by competent authorities with the help of service providers. The key element of the research was this feature, which is common to all systems of digital payments: they build a trail for the underlying transactions; thus, users are greatly discouraged from engaging into criminal activities. The empirical tests showed a negative relationship between VAT evasion and payments with cards. The existence of a positive relationship between cash withdrawals at ATMs and tax evasion, was also highlighted, suggesting that a cashless society is one in which criminal activities as such are reduced to very small numbers. An increased efficiency and transparency of the payment system would therefore increase the volume of taxes payed overall and possibly reduce the tax burden on individuals, improving welfare. In this framework, customs and ethics come to terms with the possibility of a society that could be both more efficient and more respectful of the laws: privacy concerns, which are not a minor issue when the interested matter is of financial nature,

become stronger when mixed with the lack of trust in banking systems and institutions and the reluctance of a portion of the population to conform to new technological standards.

During an interview for "pagamentidigitali.it" (12/09/2019), Francesco Luongo (President of C4DiP – Consumers for Digital Payments) has declared that the gap between northern and southern Italian regions in adopting digital payments is still too wide, and that cultural factors, together with a poor financial education, are with most probability the main problem to address. Moreover, Luongo commented that many citizens are not willing to put complete trust in electronic and digital payments and just 20% of those who use them for daily shopping feels fully confident by doing so. In a following section, the thesis is going to focus on what are the concrete measures that governments and central banks must implement in order to foster the widespread diffusion of digital payments, but the issue to be addressed from an ethical point of view concerns a controversial trade-off: is it right to force the adoption of electronic payments for people who are not willing to leave cash for privacy concerns? Is it ethical to sacrifice freedom in favour of economic efficiency and increased controls in terms of legality? It is not possible to give a unique answer, not based on personal beliefs; what is clear, considering the trends brought along by digital payment companies, the multiple marketing campaigns to improve the transparency and the efforts in the field of cyber-security to reduce the risk of privacy issues, is that it is just a matter of time before new generations become more accustomed to a digital lifestyle, and embrace the use financial products such as electronic and mobile wallets. At that point, the trade-off would seem more reasonable and the benefits would outnumber the ethical concerns.

### 3.3 Future role of Governments and regulatory authorities

Having discussed the characteristics of digital payments, the regulations have been introduced and how they could be helpful to increase financial inclusion and fight tax evasion, we will conclude by discussing the future role of governments and regulatory authorities in the diffusion of electronic payments.

First of all, in order to define what actions authorities should take, a clear objective should be defined: digital payments are in the end useful more than harmful to society and consumers, as long as they are regulated and people feel their personal data to be safe while using them. Their benefits rely on the increased efficiency brought to the payment system, and to their fundamental role in increasing financial inclusion. Moreover, the importance in implementing digital payments

is not valuable if a set of common and shared policies are adopted all over the world, or at least between countries that have a close commercial net of connections. That said, it is reasonable to assume that governments and regulatory authorities should focus their efforts towards a widespread, regulated diffusion of digital payments.

The second issue that must be addressed in this section is about what institutional actions they should implement to achieve the above-mentioned goal. We are going to divide this analysis in two sections: regulations, and social reforms.

From a regulatory point of view, there is a clear need for more specific and clear security standards. Many countries, especially emerging market countries, do not have specific laws in place to regulate the use of electronic and digital payments, making it difficult for service providers to enter the market and thus for people to benefit from them. This lack of regulation is yet another obstacle, besides ethical and religious beliefs which we analyzed in section 3.2, to Financial inclusion and consequently it slows down economic development and welfare. The regulatory issues are nonetheless crucial for western countries, which started to propose laws and regulations for modern digital payments only after the PSD2 directive has been implemented. Moreover, this directive, which is considered one of the most advanced and complete sets of regulations in place nowadays, (section 2.2) still has some flaws: it does not specify the authentication standards that must be used on hand-held devices, and it lacks in specific privacy and data storage indications. It is true indeed that it was conceptualized when the technology behind digital payments was different and less advanced and relying on mobile applications. For this reason, regulatory authorities must update and integrate these sets of rules, in parallel with the advancements of technologies, in order to respond to the most recent issues and concerns that new technologies inevitably bring. Moreover, as extensively analyzed in section 3.1, another focus must be on the implementation of shared policies, with the aim of reducing frictions and obstacles to international trade and digital payments implementation.

As we discussed in section 3.2, governments would have real advantages if consumers and merchants extensively used digital payment methods: it would limit tax evasion and reduce the costs of running a business, thus increasing competition and ultimately increasing the overall welfare of a country. Their role in helping the widespread diffusion of digital payments relies on social reforms and sensibilization of the public. They could organize advertisement campaigns to educate citizens on this matter, and incentives could be put in place for businesses that choose to

rely on digital payments. Regardless of the specific instruments that each government choose to use, their primary goal should be the diffusion of these new means of payments.

Finally, regulations and social efforts must develop together, since they are positively correlated: the more regulations there are, especially for what concerns privacy and data security, the more consumers and merchants will be willing to implement digital payments, and with the diffusion of them, the easier it will be for regulators to implement new and up to date laws to protect citizens and businesses.

### *3.4 Conclusions*

As analyzed in the 2018 World Cash Report, although many advocates of electronic payments have long predicted a cashless society, it does not seem to be a short-term goal for any country. Even Sweden, the country with the lowest dependency on cash in the world, is aware that there are many reasons to maintain cash and many obstacles to completely replace it. People often fight an ideological war between cash and cashless (with potential replacement of fiat currencies with cryptocurrencies), but it is reasonable to assume that there are additional options and that the answer to this issue is to be found on a spectrum, rather than being clearly identifiable as one way or the other.

Re-defining the concept of cashless society might help us understand the role of digital payments in the modern economy. In a cashless society every participant can enter the market, both as a consumer and as a merchant, without using cash, but still being able to use cash if preferred. This should be the goal of payment systems worldwide for the near future, and it is also the most realistic forecast one could make, especially for countries with already relatively low cash usage, such as Scandinavian countries. Cash and non-cash payments need to coexist, and there should not be any kind of competition between the two. Different means of payments simply serve different purposes, and an efficient payment system should allow consumers to make payments in all circumstances.

The present society is dominated by cash usage, with more than 2 billion people unconnected to the electronic banking infrastructure (2018 World Cash Report), and digital payments can help drastically reduce this number.

Mobile payments should represent the conjunction between a cash-only and a cashless market, with the aim of increasing financial inclusion and getting citizens closer to the banking system, allowing the greatest number of people to access credit and financial services.

In this way, the widespread diffusion of digital payments will allow for a more efficient payment system and a more competitive market, ultimately increasing the overall level of welfare.

**Bibliography**


Aigbe P. and Akpojaro J., 2014, “Analysis of security issues in electronic payment systems”, International Journal of Computer Applications;

Aina S. and Oluyombo O., 2014, “The Economy of Financial Inclusion in Nigeria: Theory, Practice, and Policy”, SSRN Electronic Journal;

Apple, 2020, “Apple Pay security and privacy overview”, https://support.apple.com/en-us/HT203027;

Batiz-Lazo B. and Del Angel G., 2018, “The Ascent of Plastic Money: International Adoption of the Bank Credit Card, 1950–1975”, Cambridge University Press;

Bezhovski Z., 2016, “The future of the Mobile Payment as Electronic Payment System”, European Jourrnal of Business and Management;

Brown A., 2016, “AliPay Vs WeChat Pay Vs UnionPay” FinanceFeeds, https://financefeeds.com/alipay-vs-wechat-pay-vs-unionpay-important-research/;

Brown S., 2019, “The risks of mobile wallets”, PCBB, https://www.pcbb.com/bid/2019-06-20-The-Risks-Of-Mobile-Wallets;

Capgemini Research Institute, 2019, “World Payment Report 2019”;

Chaum D., 1983, “Blind Signatures for Untraceable Payments”, Springer-Verlag;

Deloitte, 2019, “The future of digital payments: choices to consider for a new ecosystem”, Southeast Asia’s Financial Services;

DigiPay, 2020, “How biometric technology is enhancing the ease and security of digital payments?”, https://www.digipay.guru/blog/how-biometrics-is-driving-security-in-digital-payments/;

Directive (EU) 2015/2366 of the European Parliament and of the Council (PSD2), of 25 November 2015 on payment services in the internal market, http://data.europa.eu/eli/dir/2015/2366/oj;

Economic Times, 2020, “Definition of e-wallets”, https://economictimes.indiatimes.com/definition/e-wallets;

Emarketer and Kantar TNS, 2019, “Proximity Mobile Payment Users Worlwide, 2019”, https://www.emarketer.com/content/global-mobile-payment-users-2019;

Emarketer and Kantar TNS, 2019, “Technology use in Africa: Mobile Phones”, https://www.pewresearch.org/global/interactives/technology-use-in-africa-mobile-phones/;

G4S and Payments Advisory Group, 2018, “World Cash Report 2018”;

Gießmann S., 2015, “Money, Credit and Digital Payment 1971/2014: From the Credit Card to Apple Pay”, SAGE Publishing;

Glassman S. et Al., 1996, “The Millicent Protocol for Inexpensive Electronic Commerce”, System Research Center;

Henning M., 2019, “Data from 11.5 million customers of M-PESA land on the black market”, Sun Connect, https://sun-connect-ea.org/data-from-11-5-million-customers-of-m-pesa-land-on-the-black-market/;

Immordino G. and Russo F., 2016, “Cashless payments and Tax Evasion”, CSEF (Centre for studies in economics and finance), Working Paper 445;

Juniper Research, 2019, “Paypal heads Mobile Wallets rankings as user forecast to pass 2 billion next year”, https://www.businesswire.com/news/home/20180404005093/en/Juniper-Research-PayPal-Heads-Mobile-Wallet-Rankings;

Klein A., 2019, “Is China’s New Payment System the future?”, Center on regulation and markets by Brookings;

Liu L., 2020, “China’s finance world opens up to foreigners, sort of”, Bloomberg News, https://www.bloomberg.com/news/articles/2020-01-22/china-s-finance-world-opens-up-to-foreigners-sort-of-quicktake;

Mandell L., 1990, “The Credit Card Industry: A History”, MA: Twayne Publishers;

McKinley R., 1997, “Millicent Payment System Coming”, https://cardtrak.com/1997/03/12/news/millicent-payment-system-coming/;

Merchantsavvy, 2020, “Alipay Is Now The World’s Biggest Mobile Payment Platform With 1.2bn Users”, https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/;

MordorIntelligence, 2019, “Mobile Payment Market – Growth, Trends, and Forecasts (2020 – 2025)”;

Nambi S.N. et Al., 2019, “Near Field Communication, applications and performance studies”, DESE Indian Institute of Science;

Ozili Peterson K., 2018, “Impact of digital finance on financial inclusion and stability”, Essex Business School, Borsa Istambul Review;

PagamentiDigitali.it, 2019, “Pagamenti digitali in Italia: ancora forte il gap informative dei cittadini”, https://www.pagamentidigitali.it/news/pagamenti-digitali-in-italia-ancora-forte-il-gap-informativo-dei-cittadini/;

PayPal, 2020, “PayPal QR Code Payments”, https://www.paypal.com/us/webapps/mpp/qrcode;

Peng K. et Al., 2014, “Security Overview of QR Codes”, Massachusetts Institute of Technology;

Pitta J., 1999, “Requiem for a Bright Idea”, Forbes, https://www.forbes.com/forbes/1999/1101/6411390a.html#6a85aa62715f;

Pratini M., 2016, “How does PayPal work?”, https://fin.plaid.com/articles/how-does-paypal-work/;

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), of 27 April 2016, http://data.europa.eu/eli/reg/2016/679/oj;

Regulation (EU) 2019/881 of the European Parliament and of the Council (EU cybersecurity act), of 17 April 2019, ENISA, http://data.europa.eu/eli/reg/2019/881/oj;

ShiftProcessing, 2020, “Credit Card Fraud Statistics”, https://shiftprocessing.com/credit-card-fraud-statistics/;

Soutter L. et Al., 2019, “Digital Payments: impact factors and mass adoption in Sub-Saharan Africa”, Technology Innovation Management Review;

Statcounter, 2020, “Mobile Operating System Market Share Worldwide”, https://gs.statcounter.com/os-market-share/mobile/worldwide/2019;

Swinhoe D., 2020, “The biggest data breaches of the 21st century”, CSO Online, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html;

The UK Cards Association, 2018, “UK Card Payments 2017”;

The Street, 2019, “History of ebay: facts and timeline”, https://www.thestreet.com/markets/history-of-ebay

Wolfe D., 2016, “7 of Amazon’s failed payment predictions”, https://www.paymentssource.com/list/7-of-amazons-failed-payments-predictions;